How Secret Network Uses SGX

Secret Network leverages TEE technology to do computation with encrypted input, output, and state. The consensus and computation layer of the Secret Network is combined; every validator uses an Intel SGX CPU and processes every transaction.

Private metadata used in Secret Contracts is encrypted before sent to validators for computation. Data is only decrypted inside the TEE of any specific validator, which is inaccessible to them. Computations following the smart contract are done over the decrypted data and the output is encrypted and written to state.

The consensus encryption seed of the network is only stored inside the TEE of each validator node; no entity has access to the encryption keys.

Remote Attestation

Enclaves also go through a detailed registration and attestation process. Specifically, the attestation process which each validator running an SGX enclave must go through ensures the following assertions regarding privacy and correctness:

- The application's identity
- Its intactness (that it has not been tampered with)
- That it is running securely within an enclave on an Intel SGX enabled platform
-

For more detailed information on the Intel SGX remote attestation process you can check out this page:Remote attestation

Key Usage Inside SGX

Enclaves generate and contain their private signing/attestation keys, preventing access from any entity outside of each enclave. All data can only be signed using keys associated with specific instruction sets running in each enclave. For more details on key generation and management within enclaves, see our section aboutencryption .

For our purposes, the attestation key is only used once upon registration. After registration new keys are provisioned to the enclave and used to communicate with the network. This process is described in more detail below.

Last updated1 year ago On this page *Remote Attestation * Key Usage Inside SGX

Was this helpful? Edit on GitHub Export as PDF