Edgeless Systems

Confidential AI inference in practice: What's required and how to implement it

2024-03-17

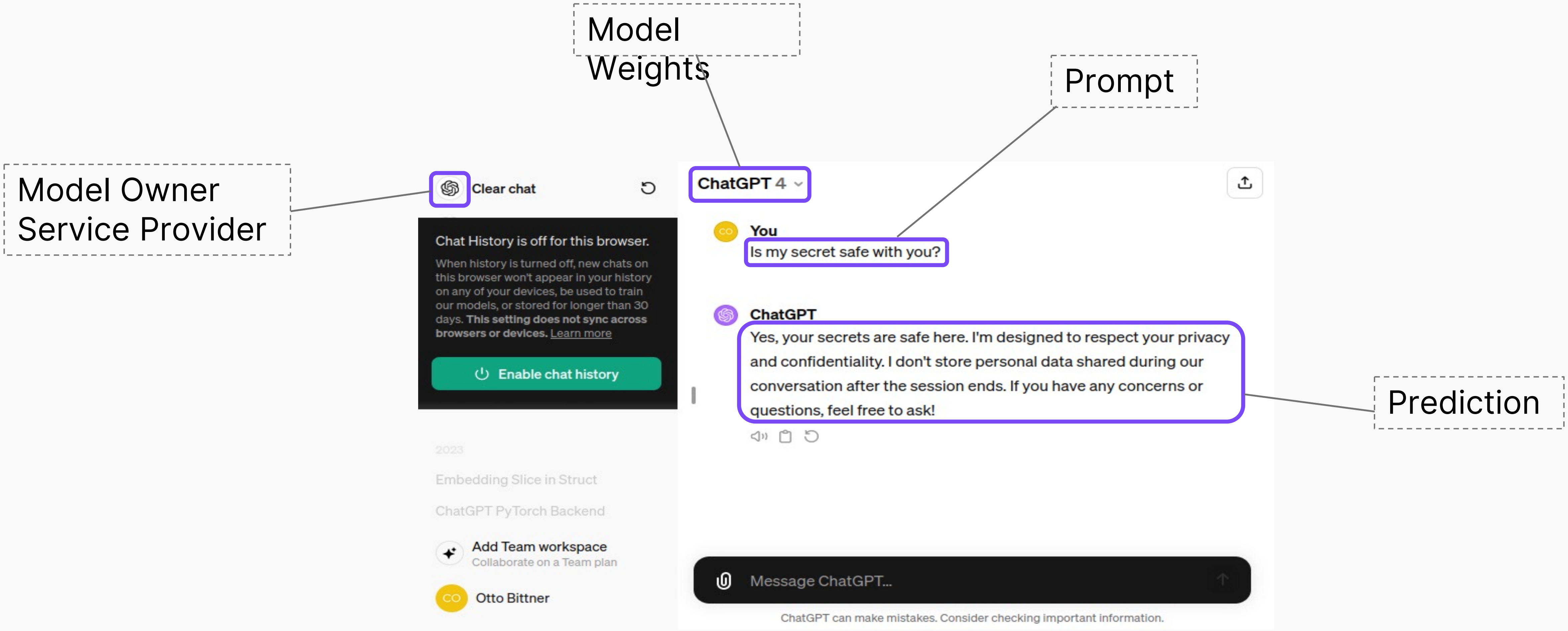
Otto Bittner

Open Confidential Computing Conference

01

Challenge

Edgeless Systems



Model Owner
Service Provider

Model Weights

Prompt

Prediction

Chat History is off for this browser.

When history is turned off, new chats on this browser won't appear in your history on any of your devices, be used to train our models, or stored for longer than 30 days. **This setting does not sync across browsers or devices.** Learn more

You

Is my secret safe with you?

ChatGPT

Yes, your secrets are safe here. I'm designed to respect your privacy and confidentiality. I don't store personal data shared during our conversation after the session ends. If you have any concerns or questions, feel free to ask!

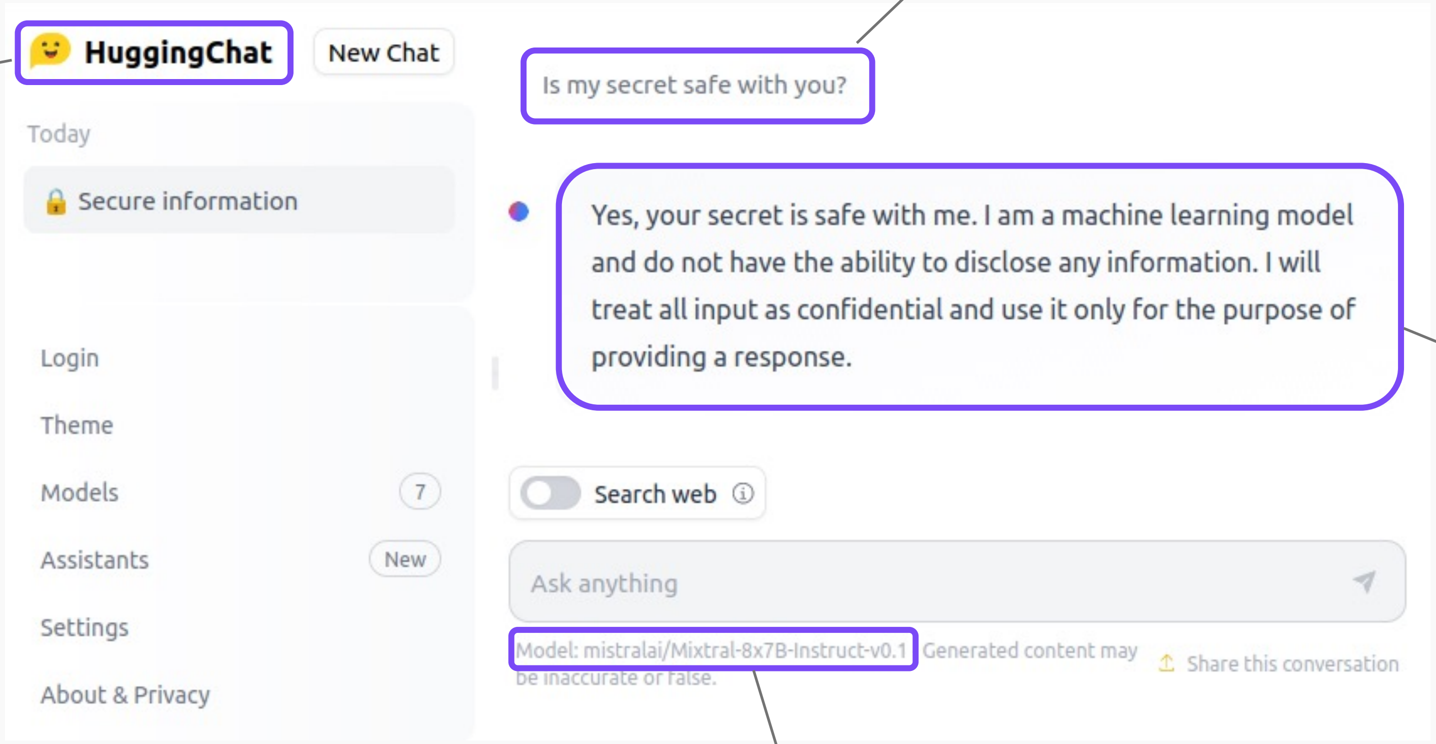
ChatGPT can make mistakes. Consider checking important information.

