Confidential Computing Consortium Introduction

Dave Thaler <dthaler@microsoft.com>
Chair, CCC Technical Advisory Council

CONFIDENTIAL COMPUTING
CONSORTIUM

The Confidential Computing Consortium will define Confidential Computing and accelerate its acceptance and adoption in the market.

The Confidential Computing Consortium

- Community focused on projects securing DATA IN USE and accelerating the adoption of confidential computing through open collaboration
- Announced the intent to form in August at the Open Source Summit North America in San Diego, formally launched on 17 October 2019 with governance in place

Please visit https://confidentialcomputing.io

CONFIDENTIAL COMPUTING CONSORTIUM

CCC Members

Premier

General

CONFIDENTIAL COMPUTING CONSORTIUM

How the Consortium Is Structured

- The Confidential Computing Consortium is an **umbrella project** of the Linux Foundation. The Consortium will support development of numerous technical projects (open source and open specification).
- High-level governance overview:
    - **Governing Board** – responsible for funding decisions; and
    - **Technical Advisory Council** – enables communication among the separate technical projects and between the technical projects and the Governing Board; and
    - **Separate technical oversight for each technical project** – separate technical oversight for each independent technical project, customized to the needs of the project and its community.

CONFIDENTIAL COMPUTING CONSORTIUM

Mission of the CCC (Charter)

The purpose of the Confidential Computing Consortium (the “Directed Fund”) is to raise, budget and spend funds in support of various open source and/or open standards projects relating to:

- defining confidential computing and accelerate acceptance and adoption in the market.
- developing open enterprise-grade building blocks (e.g. open specifications and open source licensed projects), including a confidential managed compute portfolio and development experience, to enable easy development and management of enterprise-grade confidential compute applications, and
- defining foundational services and frameworks that are confidential-aware and minimize the need for trust.

CONFIDENTIAL COMPUTING CONSORTIUM

Scope of the CCC

- The Consortium will support an ecosystem of open technical projects (open source and open standards / specifications) focused on Confidential Computing.
- The Consortium is concentrating on the area of "data in use," with the confidentiality of "data in transit" and "data at rest" as outside the scope of the Consortium.
- The Consortium is interested in including participation from a wide spectrum community of members developing, implementing or using technologies related to Confidential Computing.
- The Consortium intends to include participation from a diverse group of members including semiconductor manufacturers, cloud infrastructure organizations, hardware vendors and software developers.

“Confidential Computing”

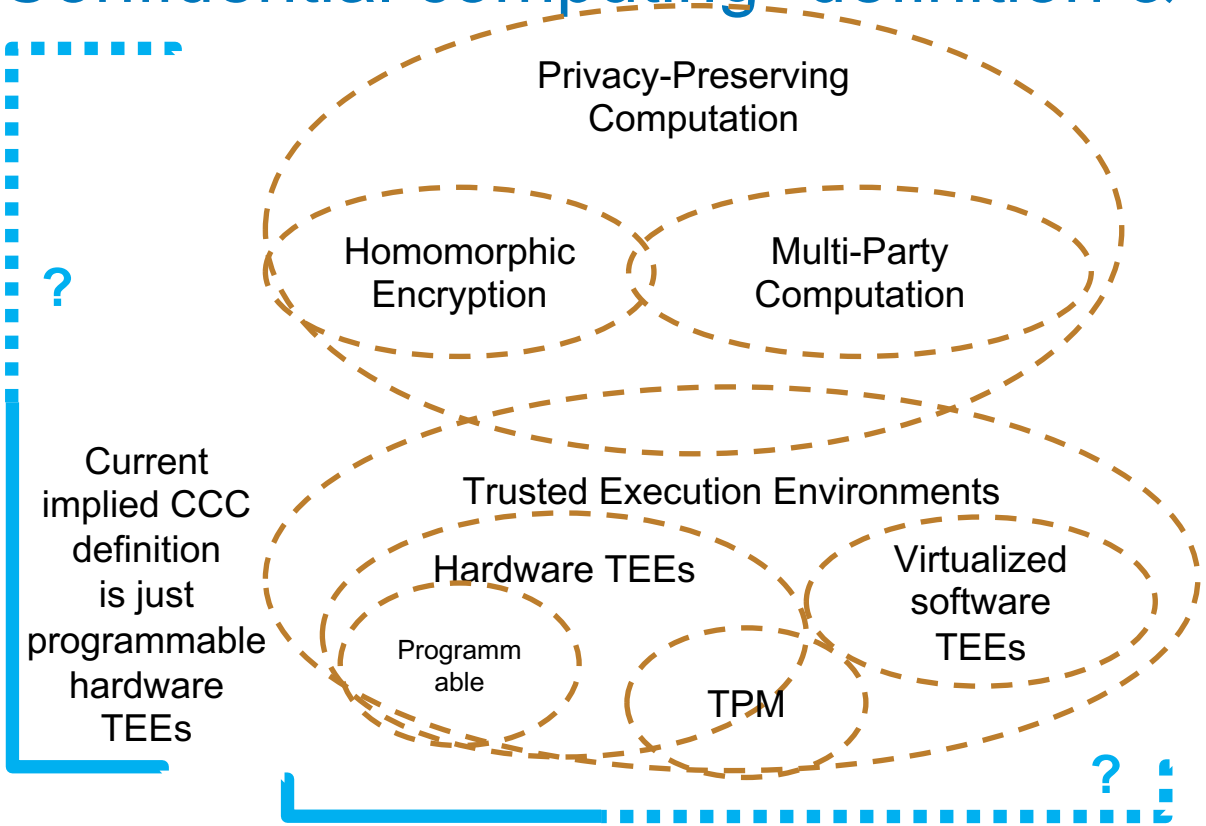
- **CCC press release:** Established in 2019, the Confidential Computing Consortium brings together hardware vendors, cloud providers, developers, open source experts and academics to accelerate the confidential computing market; influence technical and regulatory standards; build open source tools that 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.
- **TechTarget definition:** Confidential computing is a concept in which **encrypted data can be processed in memory to limit access to ensure data in use is protected**. Confidential computing is a concept promoted by the Confidential Computing Consortium, which is a group of organizations that wants to build **tools supporting the protection of data**. This concept is especially suitable for public clouds.

