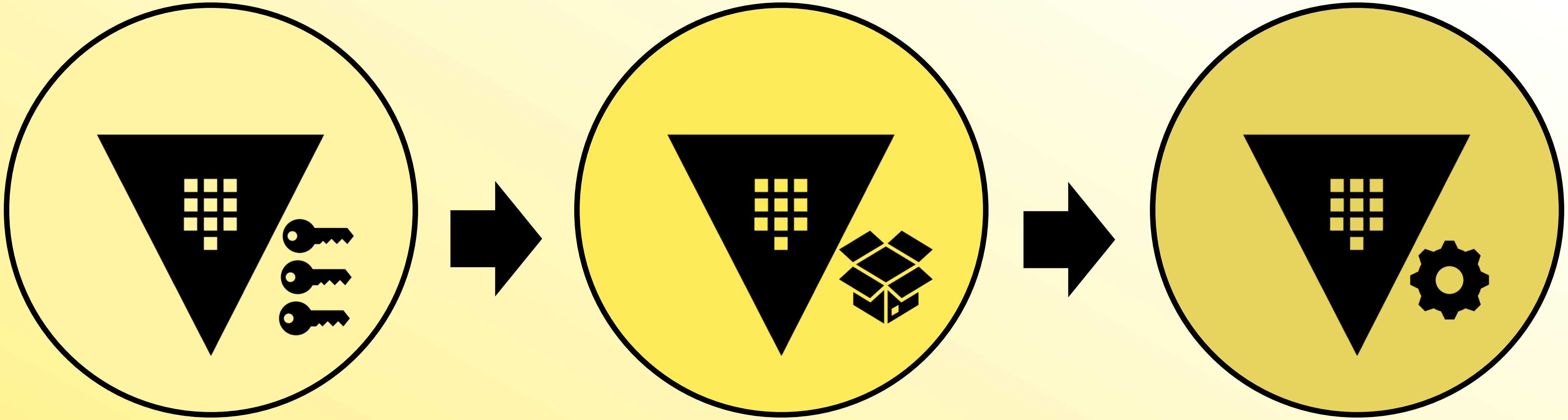
Vault

CERTIFIED
OPERATIONS
PROFESSIONAL

Practice Secure Vault Initialization

Vault Deployment Workflow



Initialize

Unseal

Configure

Vault Initialization

Initialize

- Vault initialization is when Vault creates the master key and key shares
- Options to define thresholds, key shares, recovery keys, and encryption
- Vault initialization is also where the initial root token is generated and returned to the user

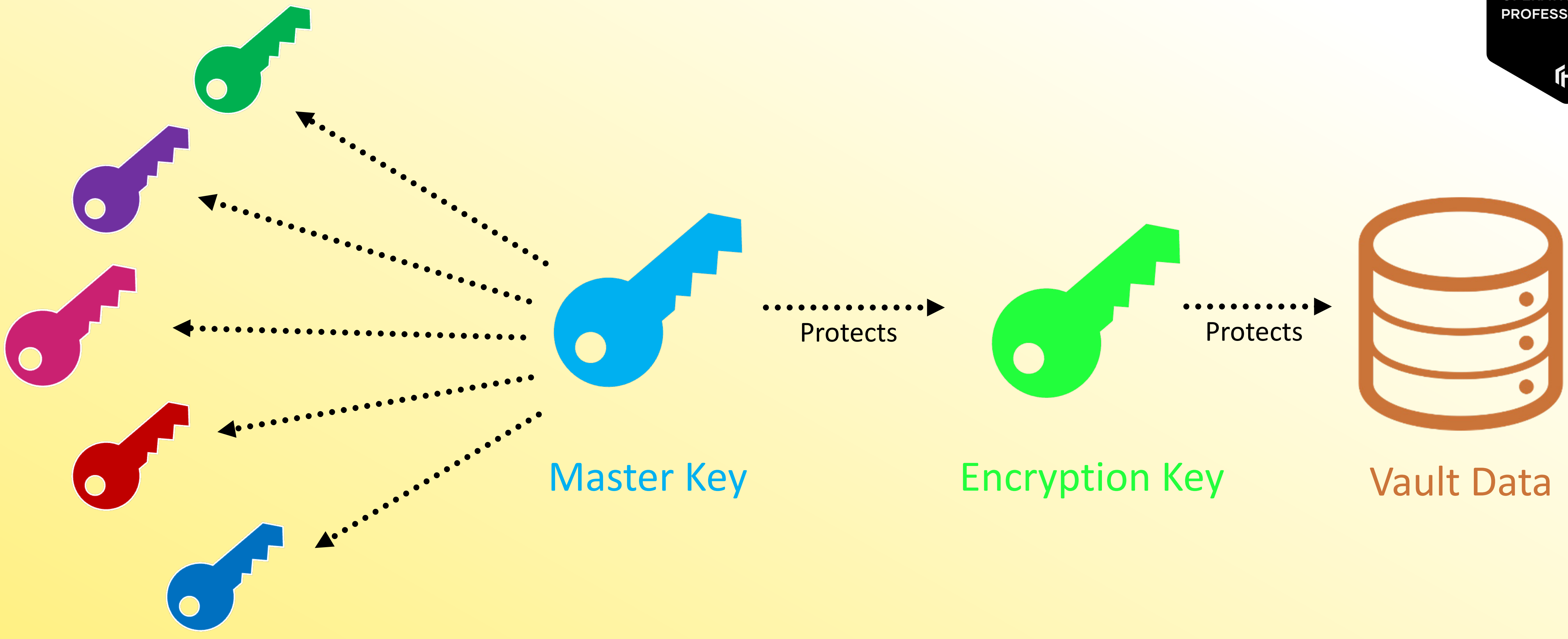
Vault Initialization

Initialize

How can you protect these keys and root token?

