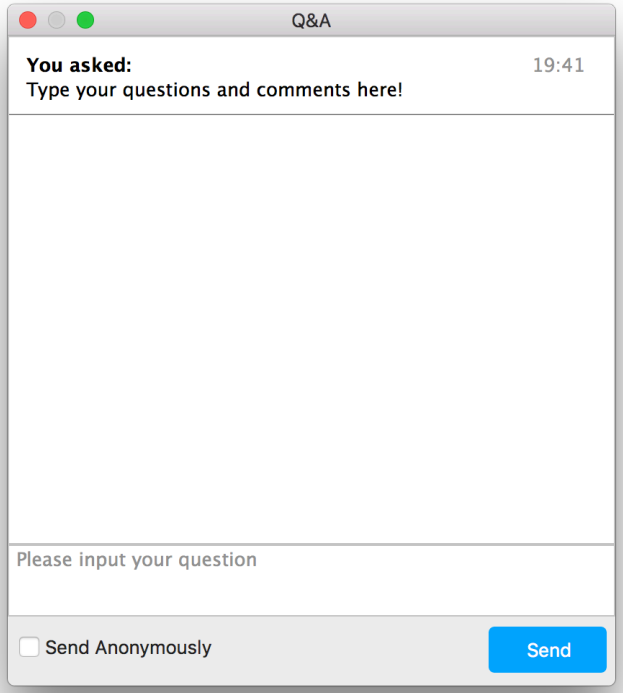
Confidential Computing:
Protecting Applications and Data In Use

Housekeeping

- Webinar recording
- Presentation slides
- Question and answer



CONFIDENTIAL COMPUTING CONSORTIUM

Seth Knox [he/him]

Outreach Committee Chair

Fortanix

@seth_knox

sethknox

Nelly Porter [she/her]

Lead Product Manager

Google

@nellyporter

nelly-porter

Dave Thaler [he/him]

Technical Advisory Council Chair

Microsoft

dthaler@microsoft.com

dthaler@microsoft.com

Aeva Black [they/them]

Open Source Program Manager

Microsoft

@aevavoom

aevaonline

CONFIDENTIAL COMPUTING CONSORTIUM

Seth Knox

Fortanix

@seth_knox

sethknox

Introduction

CONFIDENTIAL COMPUTING CONSORTIUM

The Confidential Computing Consortium

- Community focused on open source licensed 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

Consortium Members

Premier

accenture

蚂蚁集团 ANT GROUP

Google

Microsoft

Red Hat

arm

intel

FACEBOOK

HUAWEI

ORACLE

General and Associate

AMD

字节跳动 ByteDance

Fortanix

vmware

EDGELESS SYSTEMS

NVIDIA

IoTeX

Baidu 百度

Anqlave

cosmian

KINDITE

CYSEC

MADANA

MIT Connection Science
the technology of innovation

anjuna

decentriq

PHALA NETWORK

swisscom

OASIS LABS

Tencent 腾讯

CONFIDENTIAL COMPUTING CONSORTIUM

Nelly Porter
Google
@nellyporter
nelly-porter

Customers' Voice

CONFIDENTIAL COMPUTING CONSORTIUM

Data protection **challenges**

Key concerns on our customers' minds

- How do I protect sensitive data or my IP?
- How do I stay compliant with data protection regulations?
- How do I collaborate with other companies processing their sensitive data?
- How do I protect my clients' and users' data?

