Multikey parameters

The optional[metadata] section in the TOML files contains data that is not required by EthSigner. The[signing] section contains the parameters required for the signing type.

caution All parameters in the[signing] section are mandatory.

File-based signing

[metadata] createdAt = 1994-11-05T08:15:30-05:00 description = "Example of a File based configuration"

[signing] type = "file-based-signer" key-file = "/Users/me/project/78e6e236592597c09d5c137c2af40aecd42d12a2.key" password-file = "/Users/me/project/78e6e236592597c09d5c137c2af40aecd42d12a2.password" note EthSigner supports absolute paths or relative paths when specifyingkey-file andpassword-file . Relative paths are relative to the directory specified in themultikey-signer --directory subcommand. Key Description type Type of key signing. Usefile-based-signer key-file V3 keystore file containing thekey with which transactions are signed password-file File containing the password for thekey with which transactions are signed.

HashiCorp Vault signing

[metadata] createdAt = 2019-07-01T12:11:30Z description = "Example of a valid HashiCorp based configuration"

[signing] type = "hashicorp-signer" keyPath = "/v1/secret/data/ethsignerKey" keyName = "value" token = "root_token" serverHost = "localhost" serverPort = 8200 timeout = 5000 tlsEnable = true tlsTrustStoreType = "ALLOWLIST" tlsTrustStorePath = "/Users/me/project/knownHashicorpServers" note The value ofkeyPath is dependent on how HashiCorp Vault secret engine is configured. It's usually in the format of/v1//data/ . For example, in HashiCorp Vaultdev mode, a default secret engine with namesecret is created. Creating a pathEthSignerKeys insecret would result in thekeyPath value to be/v1/secret/data/EthSignerKeys . Key Description type Type of key signing. Usehashicorp-signer keyPath Path to secret in the HashiCorp Vault containing the private key for signing transactions. keyName Name of the key that maps to the private key in the secret. Defaults tovalue . token HashiCorp Vault authentication token that is required to access the secret defined by thekeyPath . serverHost Host of the HashiCorp Vault server. serverPort Port of the HashiCorp Vault server. Defaults to8200 . timeout Timeout in milliseconds for requests to the HashiCorp Vault server. Defaults to10000 . tlsEnable Enable/Disable TLS communication with HashiCorp Vault server. Defaults totrue . tlsTrustStoreType The type of Truststore that stores HashiCorp Vault server TLS certificate. Valid values areALLOWLIST ,JKS ,PKCS12 andPEM . Can be omitted if HashiCorp server's CA is already trusted. tlsTrustStorePath Path to the Truststore file. Required whentlsTrustStoreType is specified. See example ofhow to create an ALLOWLIST Truststore file. tlsTrustStorePassword Password to decrypt truststore file. Only required forJKS andPKCS12 truststore types.

Azure Key Vault signing

[metadata] createdAt = 2011-11-01T12:15:30Z description = "Example of an Azure Key Vault based configuration"

[signing] type = "azure-signer" key-vault-name = "AzureKeyVault" key-name = "ethsignerKey" key-version = "7c01fe58d68148bba5824ce418241092" client-id = "47efee5c-8079-4b48-31bb4f2e9a22" client-secret = "TW_3Uc/HLPdpLp5*om@MGcd1T29MuP*5" tenant-id = "34255fb0-379b-4a1a-bd47-d211ab86df81" Key Description type Type of key signing. Useazure-signer key-vault-name Name of the vault to access. Sub-domain ofvault.azure.net key-name Name of key to be used key-version Version of the specified key client-id ID used to authenticate with Azure Key Vault client-secret Secret used to access the vault tenant-id The tenant ID used to authenticate with Azure Key Vault. Edit this page Last updatedonJun 21, 2023 byCahyo ArissabarnoPrevious API methods Next Security disclosure policy