Co-funded by the European Union

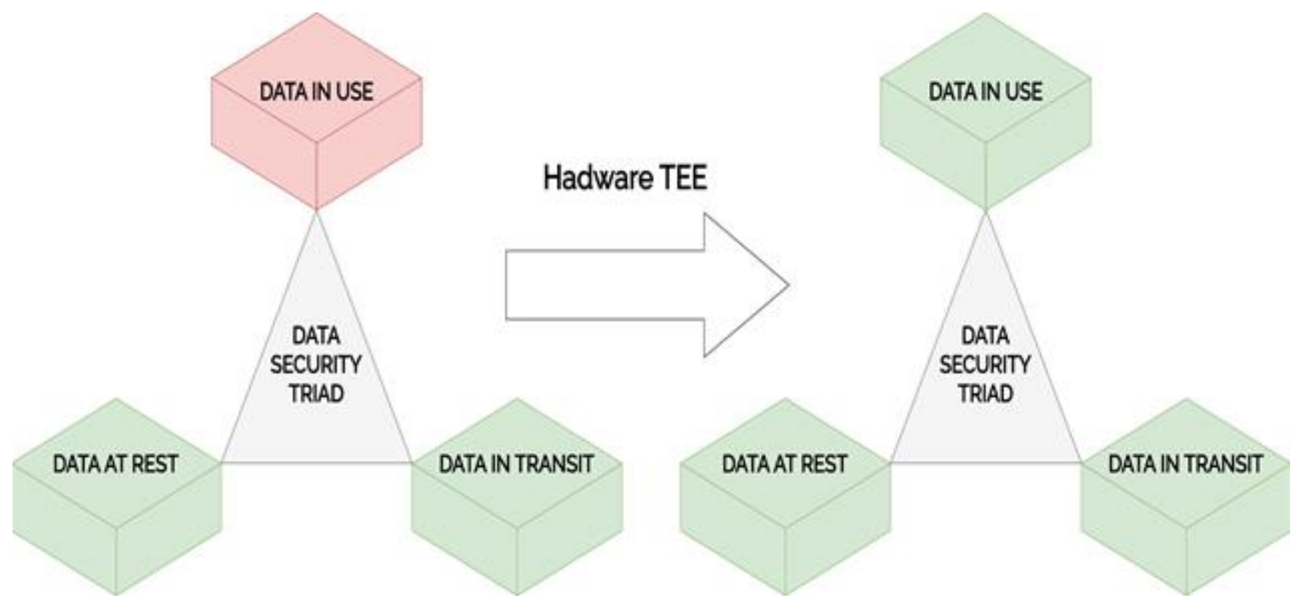
Horizon-JU-SNS-2022
Grant Agreement No. 101096435

CONFIDENTIAL6G

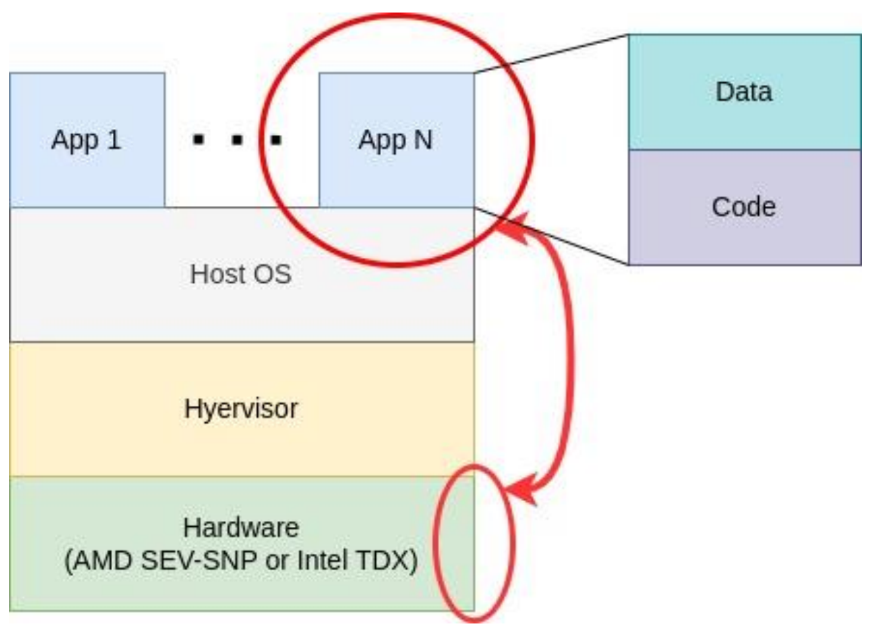
Confidential Computing and Privacy-preserving Technologies for 6G