CONFIDENTIAL COMPUTING CONSORTIUM

Defense In depth

Limit the visibility and access to sensitive data

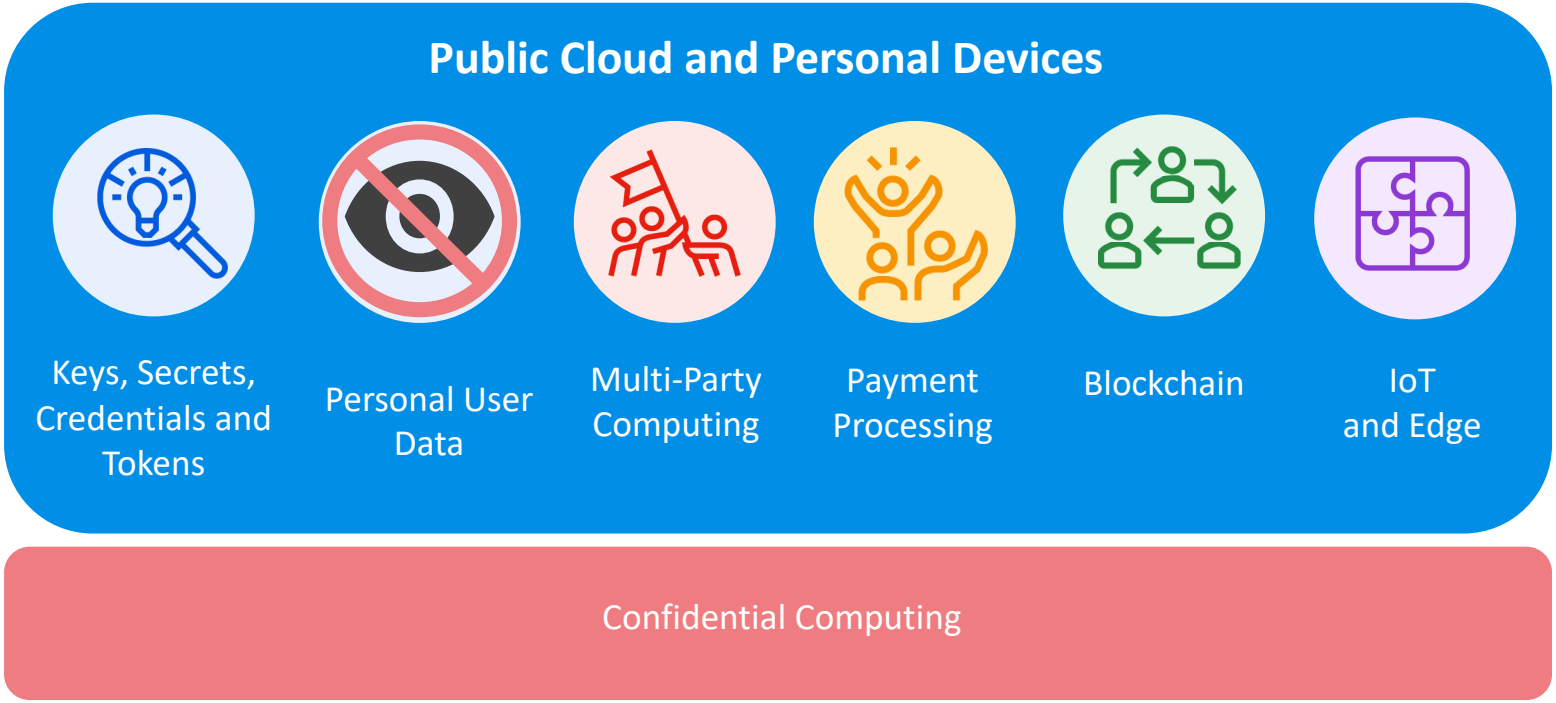
Encryption is the way how one can safeguard the sensitive data

Encryption at rest

Encryption in transit

What about processing sensitive data while it is in use?