CONFIDENTIAL COMPUTING CONSORTIUM

“Privacy-preserving computation”, from Wikipedia

- **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.

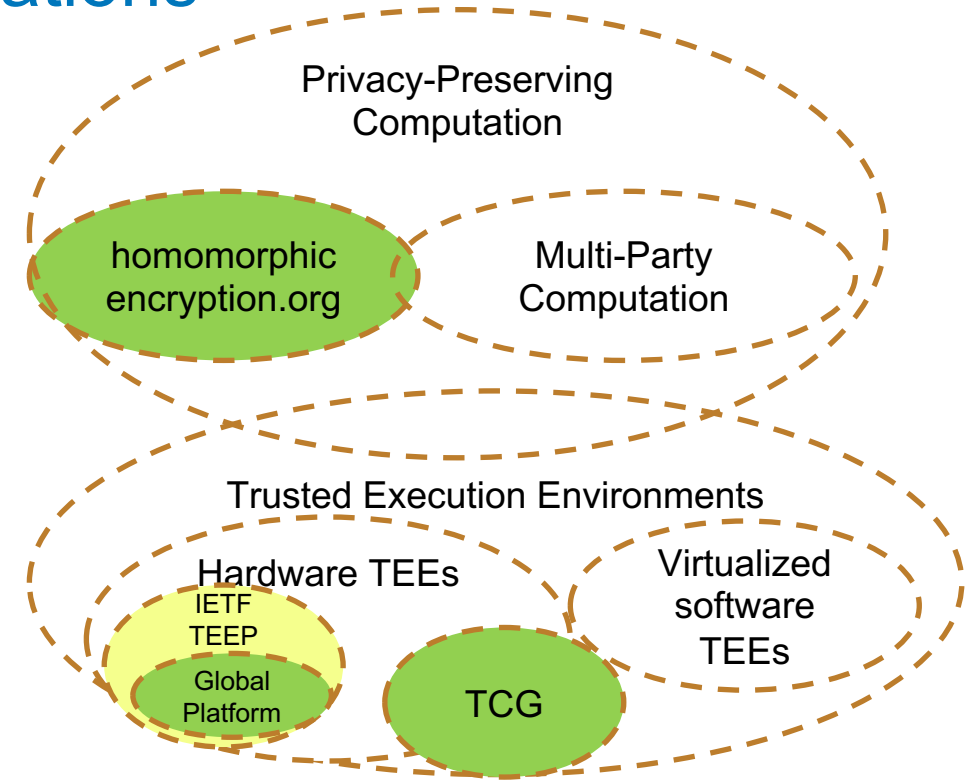
“Confidential computing” definition & CCC scope



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

CONFIDENTIAL COMPUTING CONSORTIUM

Organizations



Many different options for collaboration exist

a) CCC's legal framework could be augmented to host HE as a SIG of some sort
b) Could set up some liaison relationship between the two orgs
c) Could have a joint workshop on relevant topics
d) Could collaborate on some marketing material to be jointly authored
e) An open source project for HE library usable within a Trusted Execution Environment (SGX, TrustZone, AMD-SEV, etc.) could be contributed to the CCC