Create an asymmetric key

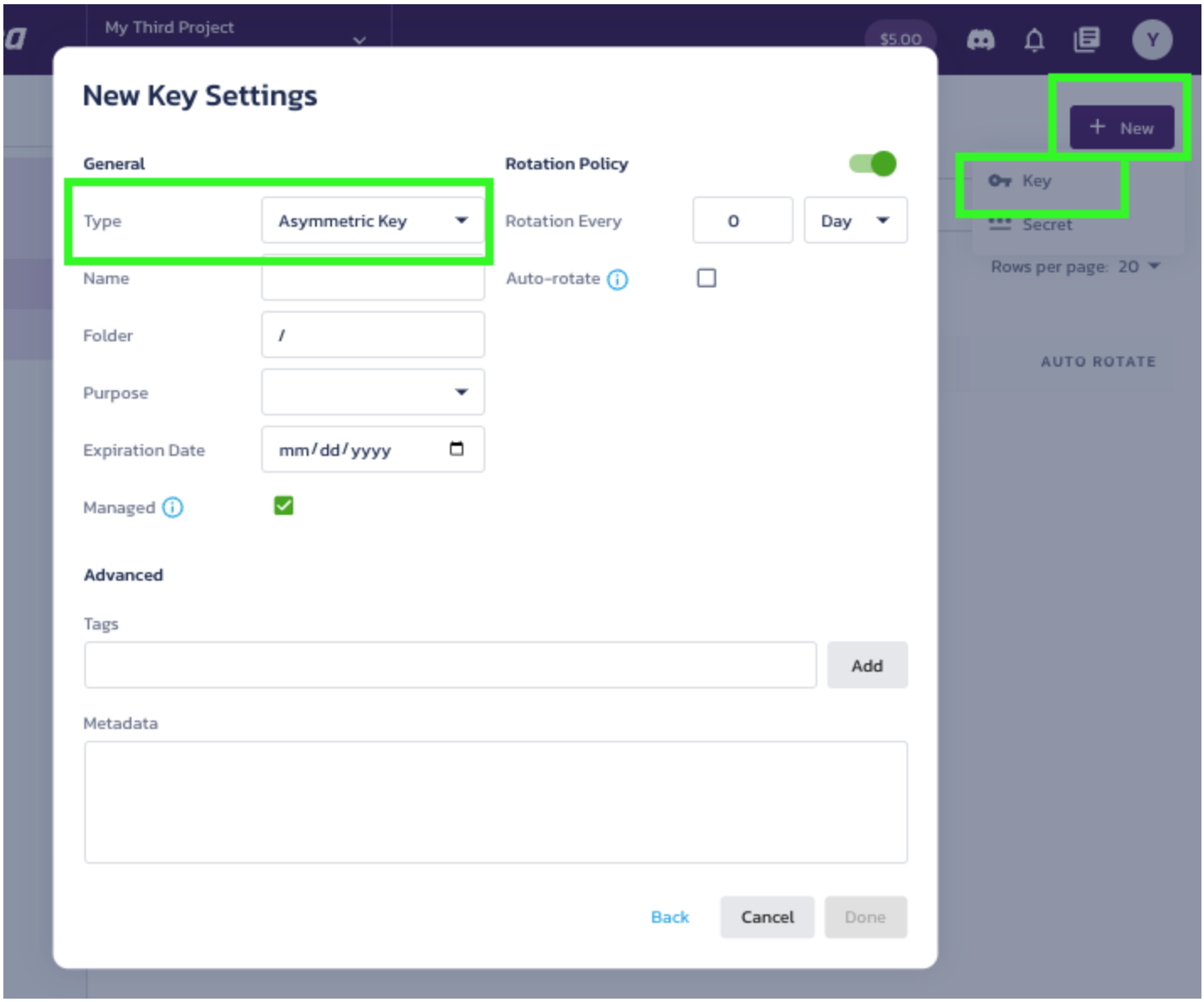
Learn to create asymmetric keys

Asymmetric keys refers to cryptographic key pairs where one key is public and the other is kept private. One key is used to encrypt plaintext, while the other is used to decrypt. (They will not perform both roles.) If the encryption key is public, then the key allows encrypted data to be passed by the public to the private key. If the decryption key is public, then the key serves as a signature verifier. Key pairs generated for a Pangea service never expose their private keys. Encrypt, decrypt, sign, and verify capabilities are built-in.

You can create asymmetric keys using the Pangea Console or with /key/generate endpoint. You can generate key pairs using a designated algorithm or import your own key pair.

In the Pangea Console

1. Go to the Pangea Console
2. Go to Vault in the left-hand navigation menu
3. Click **Secrets & Keys**. On this page, click **+ New button** and select Key. A dialog will appear asking you to choose between a Pangea generated key or to Import a key.
4. Select **Pangea generated key** and click **Next**. A new settings dialog will appear. You will see three general sections asking for information.



5. Fill out the following details:

   - **General**: Give your key basic details during creation
     - In the **Type** field, select **Asymmetric**.
     - In the **Name** field, give your key a name.
     - In the **Folder** field, create a new folder location to store your key (or choose an existing folder).
     - In the **Purpose** field, select Encryption or Signing based on your use case.
     - In the **Expiration date** field, set an expiration date for your key.
     - In the **Managed** field, place a checkmark in the box if you want your private key to only be accessible once directly after creation.
   - **Rotation Policy**: To enable rotation policy creation, switch on Rotation Policy.
     - In the **Rotation Every** field, use the calendar options to choose how often a key is rotated.