Privacy-preserving confidential computing platform

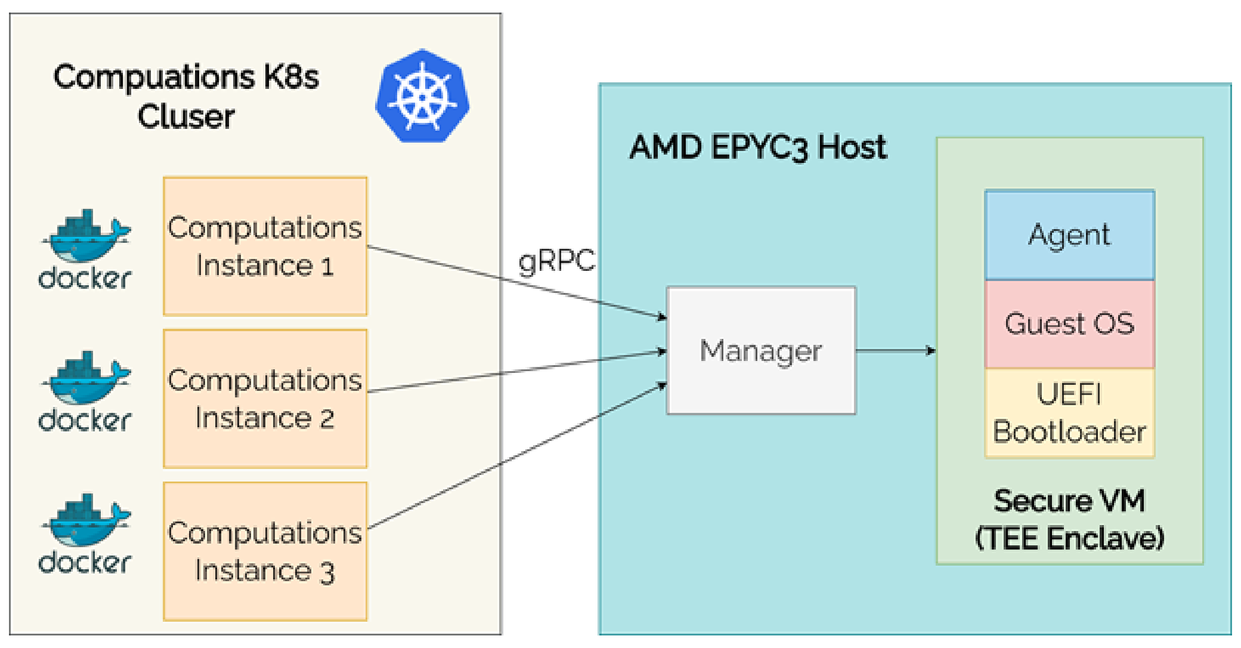
- Confidential Computing System (CoCoS) is a platform for defining and executing confidential workloads, especially in the context of data sharing and collaborative multiparty computation.
  - Protecting data “in use” using hardware Trusted Execution Environments (TEEs) or Enclaves
  - Linux-based HAL (kernel + bootloader + rootfs), low TCB and attestation with cryptographic signatures
  - Software Manager for Enclave deployment and monitoring
  - In-enclave Agent for secure networking and computation execution with remote attestation protocol support
  - User CLI for communication with the Agent
  - User roles for collaborative computation such as data provider, algorithm provider and result consumer
  - Computation service for users to form organizations
- Demo:
  - Collaborative AI with CoCoS
  - Covid19 datasets with an AI algorithm that runs in