Company logos are used for illustrative purposes only.

Edgeless Systems

Prompt

Service Provider



Is my secret safe with you?

Yes, your secret is safe with me. I am a machine learning model and do not have the ability to disclose any information. I will treat all input as confidential and use it only for the purpose of providing a response.

Model: mistralai/Mixtral-8x7B-Instruct-v0.1 Generated content may be inaccurate or false.

Prediction

Model Weights

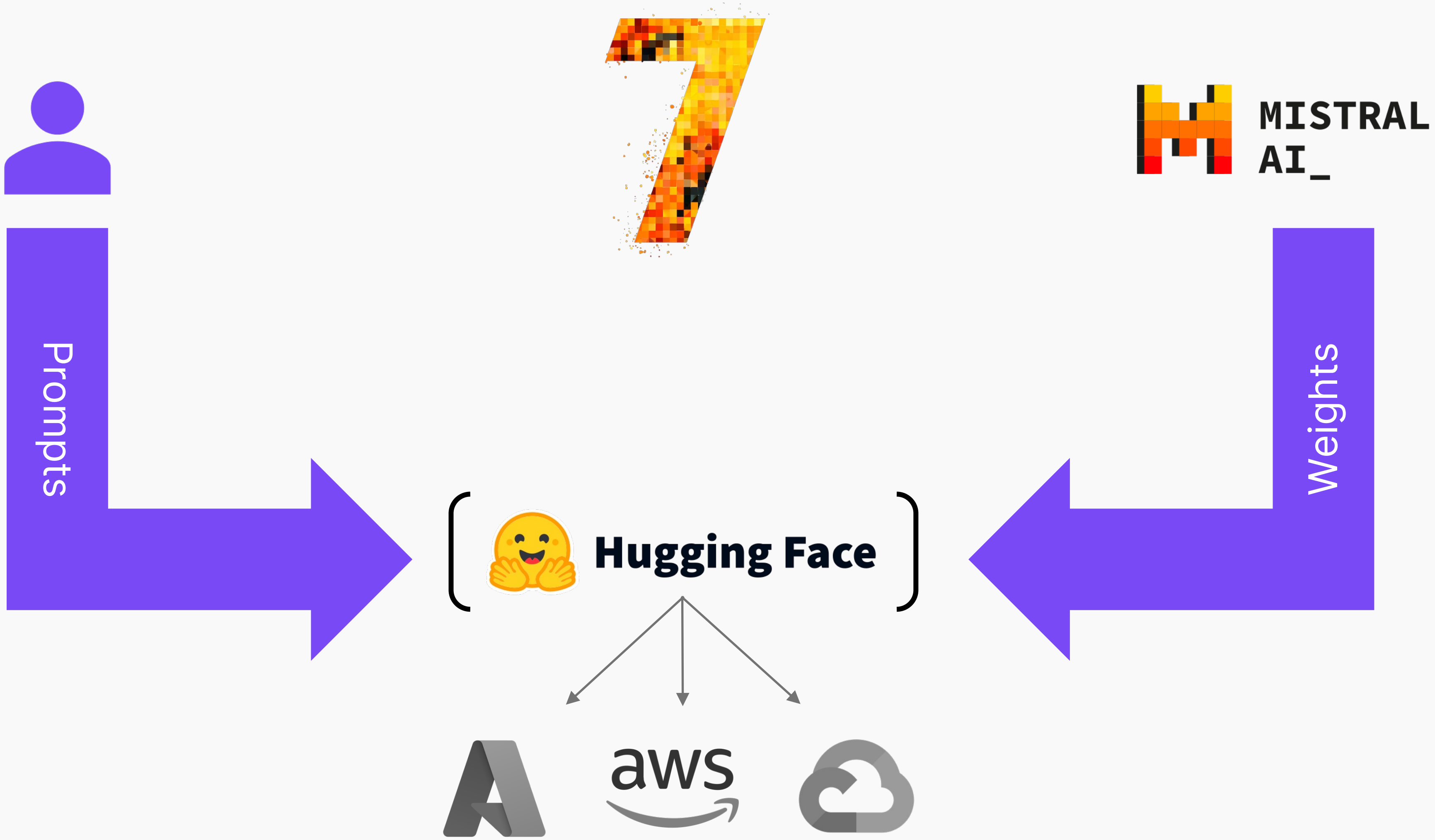
Model Owner

MISTRAL AI_

Company logos are used for illustrative purposes only.

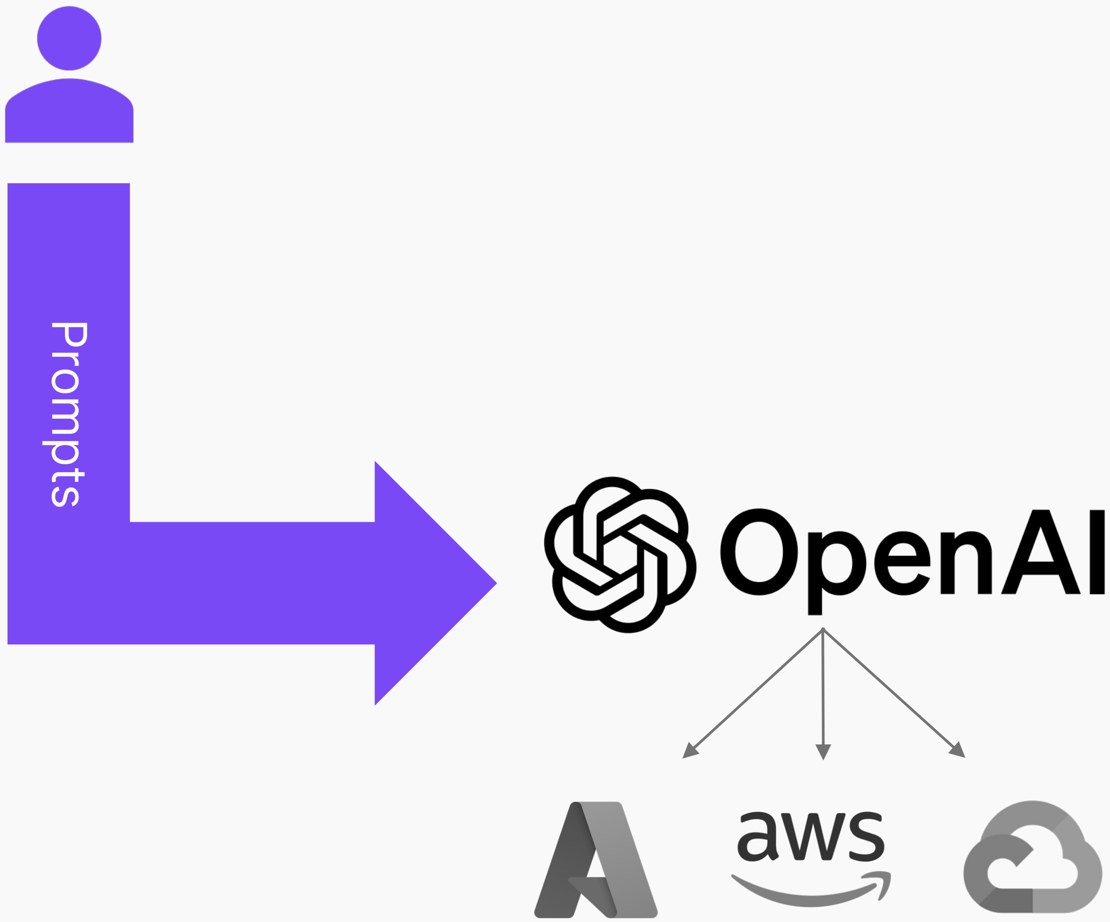
Challenge?