Customer Centric Approach



Key takeaways

01

Confidential Computing is a critical industry effort in secure computing

02

CCC focuses on the use cases that are top of the mind for customers

03

CCC ensures ecosystem and community are part of the conversation

CONFIDENTIAL COMPUTING CONSORTIUM

Dave Thaler
Microsoft
dthaler@microsoft.com
dthaler

Definitions

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing Definition

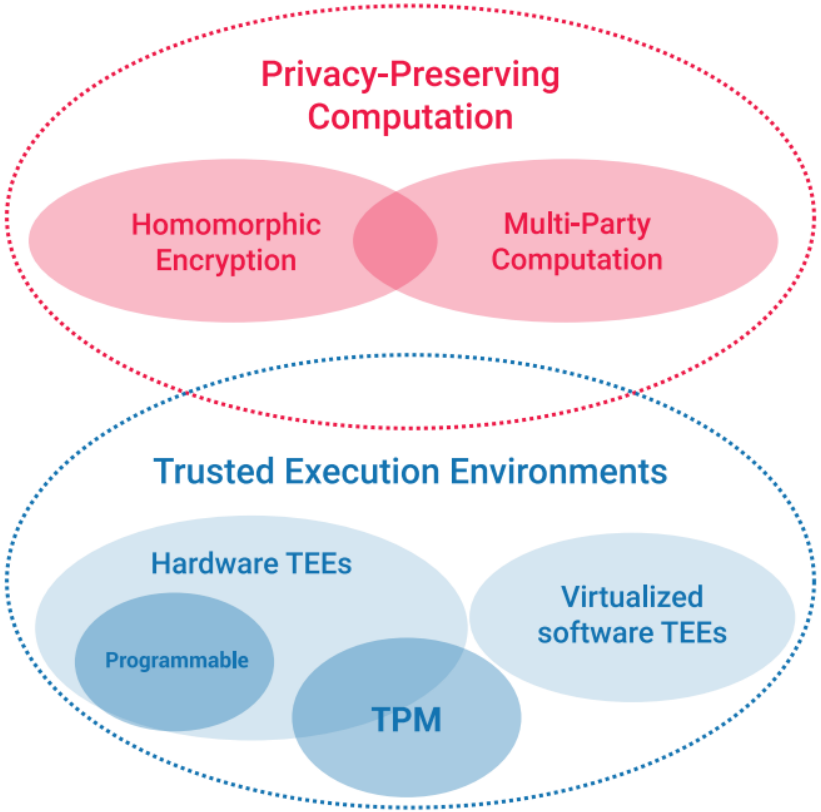
Confidential Computing is the ***protection of data in use*** *by performing computation in a* ***hardware-based Trusted Execution Environment****.*

- Definition is independent of topological location, which processor does it, and whether encryption or some other isolation technique is used.

- More discussion: confidentialcomputing.io/scoping

CONFIDENTIAL COMPUTING CONSORTIUM

Protecting Data In Use: Related Technologies



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

CONFIDENTIAL COMPUTING CONSORTIUM

Trusted Execution Environment Definition

A Trusted Execution Environment (TEE) is an environment that provides a level of assurance of three key properties:

Data confidentiality

Data integrity

Code integrity

Security Comparison vs Related Technologies

	HW TEE	Homomorphic Encryption	Secure element e.g., TPM
Data integrity	Y	Y (subject to code integrity)	Keys only
Data confidentiality	Y	Y	Keys only
Code integrity	Y	No	Y
Code confidentiality	Y (may require work)	No	Y
Authenticated Launch	Varies	No	No
Programmability	Y	Partial (“circuits”)	No
Attestability	Y	No	Y
Recoverability	Y	No	Y

Technologies can be combined to get even better security

CONFIDENTIAL COMPUTING CONSORTIUM

Scalability Comparison vs Related Technologies

	Native	HW Tee	Homomorphic Encryption
Data size limits	High	Medium	Low
Computation Speed	High	High-Medium	Low
Scale out across machines	Yes	More work	Yes
Ability to combine data across sets (MPC)	Yes	Yes	Very limited

Combining technologies generally lowers scalability

CCC Threat Model

Goal

Confidential Computing aims to reduce the ability for the owner/operator/pwner of a platform to access data and code inside TEEs sufficiently such that this path is not an economically or logically viable attack.

CCC Threat Model

Goal

> Confidential Computing aims to reduce the ability for the owner/operator/pwner of a platform to access data and code inside TEEs sufficiently such that this path is not an economically or logically viable attack.

In scope

- Software attacks
  - Host software/firmware
- Protocol attacks
  - Attestation, workload/data transport
- Cryptographic attacks
  - Mathematical/quantum attacks
- Basic hardware attacks
  - Bus/cache monitoring, cold DRAM, etc.
- Basic upstream supply-chain attack
  - E.g. addition of debugging ports

CCC Threat Model

Goal

Confidential Computing aims to reduce the ability for the owner/operator/pwner of a platform to access data and code inside TEEs sufficiently such that this path is not an economically or logically viable attack.