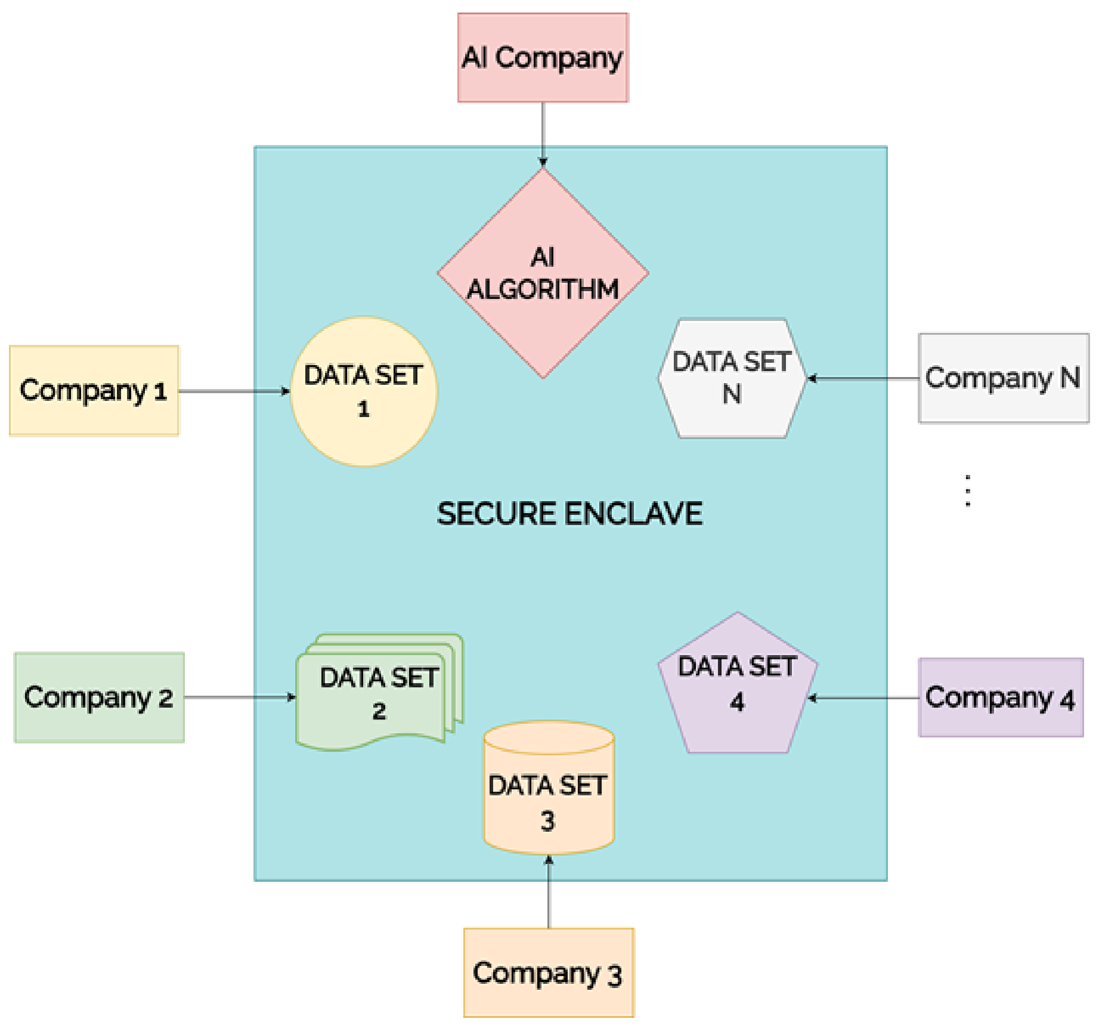
Data security triad with enabled TEEs



Enclaves are baremetal (they override host OS)



