Secure private keys using Argon2

You can encrypt private keys with a password during key generation.

After generating password-protected keys, you must add the password must to theconfiguration file to ensure it can be decrypted.

You can add passwords inline using"passwords":[] , or store them in an external file referenced by"passwordFile": "Path" .

note The number of arguments/file lines provided must equal the total number of private keys. For example, if there are three total keys and the second is not password secured, the second argument/line must be blank or contain placeholder data. Tessera usesArgon2 to encrypt private keys. By default, Argon2 is configured as follows:

{ "variant": "id", "memory": 1048576, "iterations": 10, "parallelism": 4 } You can change the Argon2 configuration by using the-keygenconfig option. Any override file must have the same format as the default configuration, and all options must be provided.

tessera -keygen -filename /path/to/key1 -keygenconfig /path/to/argonoptions.jsonEdit this page Last updatedonOct 9, 2023 bydependabot[bot] Previous HashiCorp Vault keys Next KeyVault