# TAC Meeting

*February 18, 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. Scoping discussion
    - Defining “confidential computing”
5. Agenda for face-to-face meeting next week
6. Any other business

# Roll Call of TAC Voting Representatives

Quorum requires 5 or more voting reps:

| Member | Representative | Email |
|---|---|---|
| Alibaba | Xiaoning Li | xiaoning.li@alibaba-inc.com |
| ARM | Grant Likely | grant.likely@arm.com |
| Facebook | Jinsong Yu | jinsongyu@fb.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/2020/CCC%20TAC%20Minutes%202020-02-06.pdf

**RESOLVED:** That the minutes of the February 6, 2020 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

- [Stephano] Eventually provide a better way (wiki list, perhaps GitHub issues) to track website content requests and their progress.
- ~~[Seth/Dave] Discuss how TAC/Outreach can coordinate. [DONE]~~
- [Stephano] Determine if the last meeting was recorded and if so, place a link to that recording in Groups.io
- ~~[Dave] Summarize the discussion around CCC definition and scope for the Governing Board [DONE]~~
- [Pushkar Chitnis] Provide details for OE SDK ask on CI/CD pipeline costs.
- ~~[All] Review and comment on Code of Conduct on GitHub. [NOTHING FURTHER REQUIRED]~~
- [Stephano] Move outreach files into the main group and send a link to the list so that the TAC can access their materials (specifically the Positioning)

# Scoping discussion

- Outreach Positioning document – is it visible to the TAC now?
- https://github.com/confidential-computing/governance/pull/12 has updates from last meeting and email discussion, ok to merge?
- We got consensus on wording for scoping for projects
    - But still need wording for a proposed definition of “Confidential Computing”
- We also agreed that it should not use the terms “cloud”, “main processor”, or “encrypted”, and that it should not imply it’s the *only* way to protect data in use (since privacy-preserving computation is separate)

# Defining “Confidential Computing” (1/3)

- CCC FAQ at https://confidentialcomputing.io/ has:
  - Q: What is confidential computing?
  - A: Confidential computing focuses on securing data in use. Current approaches in **cloud** computing address data at rest and in transit but **encrypting** data in use is considered the third and possibly most challenge step to providing a fully **encrypted** lifecycle for sensitive data. Confidential computing will enable **encrypted** data to be processed in memory without exposing it to the rest of the system. Confidential computing will reduce exposure for sensitive data and provide greater control and transparency for users.

True, but so does privacy-preserving computation, so this is not a definition

- We need to agree on replacement text

# Defining “Confidential Computing” (2/3)

In email (https://lists.confidentialcomputing.io/g/tac/message/161),
Dave proposed a FAQ answer for a related question:

- Q: What is the relationship between “Confidential Computing” and "Privacy-Preserving Computation"?
- A: Both are means to protecting data in use, but do so in different ways:
  - **Confidential Computing** protects data in use by doing computation inside a hardware-based Trusted Execution Environment that keeps data confidential from outside parties.
  - **Privacy-Preserving Computation**, on the other hand, protects data in use by doing computation on encrypted data such that the unencrypted data is kept private even from the processor doing the computation.
  - Thus **Privacy-Preserving Computation** "preserves" the privacy already inherent in not having the data, whereas **Confidential Computing** has the data, but keeps it confidential.

# Defining “Confidential Computing” (3/3)

- What should CCC FAQ at https://confidentialcomputing.io/ say?
  - Q: What is confidential computing?
  - A: Confidential Computing is… <need text here>
- Strawman adaptation based on previous slide (feel free to wordsmith):
  - **Confidential Computing** is means for protecting data in use by doing computation inside a hardware-based Trusted Execution Environment that keeps data confidential from outside parties.
- Can we get TAC consensus before the board meets on the 27th?