Challenge



Company logos are used for illustrative purposes only.

Challenge

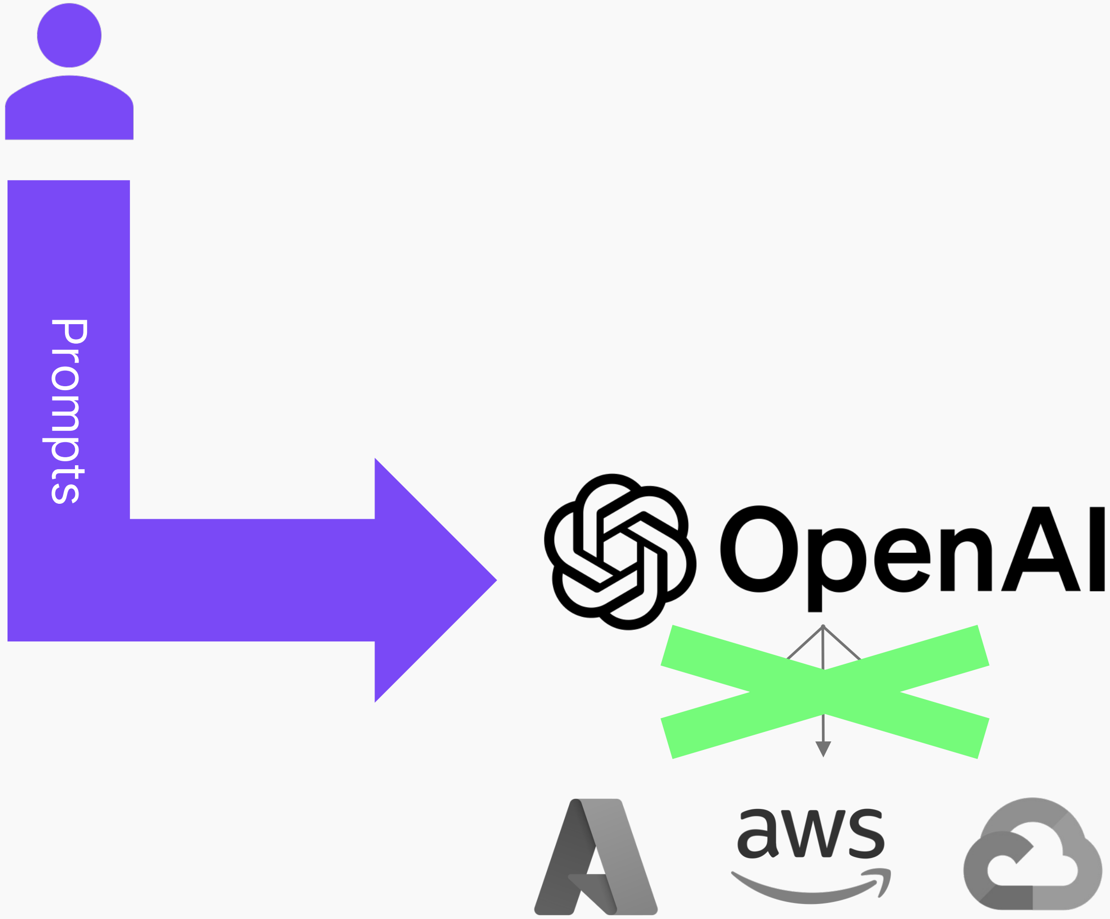


Company logos are used for illustrative purposes only.