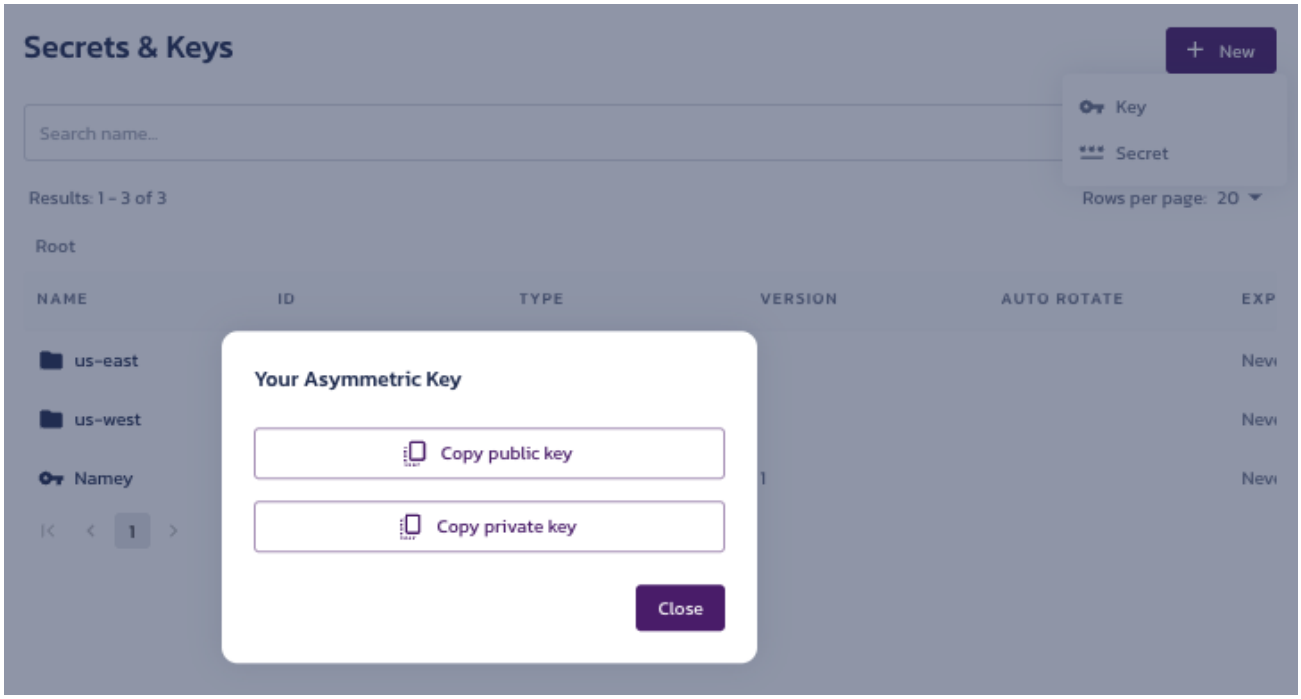
- Place a checkmark in the **Auto-rotate** box if you want Vault to automatically create new keys on each rotation.

- **Advanced**: Provide additional meta information about your key
  - In the **Tags** field, add tags to this field so additional context.
  - In the **Metadata** field, add information to a key, using JSON. Metadata is useful because it provides a summary of basic details about data.

6. Click **Done**. The next few steps will vary depending on whether you selected Managed or not.

Note

If you didn't place a checkmark next to **Managed**, then when you click **Done**, a new dialog will appear with your private and public key. Your keys will not be visible but you can copy them onto your clipboard.



Click **Close** when you're done.

Using the API

To create a asymmetric key, you'll need to:

- Call the /key/generate endpoint

- Include the following parameters in your API request:
  - `type`
  - `purpose`
  - `algorithm`
- Set `type` to `asymmetric`

Example

API Request

In the example below, the API request is calling the /key/generate endpoint, and passing the parameters listed above. Notice that `type` is set to `asymmetric`.

```
curl -sSLX POST 'https://vault.$PANGEA_DOMAIN/v1/key/generate' \
-H 'Authorization: VAULT_AUTH_TOKEN' \
-H 'Content-Type: application/json' \
-d '{"type":"asymmetric_key","purpose":"signing","algorithm":"ed25519"}'
```

API Response

A successful API response might look like this:

```
{
  "request_id": "prq_yqqlzbpgbiva2x636ouh422mtduv3kwr",
  "request_time": "2023-02-07T20:23:21.376161Z",
  "response_time": "2023-02-07T20:23:21.644556Z",
  "status": "Success",
  "summary": "Key pair created",
  "result": {
    "algorithm": "ed25519",
    "id": "pvi_wydu7diorkatuevurt2v4jkscgp5lejw",
    "public_key": "-----BEGIN PUBLIC KEY-----
\nMCowBQYDK2VwAyEArG0/YU1B24xYSShubZPbGsphH9sK/70yDd//c1WwRrk=\n-----END
PUBLIC KEY-----\n",
    "type": "asymmetric_key",
    "version": 1
```

```
    }
}
```

Was this article helpful? Yes No Contact us