CONFIDENTIAL COMPUTING CONSORTIUM

# Face-to-face meeting schedule

Dave/Seth discussed having some joint TAC/Outreach topics, which requires TAC members to be there 30 minutes early, and Outreach to stay 30 mins later:

- 8:00-8:50am BOF at RSA
- 8:00-9:30am Outreach committee meeting
- 9:30-10:30am Joint Outreach/TAC meeting
  - Discuss analyst briefing content, briefing team, list of analysts beyond Gartner [Seth]
  - Preview Definition/Positioning Proposal to Board [Seth and Dave]
- 10:30-noon TAC meeting
- Noon-1:00pm Lunch
- 1:00pm-3:00pm Board

CONFIDENTIAL COMPUTING CONSORTIUM

# Agenda items for TAC session 10:30-noon?

- Possible topics:
  - TAC Budget
  - Which other standards orgs should we interact with and how?
    - (IETF? GlobalPlatform? ITU? ISO? TCG? Etc.)
  - …

- Should focus first on topics we need movement on sooner than later

# Any other business

# BACKUP:
# Terminology/Scoping Slides from Previous Meetings

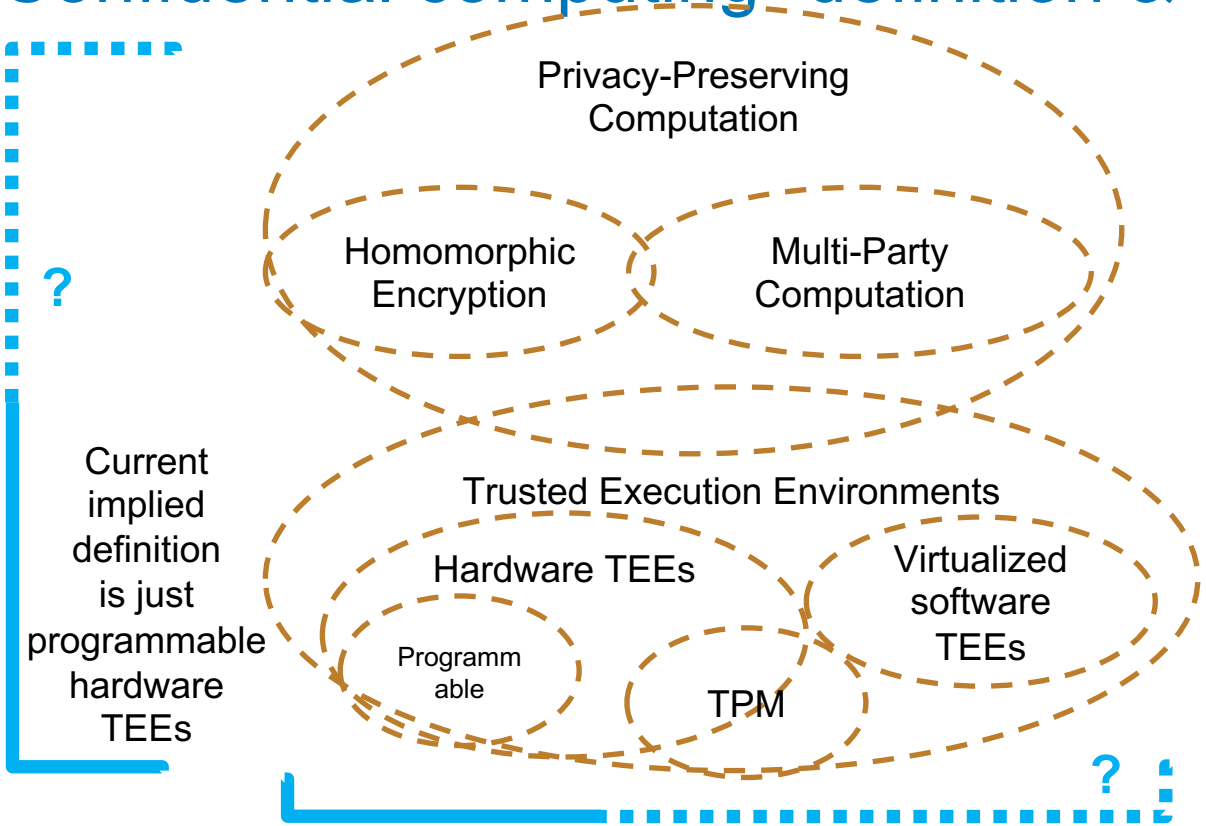
# “Confidential computing” definition & CCC scope

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

    - If narrow, focus stays on TEEs, and messaging on terminology might compete with other bodies in the industry
    - If broad, this discussion happens inside the CCC and the CCC has the opportunity to have unified messaging