In scope

- Software attacks
  - Host software/firmware
- Protocol attacks
  - Attestation, workload/data transport
- Cryptographic attacks
  - Mathematical/quantum attacks
- Basic hardware attacks
  - Bus/cache monitoring, cold DRAM, etc.
- Basic upstream supply-chain attack
  - E.g. addition of debugging ports

Out of scope

- Sophisticated hardware attacks
  - Typically require long-term and/or invasive access
  - E.g. chip-scraping or electron microscope probes
- Upstream hardware supply-chain attacks
  - Attacks on TEE-related hardware such as CPU
  - E.g. attacks at manufacturing or key injection time

CCC Threat Model

Different TEE implementations will have varying degrees of resistance to attack.

- Particularly true of integrity attacks, rollback, and replay

CCC Threat Model

Different TEE implementations will have varying degrees of resistance to attack.

- Particularly true of integrity attacks, rollback, and replay

Attestation is important – and complex

CCC Threat Model

Different TEE implementations will have varying degrees of resistance to attack.

- Particularly true of integrity attacks, rollback, and replay

Attestation is important – and complex

"Allow the Verifier to gain confidence in the trustworthiness of the Attester by obtaining an authentic, accurate, and timely report about the software and data state of the Attester."

CCC Threat Model

Different TEE implementations will have varying degrees of resistance to attack.

- Particularly true of integrity attacks, rollback, and replay

Attestation is important – and complex

- Allows you to know
  - What's running underneath your workload
  - That your workload has been correctly loaded

"Allow the Verifier to gain confidence in the trustworthiness of the Attester by obtaining an authentic, accurate, and timely report about the software and data state of the Attester."

CONFIDENTIAL COMPUTING CONSORTIUM

CCC Threat Model

Different TEE implementations will have varying degrees of resistance to attack.

- Particularly true of integrity attacks, rollback, and replay

Attestation is important – and complex

- Allows you to know
  - What's running underneath your workload
  - That your workload has been correctly loaded

"Allow the Verifier to gain confidence in the trustworthiness of the Attester by obtaining an authentic, accurate, and timely report about the software and data state of the Attester."

Example

I wish to run an app to manage cryptographic keys in the public cloud. How can TEEs help?

- Data and code Integrity protection – core capabilities
- Data confidentiality protection – core capabilities
- Workload injection attacks – attestation
- Transport substitution attacks – protocol protections

Side channels

- Novel attack chain. Significant area of research
- Some side channels considered out-of-scope by hardware vendors
- Limited utility in the wild, not seeing them in practical use
- Industry is working to address them, both in software/microcode and in subsequent hardware generations

Side channels

- Novel attack chain. Significant area of research
- Some side channels considered out-of-scope by hardware vendors
- Limited utility in the wild, not seeing them in practical use
- Industry is working to address them, both in software/microcode and in subsequent hardware generations

Designing software with TEE usage in mind can allow mitigations

- Within the application
- By a compiler
- Through an SDK model
- Within the run-time

