# TAC Meeting

*January 9, 2020*

# 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.

# Agenda

1. Roll call
2. Approval of minutes
3. Action item review
4. “Confidential computing” definition & CCC scope
5. F2F meeting opportunities
6. Budget requests
7. Any other business

# Roll Call of TAC Voting Representatives

| Member | Representative | Email |
|---|---|---|
| Alibaba | Xiaoning Li | xiaoning.li@alibaba-inc.com |
| ARM | Charles Garcia-Tobin | charles.garcia-tobin@arm.com |
| Google | Brandon Baker | bsb@google.com |
| Huawei | Zhipeng (Howard) Huang | huangzhipeng@huawei.com |
| Intel | Simon Johnson | simon.p.johnson@intel.com |
| Microsoft | Dave Thaler(*) | dthaler@microsoft.com |
| Oracle | John Haxby | john.haxby@oracle.com |
| Red Hat | Mike Bursell | mbursell@redhat.com |

**TAC chair*

# Approval of Minutes

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2019/CCC%20TAC%20Minutes%202019-12-05.docx

**RESOLVED:** That the minutes of the December 5, 2019 meeting of the Technical Advisory Committee 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

# Action Item Review (1/2)

- [Mike/Stephen] Work with the GB on charter scope. **[ON AGENDA LATER]**
- [Stephano] Create a list for submission of the Project Proposal Template. Add the chair and the PM to that list.
- [ALL] Review the Project Proposal Template, currently located here: https://lists.confidentialcomputing.io/g/tac/wiki/Project-Proposal-Template
- [Stephano] Research GitHub, if it meets our needs (and the LF doesn't have a better turnkey solution), create an org and add a document repository project to store and collaborate on docs.
  - **DONE**: https://github.com/confidential-computing
- [Stephano] Upload the Project Progression Policy to GitHub and notify the list.
  - **DONE**: https://github.com/confidential-computing/governance/blob/master/project-progression-policy.md
- [Stephano/Stephen] Work with the LF to better define budget line items. See budget section for details on immediate questions. **[ON AGENDA LATER]**

CONFIDENTIAL COMPUTING CONSORTIUM

# Action Item Review (2/2)

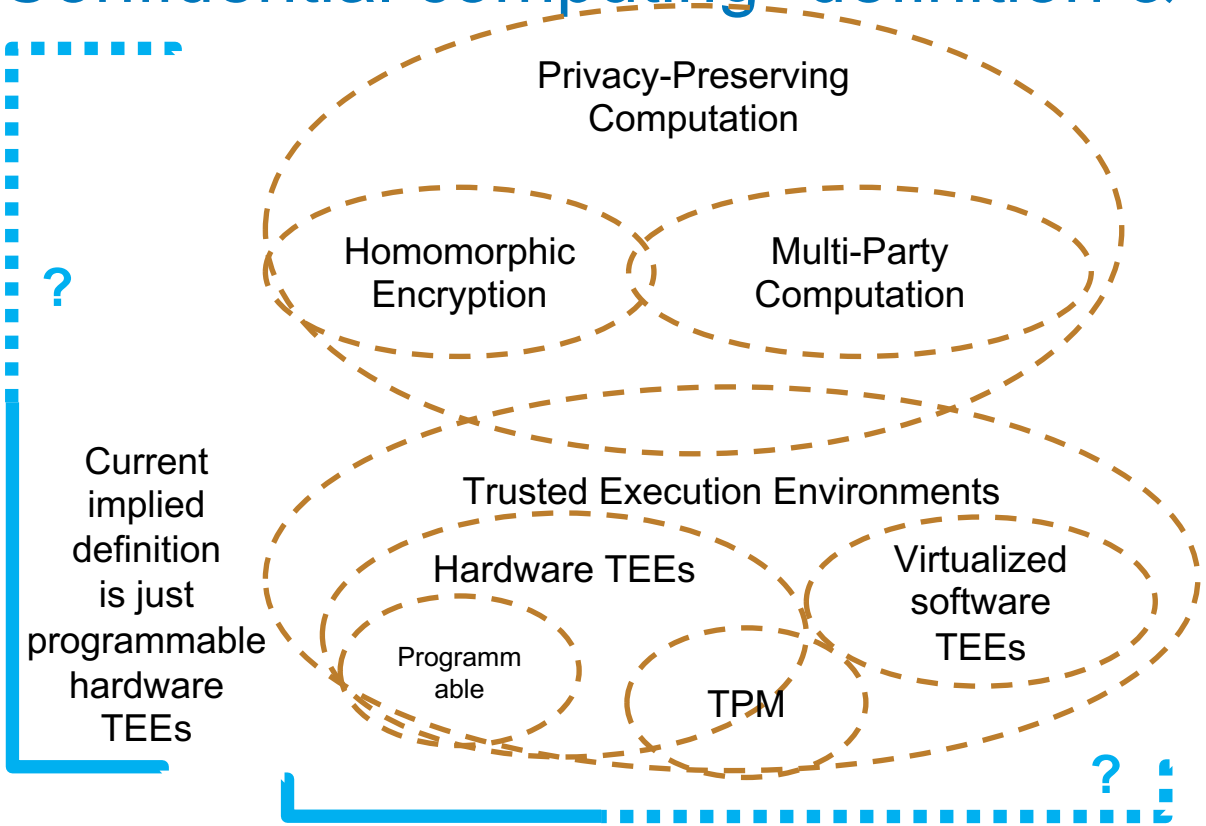
- [ALL] If you have thoughts about the website, please send those to Stephano. He will eventually provide a better way (wiki list, perhaps GitHub issues) to track those requests and their progress.
- [Mike] Put together a list of possible candidate technologies, around ½ a dozen, send it to the TAC list for review, then after review send to the GB. E.g. FPGAs, homomorphic encryption, a fully software virtualized trusted execution environment, hardware/software TEE, TPM technology, multi-party computation. You may want to define those for the GB (and for some of us) so that we can agree on them. **[ON AGENDA LATER]**
- [Simon] Chat with Jesse about documents that the consortium might publish as white papers so that Intel can coordinate with the Outreach committee.
- [Stephano] Email the list to start the discussion around if we should meet more regularly or for a longer period of time.
- [ALL] Please email the list, or Stephano/Dave directly with any comments regarding how they would like to see the meetings improve.