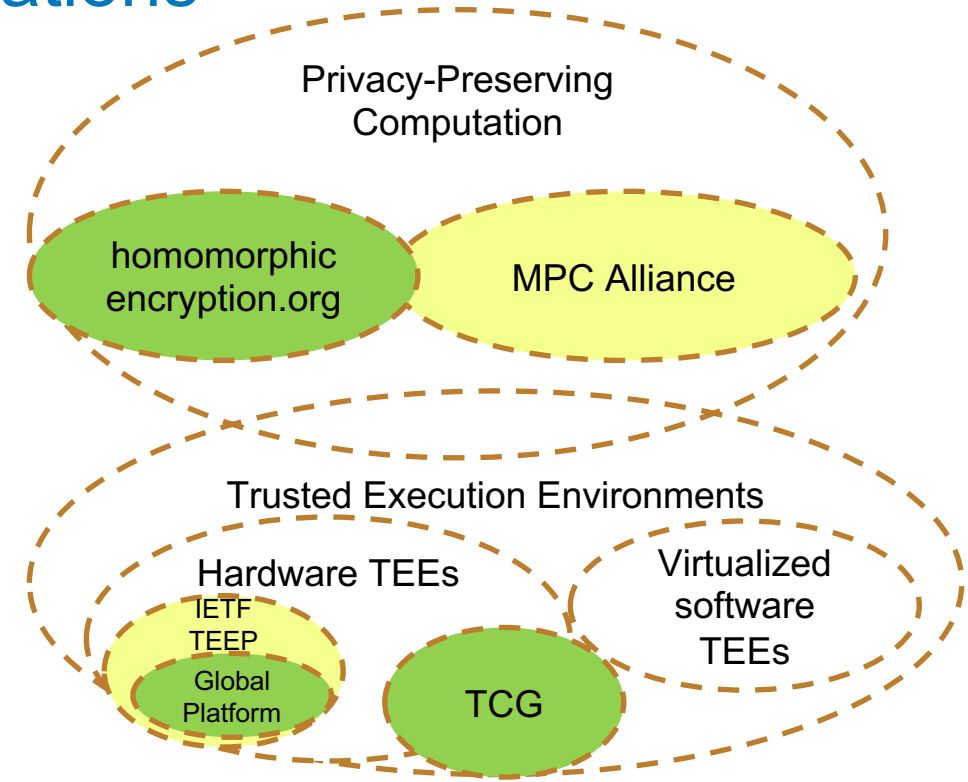
# “Confidential computing” definition & CCC scope




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

CONFIDENTIAL COMPUTING CONSORTIUM

# Organizations




CONFIDENTIAL COMPUTING CONSORTIUM

# Possible axes for categorising technologies

Rough consensus that the following 5 axes are important to answer:

| Axis | TAC Consensus |
|---|---|
| algorithmic (mathematical) vs hardware/software | ? (split opinions) |
| hardware (+firmware?) vs software | ? (some argued for software too) |
| generalised vs specialised computation only | No one argued for non-programmable |
| on-main CPU vs off-main CPU | Broad |
| cloud vs on-prem (incl. IoT) | Broad (whole axis) |

Other attributes (e.g., TCB size) are also important evaluation criteria but by themselves weren't seen as part of scoping question per se

| **Example technology** | Hard-/software **I**mplementation or **A**lgorithmic | **H**ardware or **S**oftware) | **G**eneralised compute or **S**pecialised) | O**N**-main CPU (vs o**F**f-main CPU) | **C**loud (vs on-**P**rem, incl. IoT) |
|---|---|---|---|---|---|
| Homomorphic encryption | A | --- | S? | --- | C/P |
| Multi-party Computation | A | --- | G? | --- | C/P |
| HSM | I | H | S (can be G?) | F | C/P |
| TPM | I | H | S | F | C/P |
| **Hardware TEE on main CPU (e.g., SGX)** | I | H | G | N | C/P |
| Virtualised software TEE | I | S | G | **N** | **C/P** |
| FPGA | I | H | S | F | C/P |
| **TEE in NIC** | I | H | S | F | C/P |
| Secure Element | I | H | S? | F | P |
| …? | | | | | |

# 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

# 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.