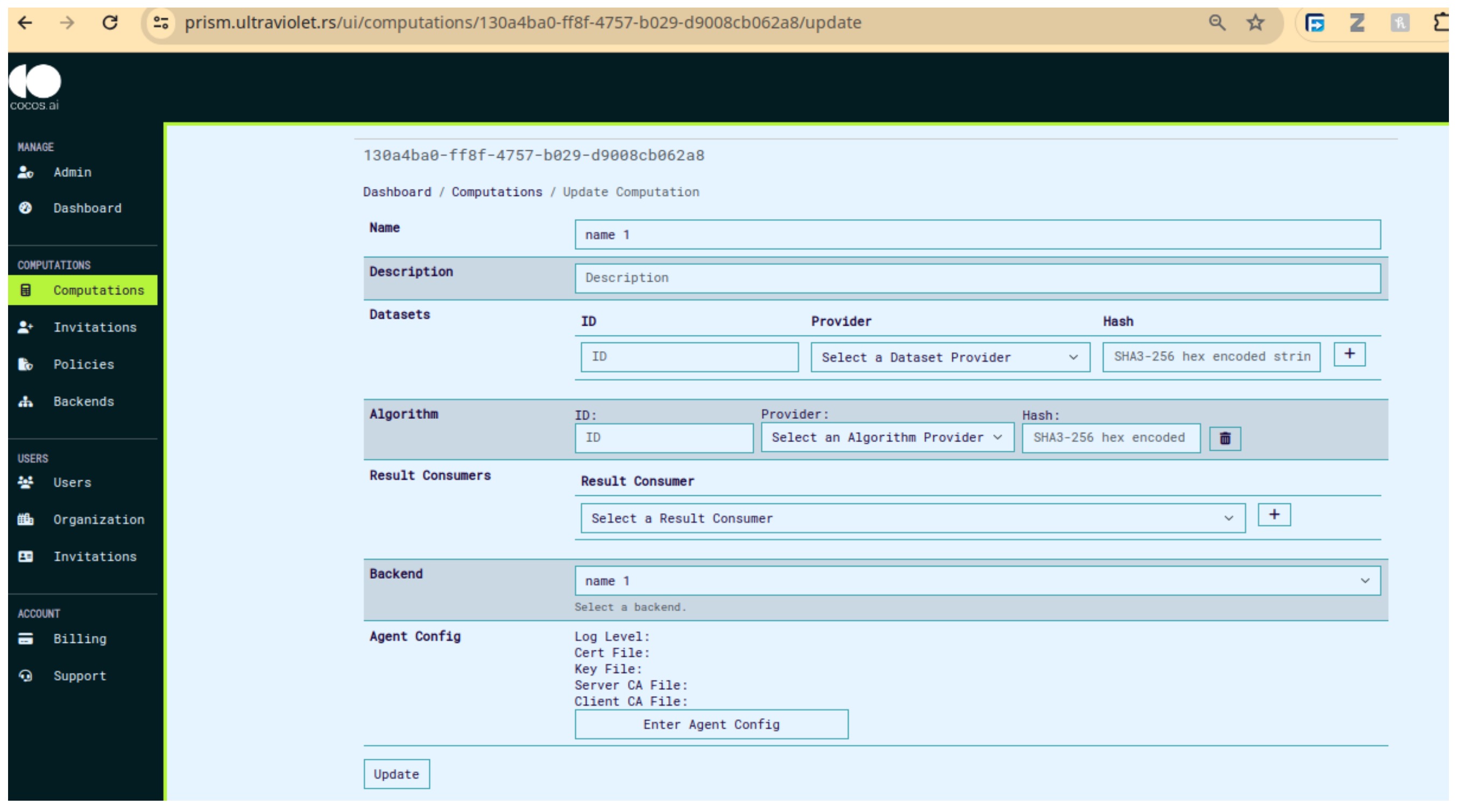
Manager with computation service



Collaborative AI

Technical approach - CoCoS with AMD SEV-SNP

- Goals:
  - Provide demonstration of secure execution for multiple users on AMD SEV-SNP enabled hardware
  - Bring up a secure VM using AMD SEV-SNP enabled hardware
  - Establish a secure networking channel with in-enclave Agent for secure transport of data and algorithm files
  - Test the obtained results from the computation
- Flow:
  - Users define the computation using the computation management service
  - The Manager receives the configuration files (computation manifest) and TLS certificates from the computation management service
  - The Manager launches the Confidential VM (CVM) and forwards the configuration and certificates to the Agent
  - CVM is a small Enclave OS completely in RAM thus ensuring that once the VM shuts down all the data inside the VM is deleted/gone
  - Users use CLI to verify and validate the CVM by validating and verifying the attestation report of the CVM sa part of the remote attestation process
- Remote attestation is a process in which one side (the CVM) collects information about itself and sends that information to the client (user) so that the user can verify and validate the CVM. The successful verification proves to the user that the CVM runs the expected code on the expected hardware and is configured correctly.



130a4ba0-ff8f-4757-b029-d9008cb062a8

Dashboard / Computations / Update Computation

Name: name 1

Description: Description

Datasets: ID: ID | Provider: Select a Dataset Provider | Hash: SHA3-256 hex encoded strin | +

Algorithm: ID: ID | Provider: Select an Algorithm Provider | Hash: SHA3-256 hex encoded

