Vaults

Web3 · https://namazustudios.com/docs/namazu-elements-core/features/web3/vaults/

Vaults store encrypted Wallet information in Elements using a public/private key pair.

Vaults are the heart of the custodial wallet system provided by Elements. A Vault securely stores multiple wallets and consists of a public/private key pair.

The contents of the vault's private key can be optionally secured using AES-256. If enabled on a vault, the user must supply their secret passphrase on each request to unlock the contents of the vault.

Warning

When designing an application, we strongly recommend that all vaults are encrypted with a passphrase.

Because the Vault uses private key encryption, it is possible to generate or insert new custodial wallets without needing to unlock the vault first. In this case, Elements simply uses the public key to insert the wallet into the Vault.

Vault Properties

- id
- displayName
- **user** - The user which owns the vault
- **key** - The key pair which Elements uses to store the wallets in the Vault

Vault Key Properties

- **algorithm** - this is the encryption algorithm Elements uses to store the wallets in the vault. The available algorithms are as follows:
- Elliptic Curve 256
- Elliptic Curve 384

- Elliptic Curve 512
- RSA 256
- RSA 384
- RSA 512
- **publicKey** - This is the public key portion of the vault. This is always stored unencrypted.
- **privateKey** - This is the private key portion of the vault. This is either encrypted or stored as plain text.
- **encrypted** - A boolean value indicating whether the vault private key is encrypted
- **encryption** - An arbitrary key-value object which contains encryption metadata. Elements uses this internally to perform various operations against the private key itself.