# “Confidential computing” definition & CCC scope

Two related, but different, questions:

1. Should the term “confidential computing” be broad like “privacy preserving computation”, or narrowly scoped to TEEs (or even certain classes of TEE)?
2. Should the consortium’s scope be more inclusive, or narrowly scoped to TEE-based projects

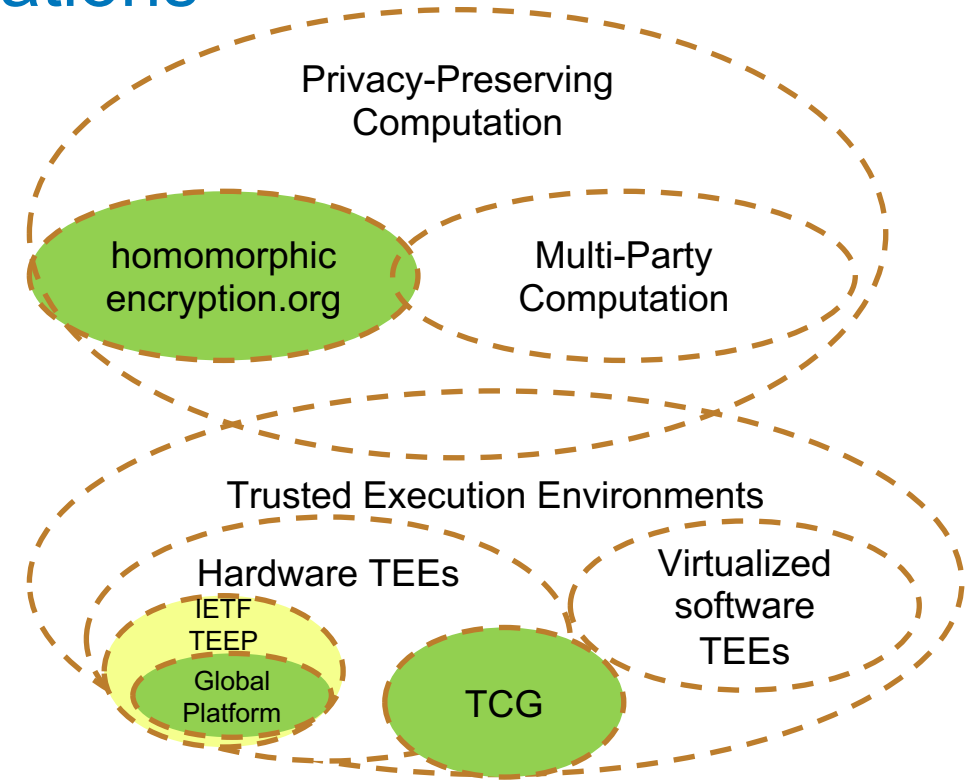
# “Confidential computing” definition & CCC scope




*Disclaimer:*
*Some terms have multiple competing definitions, so boundaries are often fuzzy.*

CONFIDENTIAL COMPUTING CONSORTIUM

# Organizations




CONFIDENTIAL COMPUTING CONSORTIUM

# Different definitions of TEE

Problem

- **Wikipedia:** A secure area of a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. A TEE as an isolated execution environment provides security features such as isolated execution, integrity of applications executing with the TEE, along with confidentiality of their assets.
- **ARM:** a secure area inside a main processor. It runs in parallel of the operating system, in an isolated environment. It guarantees that the code and data loaded in the TEE are protected with respect to confidentiality and integrity.
- **IETF TEEP WG:** An environment that enforces that only authorized code can execute with that environment, and that any data used by such code cannot be read or tampered with by any code outside that environment.
- **GlobalPlatform:** A device that conforms to specifications from GP's TEE Committee
- **Mike**: a hardware-based technique for securing sensitive data and algorithms in such a way that even the kernel, root user or hypervisor can't see what's going on