All of the above mitigations are within scope of the CCC

Aeva Black

Microsoft

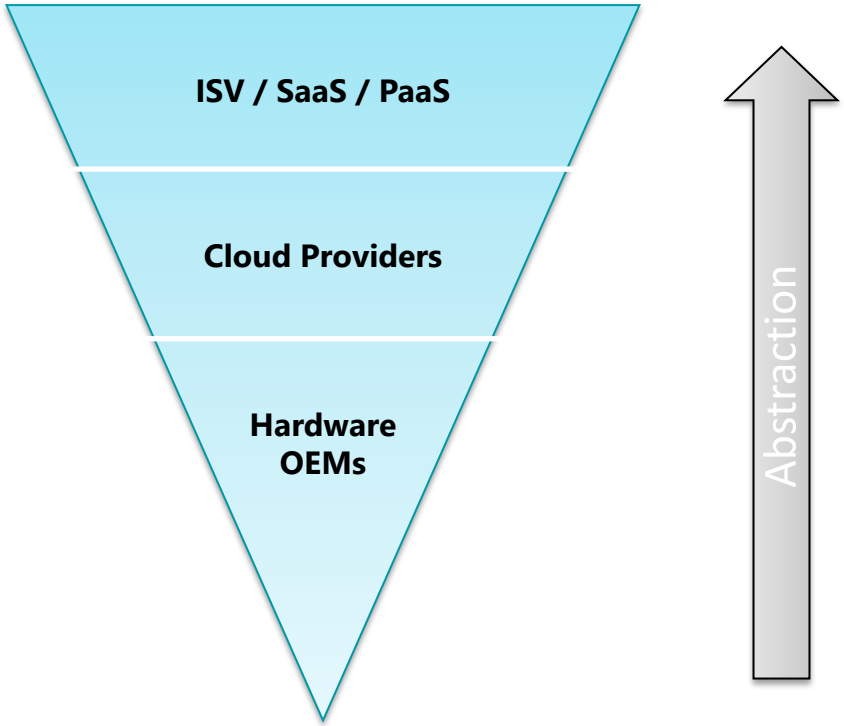
@aevavoom

aevaonline

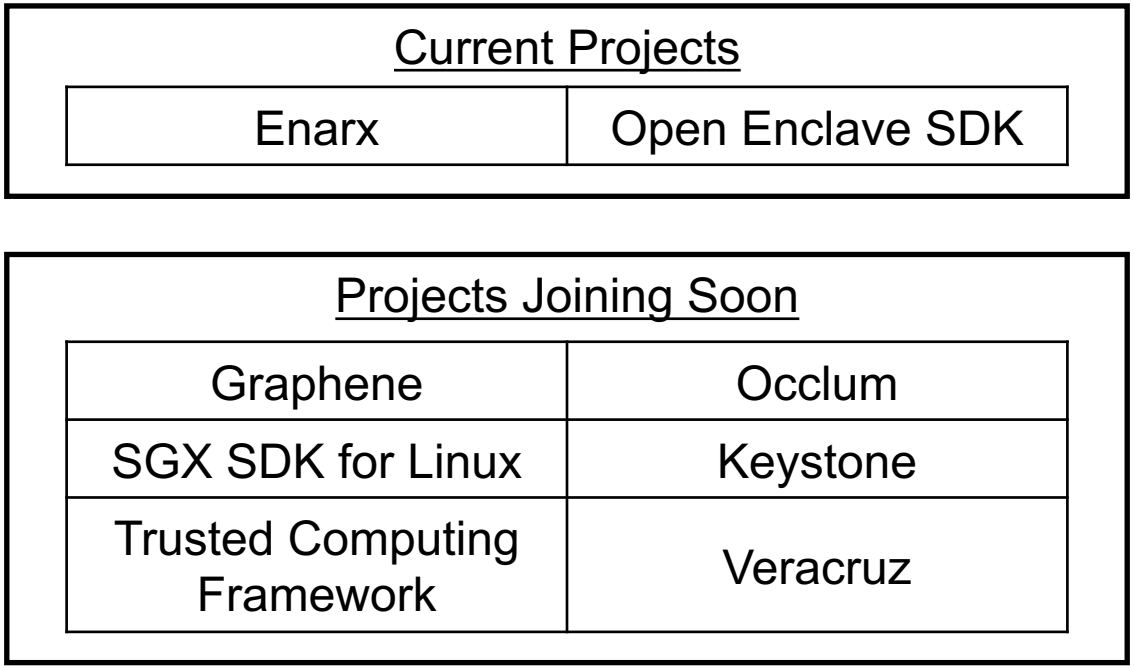
Adoption

CONFIDENTIAL COMPUTING CONSORTIUM

Product Abstractions



Project Landscape



Paradigm #1: App Development

Current Projects	
Enarx	Open Enclave SDK

Projects Joining Soon	
Graphene	Occlum
SGX SDK for Linux	Keystone
Trusted Computing Framework	Veracruz

