Enclave verification

In this section we quickly explain what the verification process for your hardware entails and how it works. Instructions for verification are included in the setup guides!

Terms used:

Attestation Certificate

This is a self-signed X.509 certificate that contains a signed report by Intel, and the SGX enclave. The report contains both a report that the enclave is genuine, a code hash, and a signature of the creator of the enclave.

Seed

this is a parameter that is shared between all enclaves on the network in order to guarantee deterministic calculations. When a node authenticates successfully, the network encrypts the seed and shares it with the node. Protocol internals are describedhere

Background

This section will explain node registration in the Secret Network. If you just care about installation you can just follow the setup guides and ignore this document. If, however, you want to learn more about what's going on behind the scenes here read on.

In order to verify that each node on the Secret Network is running a valid SGX node, we use a process that we call registration. Essentially, it is the process of authenticating with the network.

The process is unique and bound to the node CPU . It needs to be performed for each node, and you cannot migrate registration parameters between nodes. The process essentially creates a binding between the processor and the blockchain node, so that they can work together.

For this reason, the setup will be slightly more complex than what you might be familiar with from other blockchains in the Cosmos ecosystem.

The registration process is made up of three main steps:

1. Enclave verification with Intel Attestation Service - this step creates anattestation certificate
2. that we will use to validate the node
3. On-chain network verification - Broadcast of theattestation certificate
4. to the network. The network will verify that the certificate is signed by Intel, and that the enclave code running is identical to what is currently running on the network. This means that running an enclave that is differs by 1 byte will be impossible.
5. Querying the network for theencrypted seed
6. and starting the node
7.

At the end of this process (if it is successful) the network will output anencrypted seed (unique to this node), which is required for our node to start. After decryption inside the enclave, the result is a seed that is known to all enclaves on the network, and is the source of determinism between all network nodes.

For a deeper dive into the protocol see theprotocol documentation

```

Copy Note: Due to the way rust and C code are compiled recompilation of the enclave code is non deterministic, and will be rejected during the attestation process. This feature is refered to as a reproducable build, and is a feature that will be included in future releases.

```

Registration instructions are included in the Mainnet and Testnet Setup guides!

Last updated5 months ago On this page *Terms used: * Background

Was this helpful? Edit on GitHub Export as PDF