Verify Attestation

Galadriel Verified Inference API provides LLM inferences results that are signed by the TEE private key and attested by AWS enclave. This page gives overview on how to verify the attestation.

Please see the quickstart to get an LLM inference response. Please see the verify-signatures to see how to verify the signature 1 Get the LLM inference response as in quickstart

This is an example response with some information redacted:

{ "id" : "chatcmpl-AgAQhAGTZKog9p0wPC7aVOXT44046" , "choices" : [{ "finish_reason" : "stop" , "index" : 0 , "logprobs" : null , "message" : { "content" : "Hello! How can I assist you today?" , "refusal" : null , "role" : "assistant" , "function_call" : null , "tool_calls" : null , "audio" : null } }] , "hash" : "fa1eb8b9c330cf13f3643d46bc7e10510fa207a4e80645c795f82c3ddf9806ad" , "public_key" : "Dp2k554Ebsij5RjuhjsZujVW2bJnQzfb43VYZSQ4NZo1" , "attestation" : "hEShATgioFkRP6lpbW9kdWxlX2lkeCdpLTAxYWMwZDExNTgyMTE5Yzc5LWVuYzAxOTNkNGY0YTl5MDI5NDNmZGlnZXN0ZlNIQTM4NGl0aW1lc3RhbXBXAbAAAABk98BdQlkcGNyc7AAWDCjV1iARxeB } 2 Clone the TEE repo

git clone git@github.com:galadriel-ai/sentience.git cd sentience/verified-inference/verify 3 Install deps

Optional

python3 -m venv venv source venv/bin/activate pipinstall -r requirements.txt 4 Verify attestation

Take the attestation from the LLM inference response

python verify.py --pcr0_hash a3575880471781514c83935ee77dd8fc710512daf5d306ccee2c2abb0985e35fea0843f0e950a74f8d17541fc66dd0e4 --attestation insert-your-attestation 5 See more information in the TEE repo