HashiCorp Vault key pairs

To configure Tessera to use HashiCorp Vaultkey pairs , provide the vault information in theconfiguration file . You can use Tessera togenerate HashiCorp Vault keys .

You can provide additional configuration items if the vault is configured to useTLS , and if the AppRole authentication method is used at a non-default path.

HashiCorp Vault key pair configuration "keys": { "keyVaultConfigs": [{ "keyVaultType": "HASHICORP", "properties": { "url": "https://localhost:8200", "tlsKeyStorePath": "/path/to/keystore.jks", "tlsTrustStorePath": "/path/to/truststore.jks", "approlePath": "not-default" } }], "keyData": [{ "hashicorpVaultSecretEngineName": "engine", "hashicorpVaultSecretName": "secret", "hashicorpVaultSecretVersion": 1, "hashicorpVaultPrivateKeyId": "privateKey", "hashicorpVaultPublicKeyId": "publicKey", }] } This example configuration retrieves version1 of the secretengine/secret from its corresponding values forprivateKey andpublicKey .

If nohashicorpVaultSecretVersion is provided, the latest version of the secret is retrieved.

Tessera requires TLS certificates and keys to be stored in the.jks Java keystore format. If the.jks files are password protected, the following environment variables must be set:

- HASHICORP_CLIENT_KEYSTORE_PWD
- HASHICORP_CLIENT_TRUSTSTORE_PWD

info Additional environment variables must be set and a version 2 Key/Value secrets engine must be enabled. Edit this page Last updatedonOct 9, 2023 bydependabot[bot] Previous AWS Secrets Manager keys Next Secure keys