Result Consumers: Result Consumer: Select a Result Consumer | +

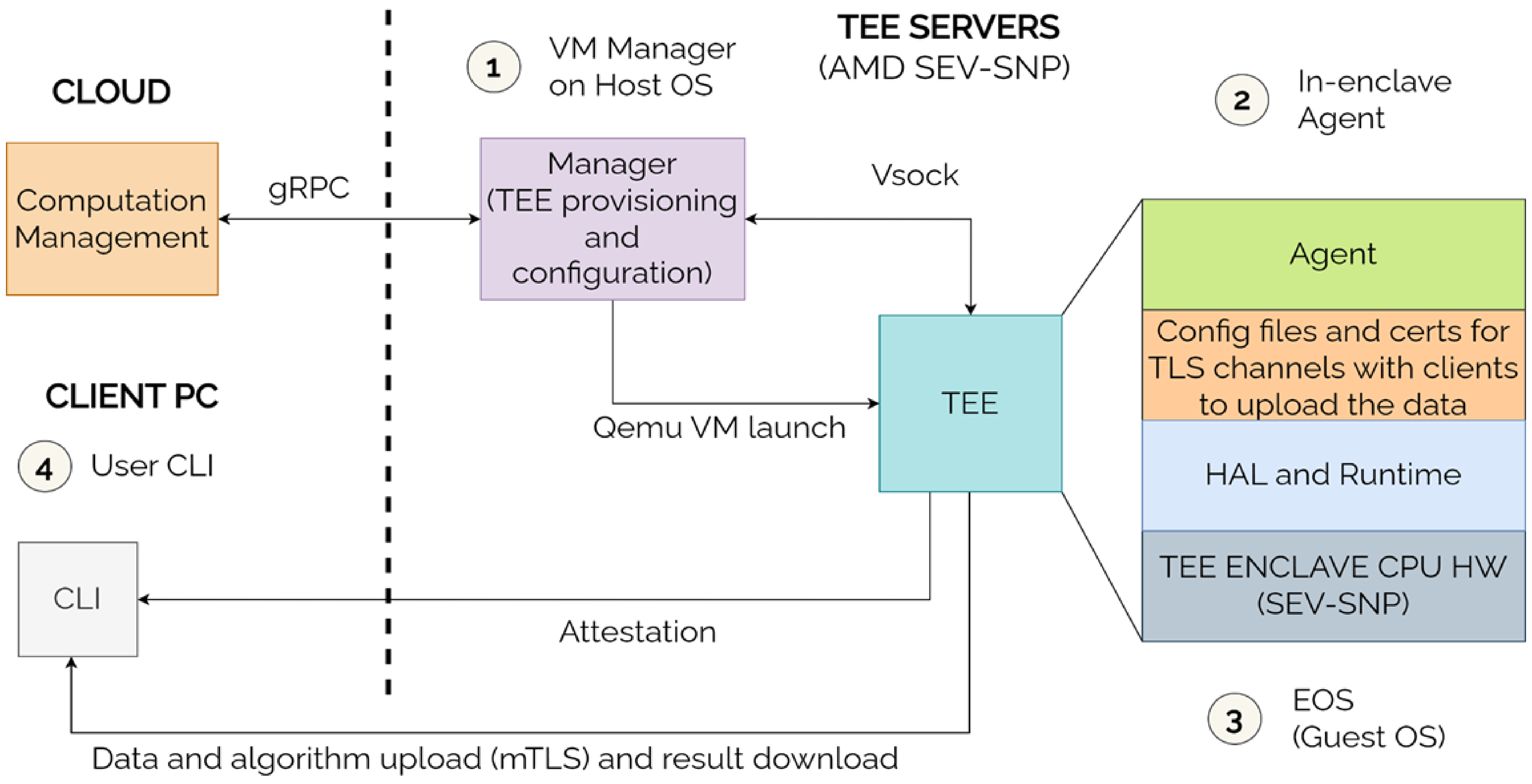
Backend: name 1
Select a backend.

Agent Config:
Log Level:
Cert File:
Key File:
Server CA File:
Client CA File:
Enter Agent Config

Update

Cloud UI

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.


CLOUD
Computation Management
gRPC
1 VM Manager on Host OS
Manager (TEE provisioning and configuration)
TEE SERVERS (AMD SEV-SNP)
Vsock
2 In-enclave Agent
Agent
Config files and certs for TLS channels with clients to upload the data
HAL and Runtime
TEE ENCLAVE CPU HW (SEV-SNP)
TEE
Qemu VM launch
CLIENT PC
4 User CLI
CLI
Attestation
3 EOS (Guest OS)
Data and algorithm upload (mTLS) and result download

Computation flow

@ C6G_eu @c6g-project https://confidential6g.eu