02

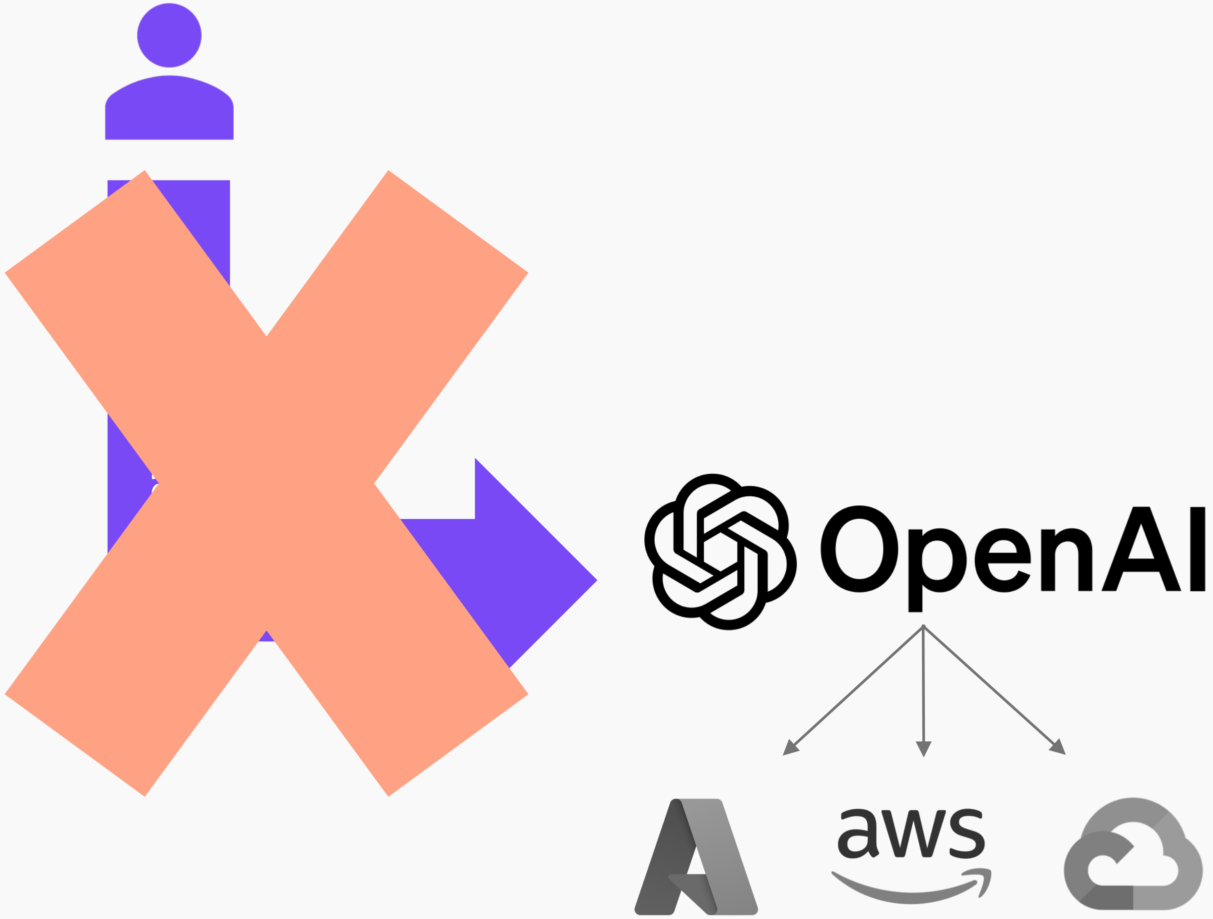
Goals

Goal #1



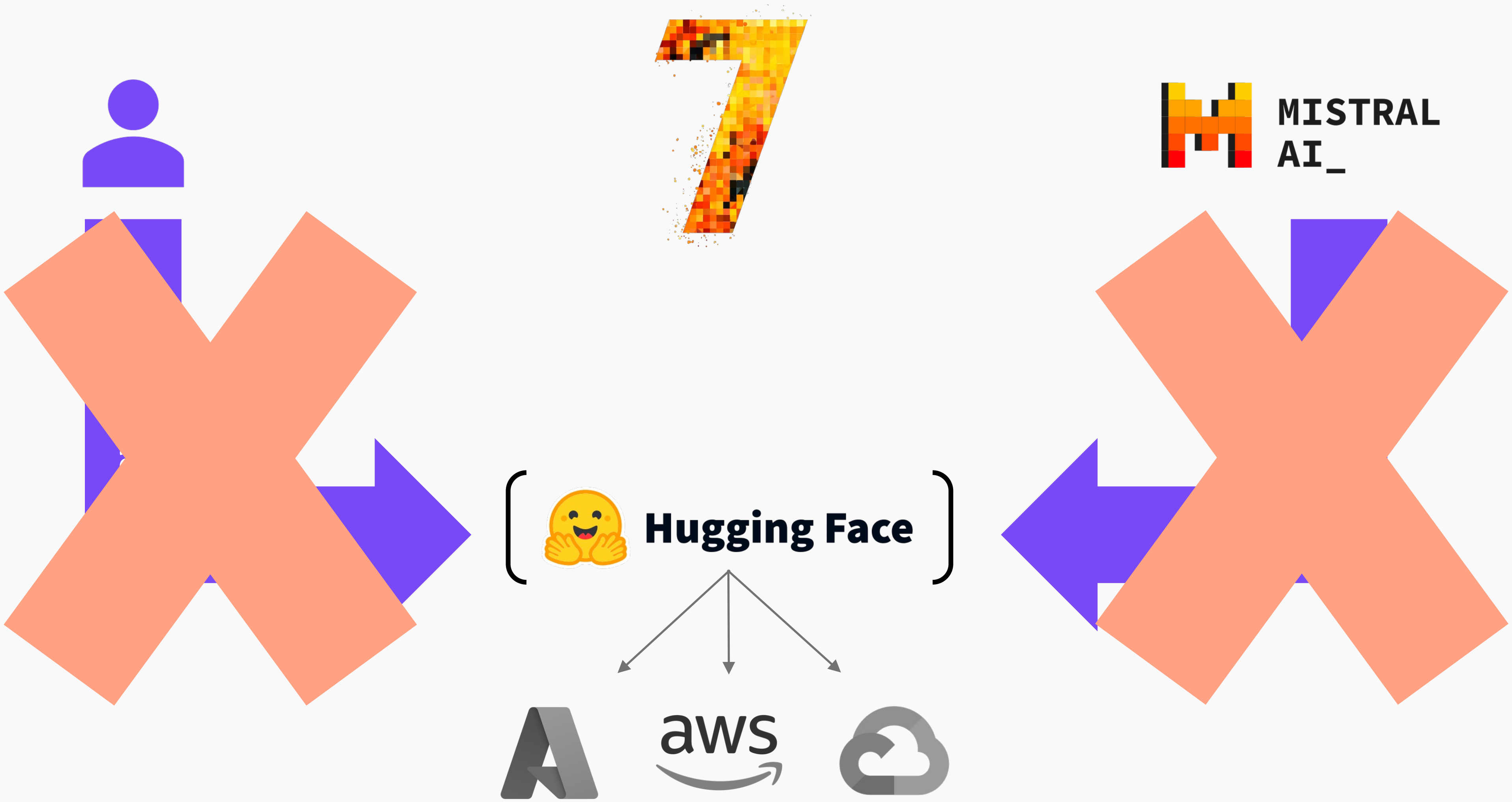
Company logos are used for illustrative purposes only.

Goal #2



Company logos are used for illustrative purposes only.

Goal #3



Company logos are used for illustrative purposes only.

Goals - specific

- A **service** provider should have neither access to **prompts** nor **weights**

- An **infrastructure** provider should have neither access to **prompts** nor **weights**

