Using EthSigner with Azure Key Vault

EthSigner supports storing the signing key in anAzure Key Vault .

Storing private key in Azure Key Vault

Create a SECP256k1 key in theAzure Key Vault and register EthSigner as an application for the key.

Take note of the following to specify when starting EthSigner:

- Key vault name
- Key name
- Key version
- Client ID
- File containing client secret for the client ID

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 Azure Key Vault signing

Start EthSigner.

ethsigner --chain-id

2018 --downstream-http-port = 8590 azure-signer --client-id = < ClientID

--client-secret-path

mypath/mysecretfile --key-name

< KeyName

--key-version

< KeyVersion

--keyvault-name

< KeyVaultName

Important 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 Azure Key Vault.Edit this page Last updatedonMar 30,

Previous Make transactions Next Using EthSigner with HashiCorp Vault