Other aspects that are important but may not be part of the definition itself:
attestation, identity, hardware tamper-evident/resistant, …

# TEE variations

- A processor (e.g., an MCU) might *only* have a TEE and no REE
- Separate processors may have (or be) a “TEE”:
    - Secure Element, FPGA, HSM, TPM, NIC
- A “TEE” might not be programmable
    - E.g., TPM, secure cryptoprocessor
- A virtualized TEE might be indistinguishable in practice from a hardware TEE except in terms of which certificate(s) it chains up to

# TEE variation definitions

- **secure cryptoprocessor**: a dedicated computer-on-a-chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, which give it a degree of tamper resistance. Unlike cryptographic processors that output decrypted data onto a bus in a secure environment, a secure cryptoprocessor does not output decrypted data or decrypted program instructions in an environment where security cannot always be maintained. The purpose of a secure cryptoprocessor is to act as the keystone of a security subsystem, eliminating the need to protect the rest of the subsystem with physical security measures.
- **Trusted Platform Module** (**TPM**, also known as **ISO/IEC 11889**): an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.
- **hardware security module** (**HSM**): a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
- **Secure Element (SE)**: a microprocessor chip which can store sensitive data and run secure apps such as payment. It acts as a vault, protecting what's inside the SE (applications and data) from malware attacks that are typical in the host (i.e. the device operating system).

# Privacy-preserving computation

- **multi-party computation (MPC)**, or **privacy-preserving computation**: a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.
- **Homomorphic encryption**: a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.  Homomorphic encryption can be used for **privacy-preserving** outsourced storage and **computation**. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted.

# Confidential Computing (1/2)

Problem

- **Gartner report:** Confidential computing is the combination of CPU-based hardware technology and infrastructure as a service (IaaS) cloud provider virtual machine (VM) images and software tools that enable cloud-using organizations to create completely isolated trusted execution environments (TEE), also called enclaves. Because they offer a form of encryption of data in use, these enclaves render sensitive information invisible to host OSs and cloud providers.
- **CCC press release:** Established in 2019, the Confidential Computing Consortium brings together hardware vendors, cloud providers, developers, open source experts and academics to accelerate the confidential computing market; influence technical and regulatory standards; build open source tools that provide the right environment for **TEE** development' and host industry outreach and education initiatives. Its aims to address **computational trust and security for data in use, enabling encrypted data to be processed in memory without exposing it to the rest of the system**, reducing exposure to sensitive data and providing greater control and transparency for users.

CONFIDENTIAL COMPUTING CONSORTIUM

# Confidential Computing (2/2)

- **Mark Russinovich blog:**
  - Put simply, confidential computing offers a protection that to date has been missing from public clouds, **encryption of data while in use**. …
  - Confidential computing ensures that when data is “in the clear,” which is required for efficient processing, the data is protected inside a **Trusted Execution Environment** (TEE - also known as an enclave), an example of which is shown in the figure below. TEEs ensure there is no way to view data or the operations inside from the outside, even with a debugger. They even ensure that only authorized code is permitted to access data. If the code is altered or tampered, the operations are denied and the environment disabled. The TEE enforces these protections throughout the execution of code within it.

# Face to face meeting opportunities

Joint email thread with Board, TAC, and Outreach

Following candidates were listed:

- **RSA Moscone Center, San Francisco, February 24 - 28, 2020**
- SCaLE 18x Pasadena CA, Convention Center, March 5 - 8, 2020
- Linux Foundation Member Summit, Lake Tahoe, CA, March 10 – 12, 2020

# Budget requests

- https://lists.confidentialcomputing.io/g/tac/attachment/30/0/Consortium%20Budget%20Nov%202019.xlsx

| V. IT Infrastructure and Staff | | | |
|---|---|---|---|
| License Scanning | $40,000.00 | Will grow as projects are added | Compliance |
| Test infrastructure | $50,000.00 | A placeholder figure for now, discussion | IT Infrastructure |
| General Infrastructure | $10,000.00 | IT Infrastructure | IT Infrastructure |

- OpenEnclave group reports on current CI/CI budget for the CCC OE repo:
  - “the annual budget for CI/CD project will be (2K * 4) * 12 = 96K. I will recommend reserving 100K for OE CI/CD.”
- Since the Intel SGX SDK is in the process of merging with the OpenEnclave SDK, we believe this budget request covers both?

CONFIDENTIAL COMPUTING CONSORTIUM

# Any other business

- Next meeting: January 16 or 23? 1 hour or 1.5 or 2 hours?
    - “There is agreement that 1 hour every 2 weeks is not enough time to be productive.”

# Legal Notices

The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation's Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.

Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute's trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.

Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.

TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.

Facebook and the "f" logo are trademarks of Facebook or its affiliates.

LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.

YouTube and the YouTube icon are trademarks of YouTube or its affiliates.

All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.

The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy. each as may be modified from time to time. More information about The Linux Foundation's policies is available at https://www.linuxfoundation.org.

Please email legal@linuxfoundation.org with any questions about The Linux Foundation's policies or the notices set forth on this slide.