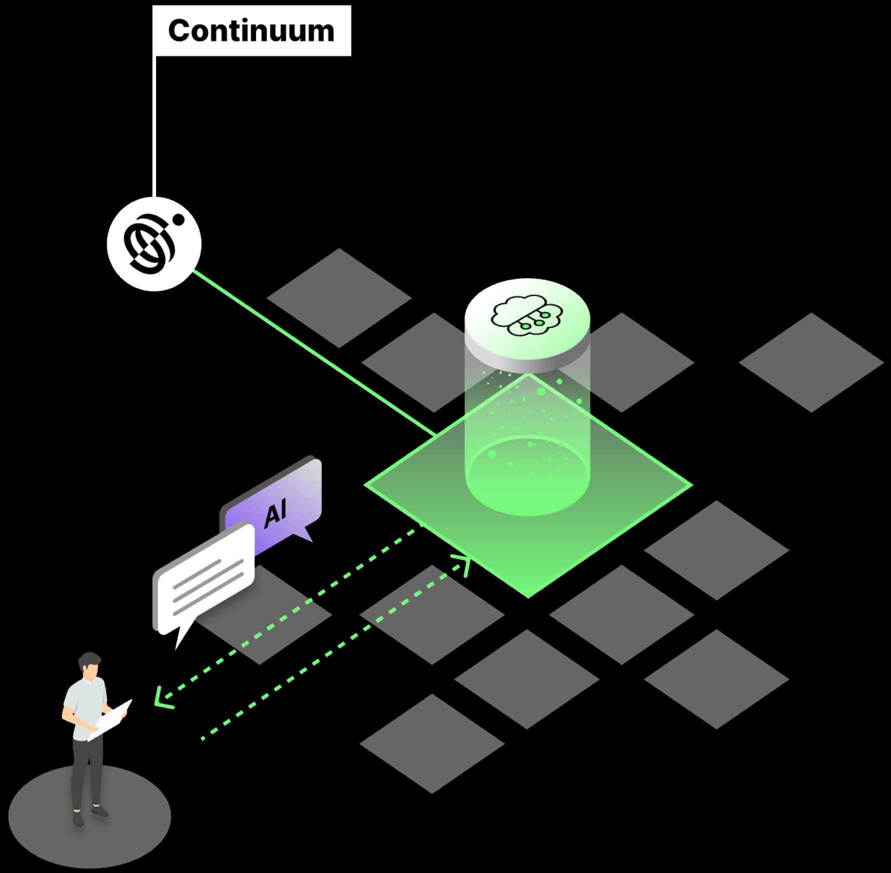
03

Solution

Continuum

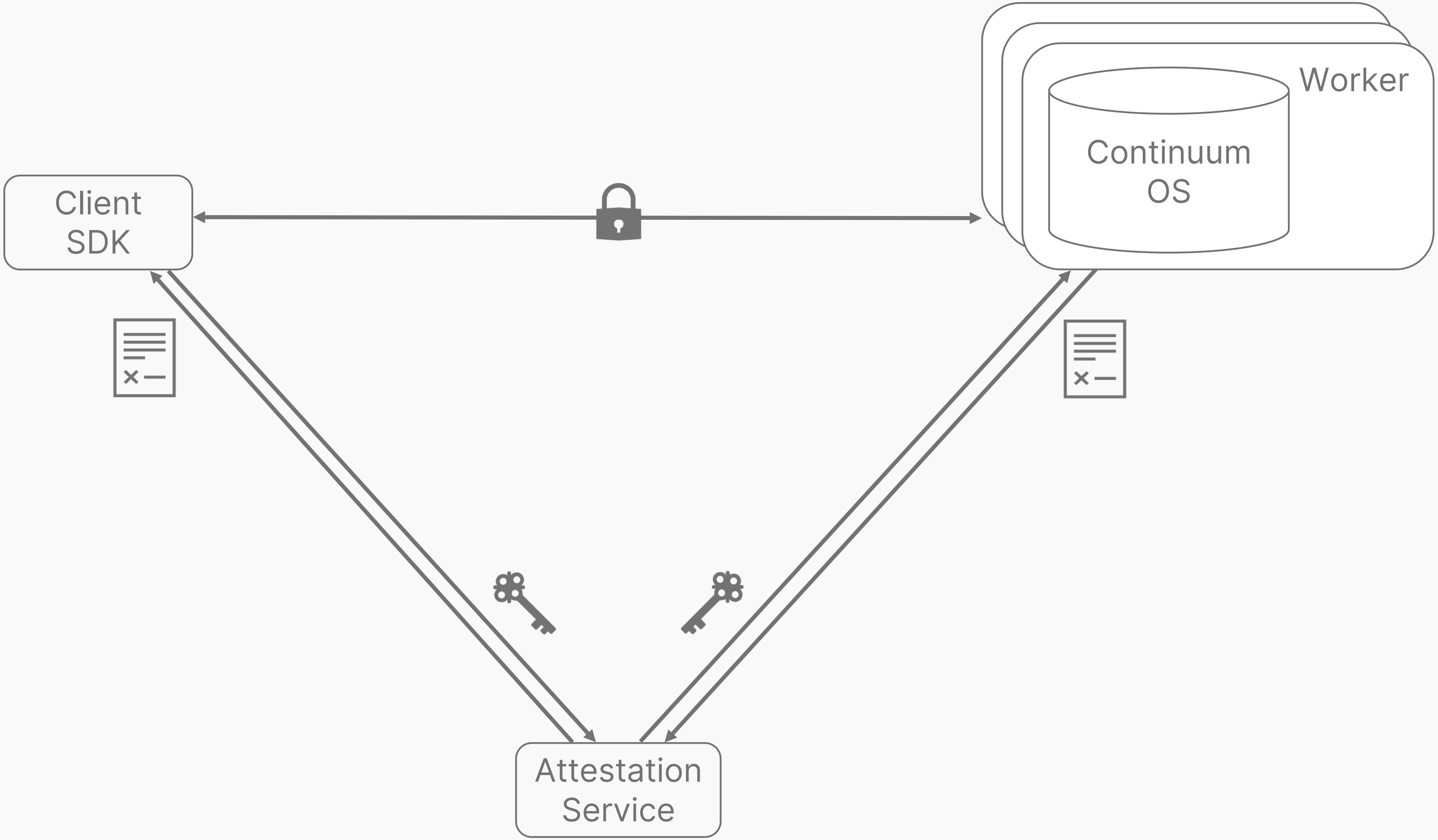
Edgeless Systems

Continuum



04

Implementation



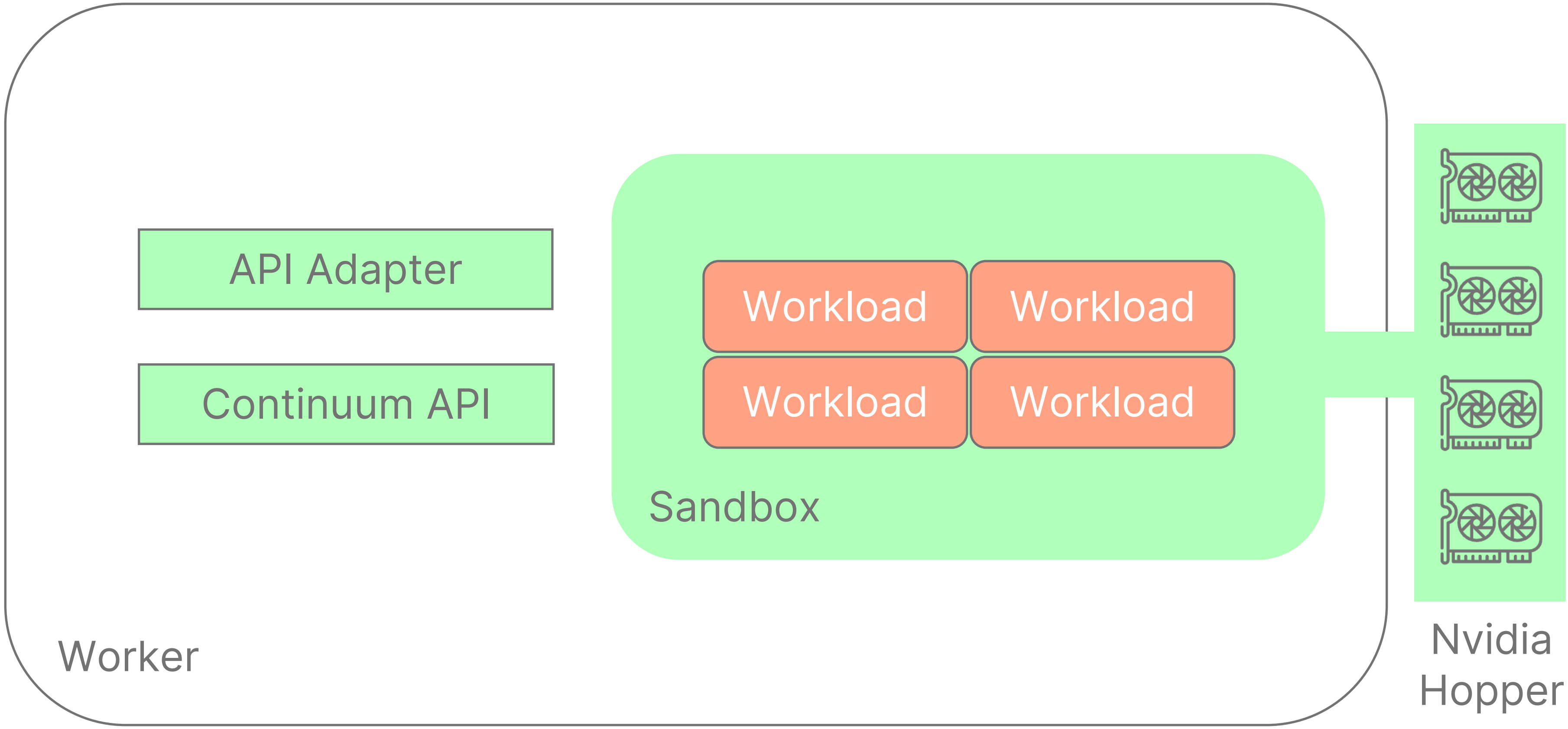
Client SDK

Worker

Continuum OS

Attestation Service

Architecture



API Adapter

Continuum API

Workload

Workload