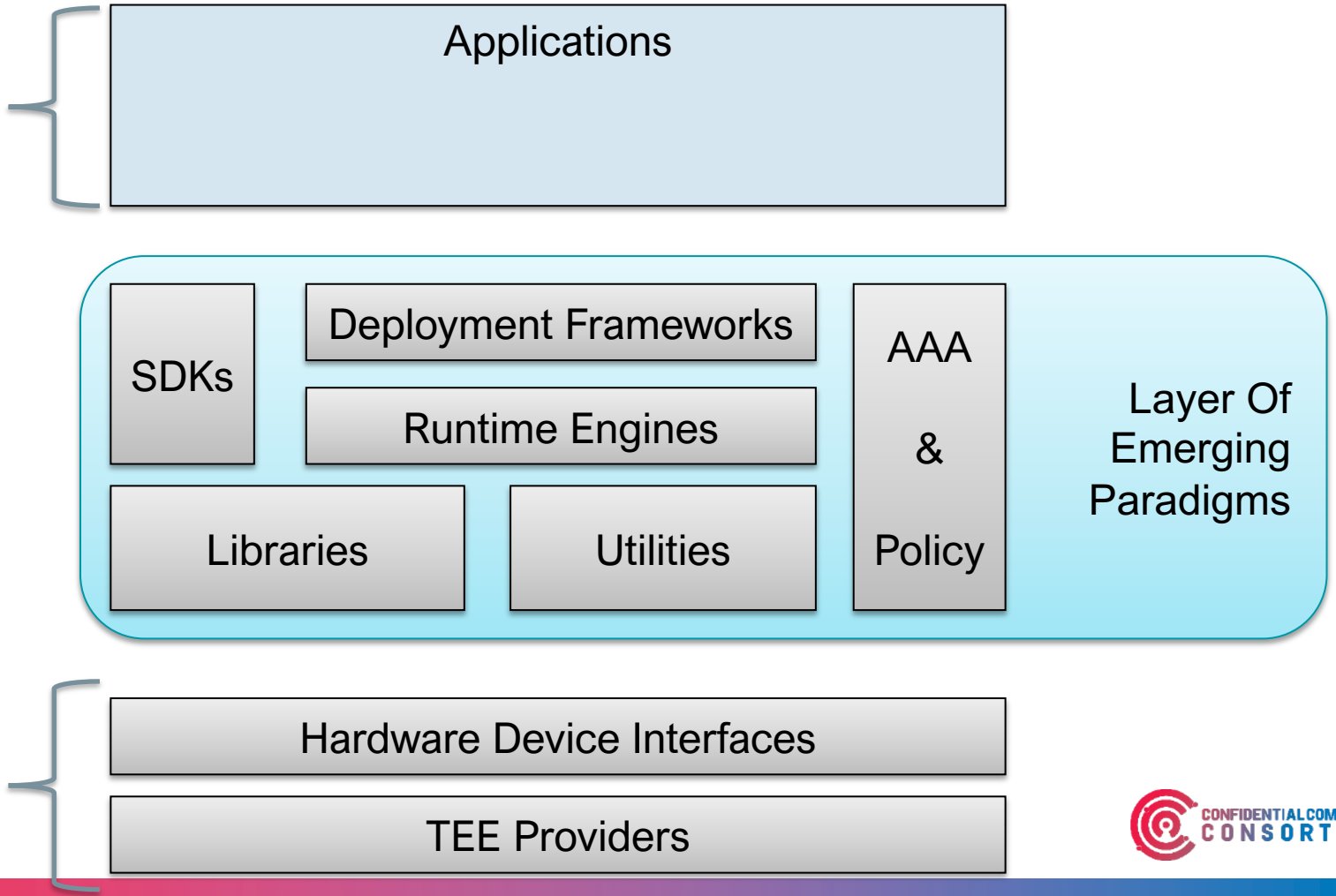
Paradigm #2: App Deployment

Current Projects	
Enarx	Open Enclave SDK

Projects Joining Soon	
Graphene	Occlum
SGX SDK for Linux	Keystone
Trusted Computing Framework	Veracruz

Applications may simply benefit from protections of Confidential Computing.

Applications may also create novel solutions leveraging unique properties of Confidential Computing.

