Inline key pairs

You can configure inline key pairs in the configuration file .

Unprotected

"Security warning" Inline unprotected key pairs are not secure because the private key is exposed in the configuration file. Do not use inline unprotected key pairs in production environments. In unprotected inline key pair configuration, provide key pair data in plain text. Provide the plain text private key in a config JSON object.

Unprotected inline key pair configuration "keys": { "keyData": [{ "config": { "data": { "bytes": "yAWAJjwPqUtNVlqGjSrBmr1/iIkghuOh1803Yzx9jLM=" }, "type": "unlocked" }, "publicKey": "/+UuD63zItL1EbjxkKUljMgG8Z1w0AJ8pNOR4iq2yQc=" }] }

Protected

In protected inline key pair configuration, provide the public key in plaintext. The private key must be password-protected using Argon2 . Provide the corresponding encrypted data in a config JSON object.

"keys": { "passwordFile": "/path/to/pwds.txt", "keyData": [{ "config": { "data": { "aopts": { "variant": "id", "memory": 1048576, "iterations": 10, "parallelism": 4, }, "snonce": "x3HUNXH6LQldKtEv3q0h0hR4S12Ur9pC", "asalt": "7Sem2tc6fjEfW3yYUDN/kSslKEW0e1zqKnBCWbZu2Zw=", "sbox": "d0CmRus0rP0bdc7P7d/wnOyEW14pwFJmcLbdu2W3HmDNRWVJtoNpHrauA/Sr5Vxc" }, "type": "argon2sbox" }, "publicKey": "/+UuD63zItL1EbjxkKUljMgG8Z1w0AJ8pNOR4iq2yQc=" }] } Provide passwords using the following methods to ensure Tessera can decrypt and use the private keys.

Method Description File Supply a password file using the passwordFile field. The password file must contain only one password per line. Empty lines should be used for unlocked keys, and passwords must be provided in the order that key pairs are defined in the configuration file. Direct Supply an unencrypted password using the passwords field, for example "passwords": ["pwd1", "pwd2", ...] . Empty strings should be used for unlocked keys. Passwords must be provided in the order that key pairs are defined in the configuration file. Not recommended for production use. CLI Tessera displays a prompt on the CLI for the passwords of encrypted keys that have not had passwords supplied in the configuration. This process only needs to be performed once, when starting the node. Edit this page Last updatedonOct 9, 2023 bydependabot[bot] Previous Direct keys Next File-based keys