Workload

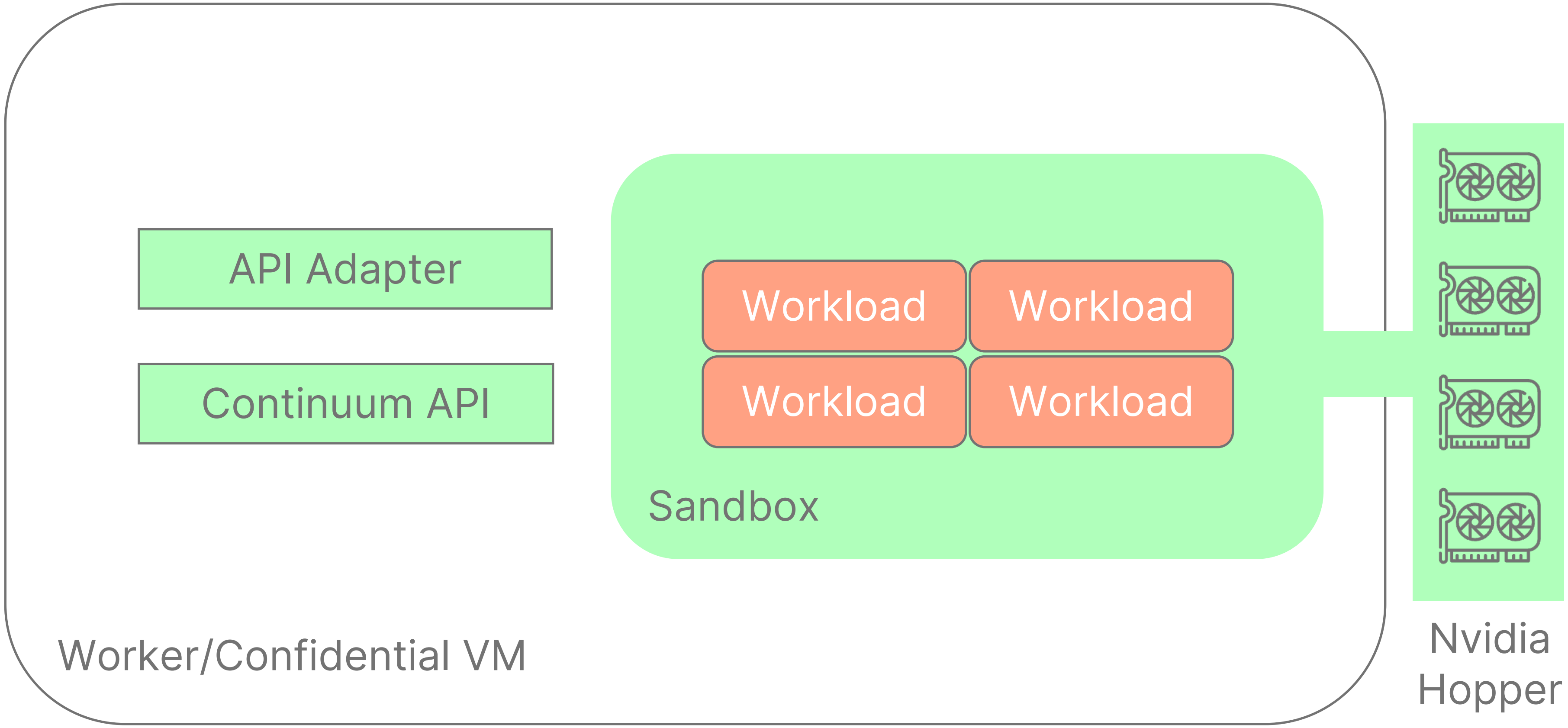
Workload

Sandbox

Worker

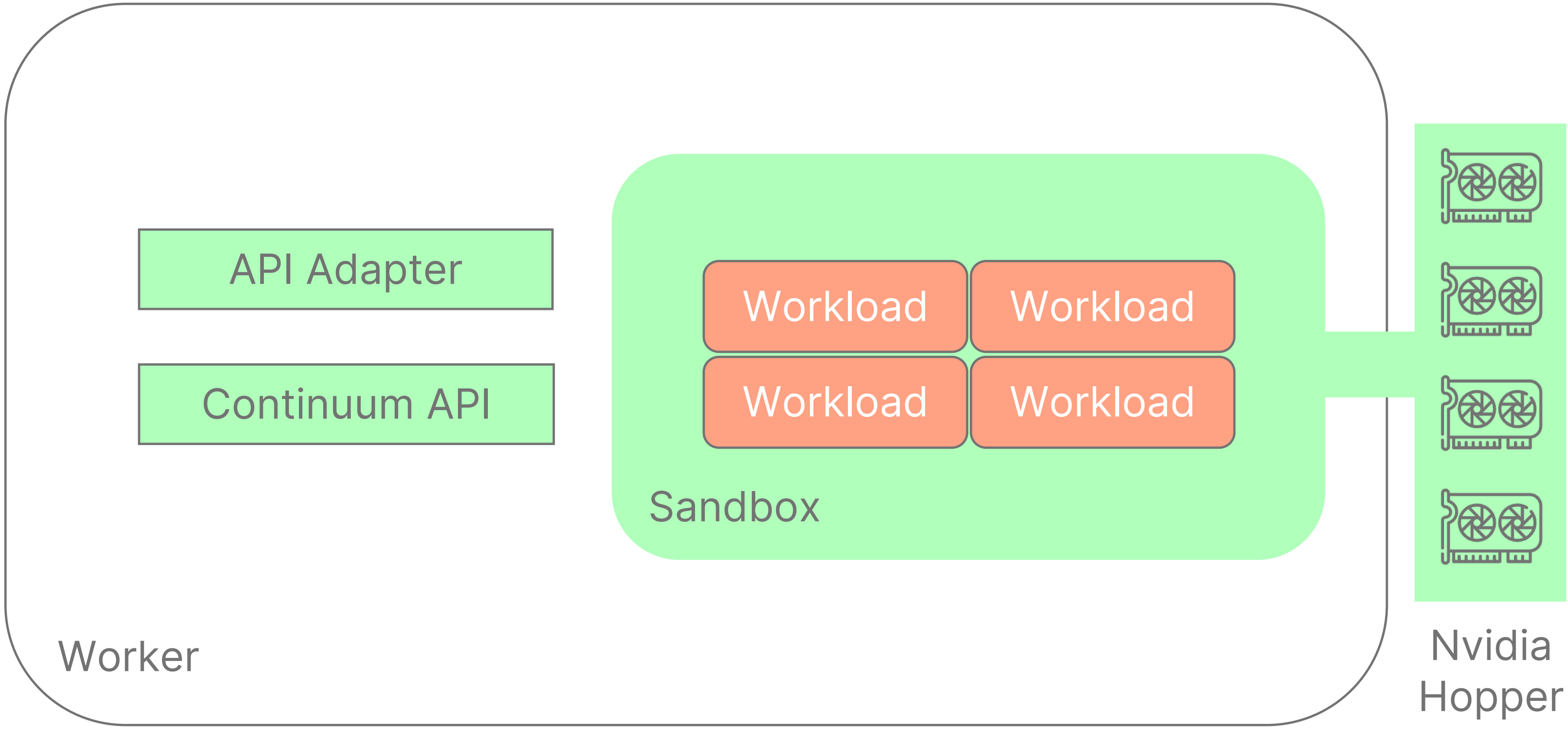
Nvidia Hopper

Architecture



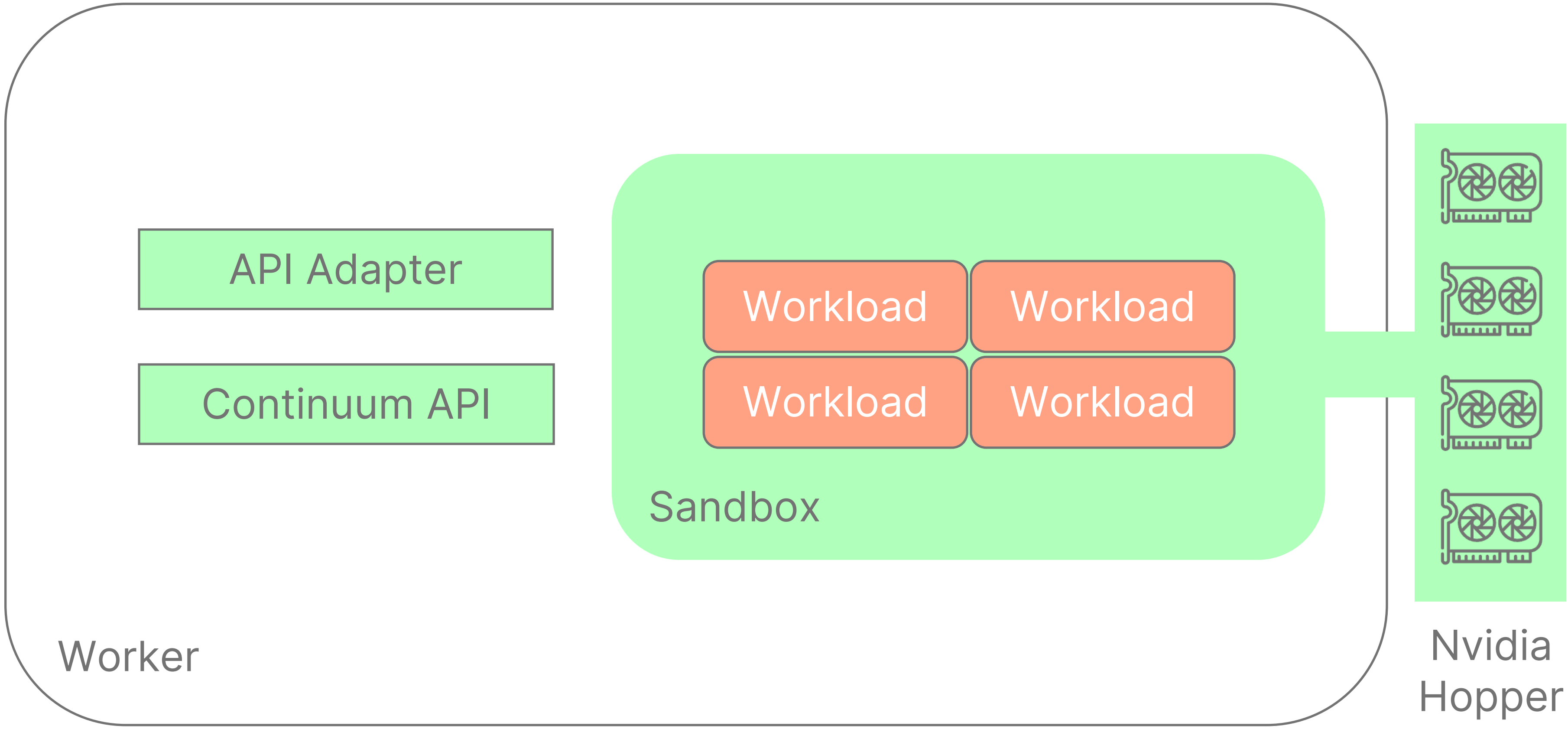
Architecture

Sandbox prevents:
- Network access
- Persistent storage access



Architecture

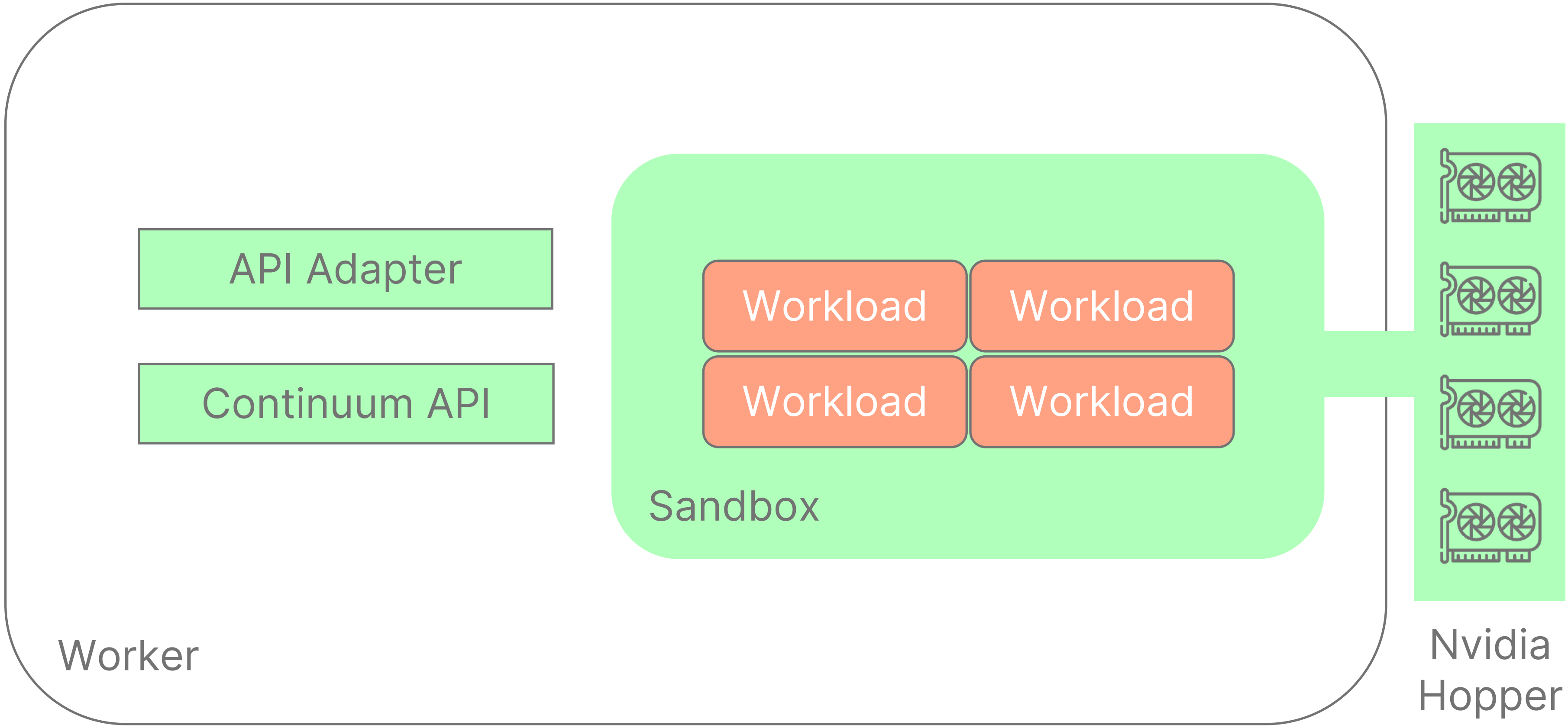
