Using EthSigner with HashiCorp Vault

EthSigner supports storing the signing key inHashiCorp Vault .

This example uses a HashiCorp development server without TLS and disables TLS when starting EthSigner. TLS is enabled by default between EthSigner and HashiCorp Vault andmust be configured when not explicitly disabled.

caution We do not recommended disabling TLS in production environments.

Storing private key in HashiCorp Vault

After installingHashiCorp Vault andstarting the server :

1. Set theVAULT_ADDR
2. environment variable using the command displayed after starting the server:
3. export
4. VAULT_ADDR
5. =
6. 'http://127.0.0.1:8200'
7. Save the root token displayed after starting the server in a file calledauthFile
8. .
9. Put your signing key into the HashiCorp Vault:
10. Command
11. Example

vault kv put secret/ethsignerSigningKey value = < Private Key without 0x prefix

vault kv put secret/ethsignerSigningKey value = 8f2a55949038a9610f50fb23b5883af3b4ecb3c3bb792cbcefbd1542c692be63 The private key is stored in the default location for EthSigner. The key must be a base 64 encoded private key for ECDSA for curve secp256k1.

Start Besu

Start Besu with the--rpc-http-port option set to8590 to avoid conflict with the default EthSigner listening port (8545).

besu --network

dev --miner-enabled --miner-coinbase

0xfe3b557e8fb62b89f4916b721be55ceb828dbd73 --rpc-http-cors-origins

"all" --host-allowlist = * --rpc-http-enabled --rpc-http-port = 8590 --data-path = /tmp/tmpDatadir caution EthSigner requires achain ID to be used when signing transactions. The downstream Ethereum client must be operating in a milestone supporting replay protection. That is, the genesis file must include at least the Spurious Dragon milestone (defined aseip158Block in the genesis file) so the blockchain is using a chain ID.

Start EthSigner with HashiCorp Vault signing

Start EthSigner.

ethsigner --chain-id

2018 --downstream-http-port = 8590 hashicorp-signer --host = 127.0 .0.1 --port = 8200 --auth-file = authFile --tls-enabled = false --signing-key-path = /v1/secret/data/ethsignerSigningKey The path to the key in the HashiCorp Vault specified by--signing-key-path is prefixed by the key version and includesdata . For example, if the following command is used put the key into the Vault:vault kv put secret/ethsignerSigningKey value=

The path specified for--signing-key-path is/v1/secret/data/ethsignerSigningKey

tip Use the--http-listen-port option to change the EthSigner listening port if8545 is in use. You can nowuse EthSigner to sign transactions with the key stored in the HashiCorp Vault.Edit this page Last updatedonMar 30, 2023 byEric LinPrevious Using EthSigner with Azure Key Vault Next Using the configuration file