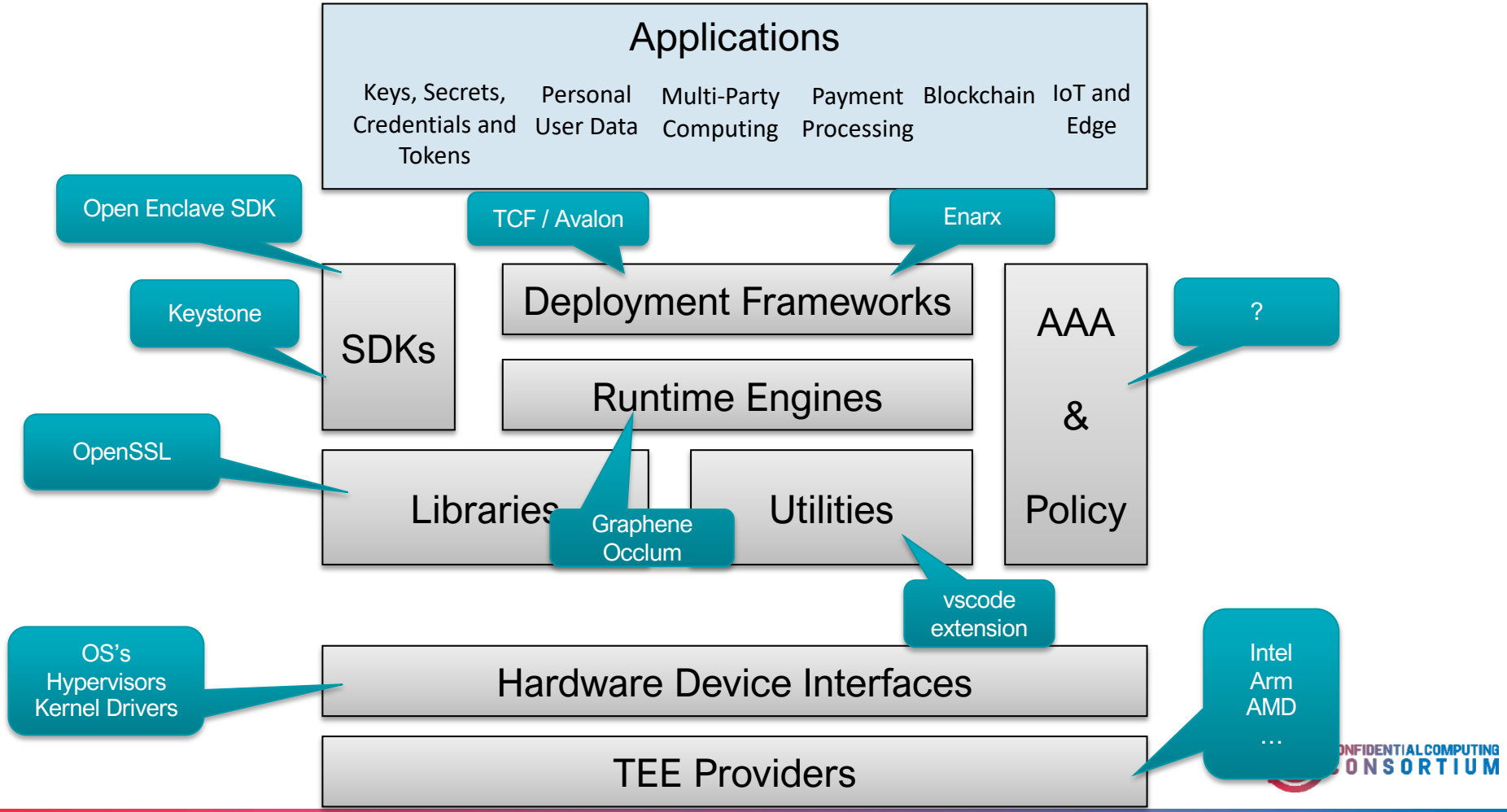


Physical & Virtualized Infrastructure

Hardware & Firmware

OS's & Hypervisors

CONFIDENTIAL COMPUTING CONSORTIUM


Applications
Keys, Secrets, Credentials and Tokens
Personal User Data
Multi-Party Computing
Payment Processing
Blockchain
IoT and Edge
Open Enclave SDK
TCF / Avalon
Enarx
Keystone
SDKs
Deployment Frameworks
AAA & Policy
?
Runtime Engines
OpenSSL
Libraries
Graphene Occlum
Utilities
vscode extension
OS's Hypervisors Kernel Drivers
Hardware Device Interfaces
Intel Arm AMD …
TEE Providers

Questions & Answer

Read the whitepapers
confidentialcomputing.io/whitepapers

Sign up to receive updates
confidentialcomputing.io/news

@ConfidentialC2

confidential-computing

confidentialcomputing.io