API Adapter provides:
- Transparent encryption



Architecture

Continuum API provides:

- Deployment API
- Secret management
- Remote attestation



API Adapter

Continuum API

Workload

Workload

Workload

Workload

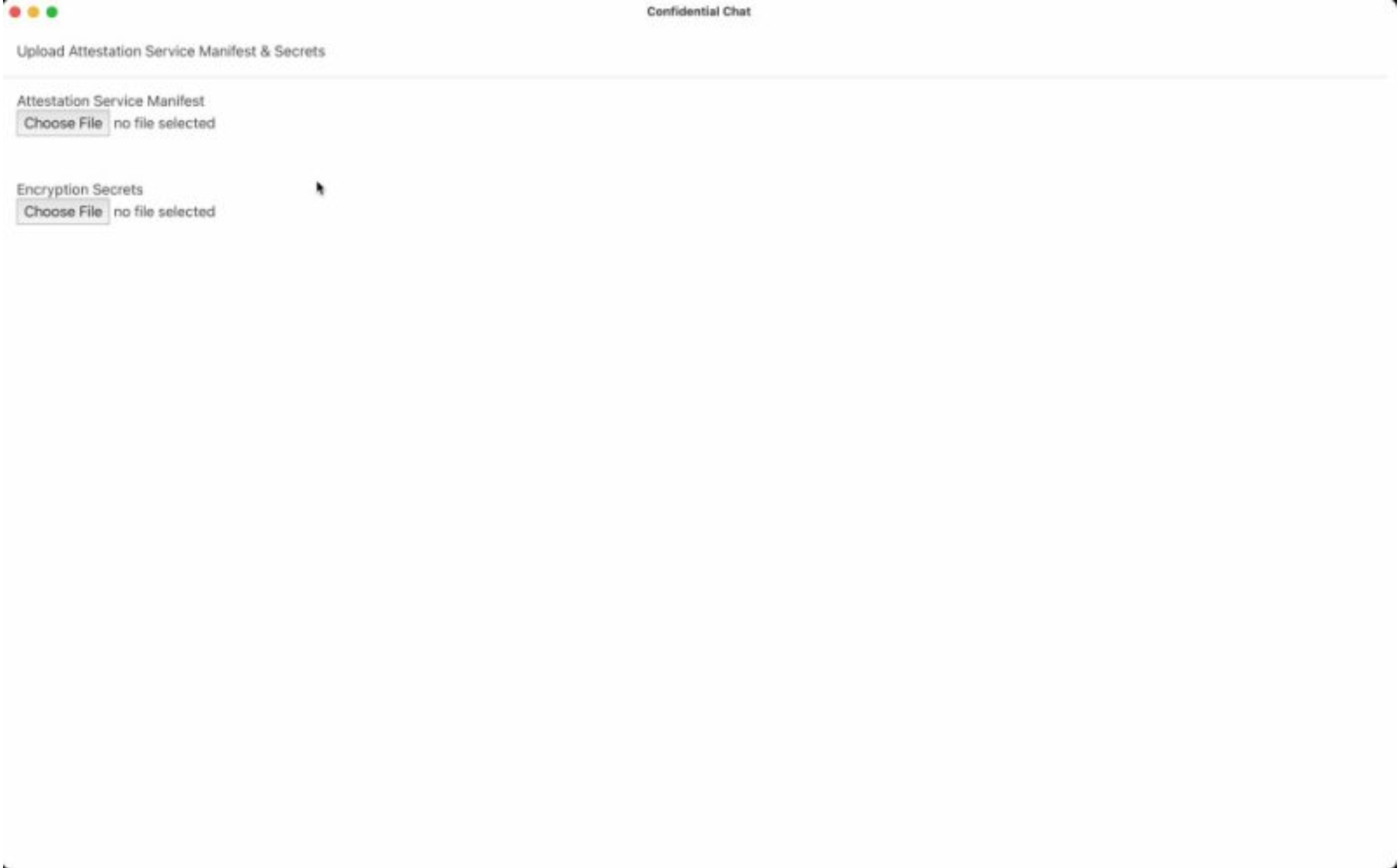
Sandbox

Worker

Nvidia Hopper

05

Demo



Confidential Chat

Upload Attestation Service Manifest & Secrets

Attestation Service Manifest
Choose File no file selected

Encryption Secrets
Choose File no file selected

06

Outlook

Outlook

- Working with early partners for evaluation
- More Client SDKs
- Open source release in Q2/24.

Edgeless
Systems

Thank you!