How TEE works

TEE (Trusted Execution Enclave) proves that a given code is running as expected

The whole source code is availablehere

1 Code gets packed into TEE

The Sentience enclavecode is first packaged into a Docker image, which is then packaged into an enclave image. This is a deterministic process: the resultingenclave image hash verifies that the code running inside the TEE (Trusted Execution Environment) is indeed the original code.

To confirm which code is running in the TEE, take the source code and generate a new enclave image. If you end up with the sameenclave image hash , you have verified that it matches the code currently running inside the TEE. 2 TEE starts

Upon TEE startup, a private key is generated. Since no one can access the internal components of the TEE, any data signed with this key can be trusted as authentic. 3 AWS signs the attestation

AWS signs the resulting enclave image hash alongside the generated public key inside the TEE. This signature provides a final guarantee that the code is running exactly as intended, without any intermediaries.

You can read more about Nitro Enclaveshere 4 LLM Proofs

Each LLM inference request to the Galadriel Verified API is processed in the enclave. After the LLM generates a response, both the request and the response are hashed using SHA256. This hash is provided in the LLM response under thehash field.

The hash is then signed with the TEE's private key, producing thesignature field.

Finally, the Galadriel API includes the fullattestation andpublic_key in the LLM response. With these four pieces of information:hash ,signature ,attestation , andpublic_key you can verify that an LLM inference genuinely took place inside the enclave.

What's next?

- To see more details about the API check out the fullAPI docs
- To see how to verify the signaturesVerify Signatures
- To see how to verify the attestationVerify Attestation