Vault Initialization

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL



Key Shards
(Unseal Keys)

Provide Keys to Trusted Employees

But...Only a Single Person Can Initialize Vault

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL

```
$ vault operator init
```

Wait...he has all the keys? That doesn't seem very secure

Vault

CERTIFIED
OPERATIONS
PROFESSIONAL

How can we better protect our keys and root token while following the Vault security model?

Vault Initialization

Common options for: `vault operator init`

Change the Number of
<u>Unseal Keys/Threshold</u>

```
-key-shares=5
-key-threshold=3
```

Change the Number of Keys/Threshold
<u>for Auto Unsealed Clusters</u>

```
-recovery-shares=5
-recovery-threshold=3
```

Vault Initialization

Common options for: `vault operator init`

Encrypt the Unseal Keys with Provided PGP Keys

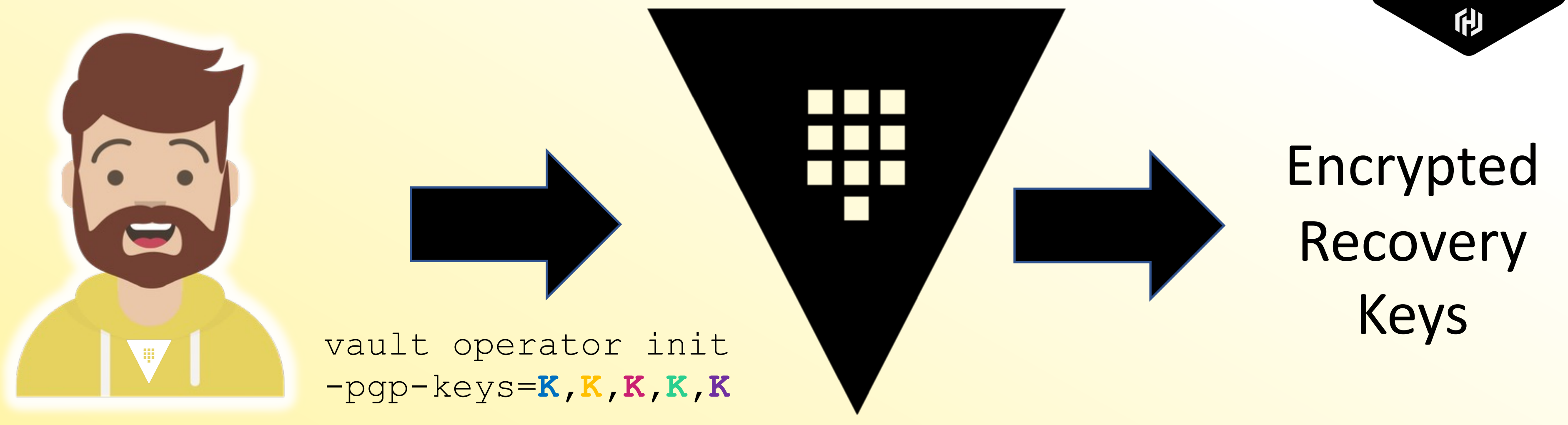
```
-pgp-keys=<keys>
```

Encrypt the Recovery Keys with the Provided PGP Keys

```
-recovery-pgp-keys=<keys>
```

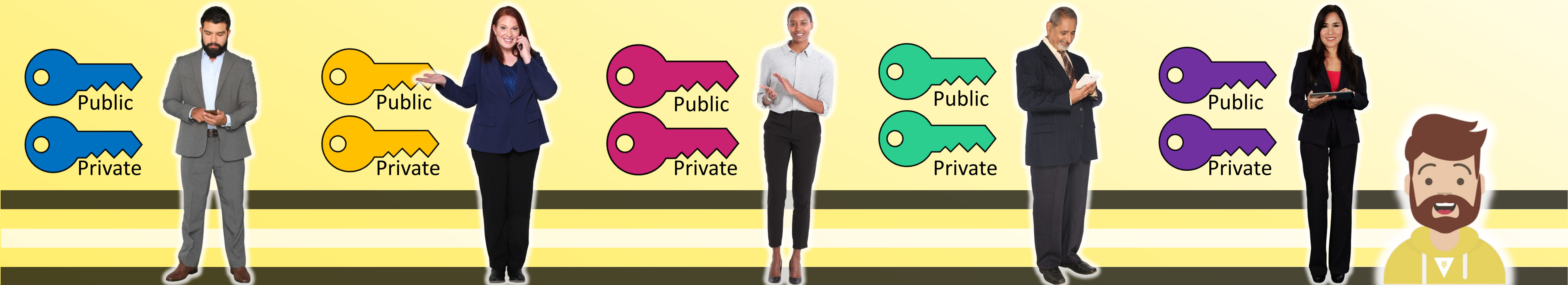
Secure Vault Initialization

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL



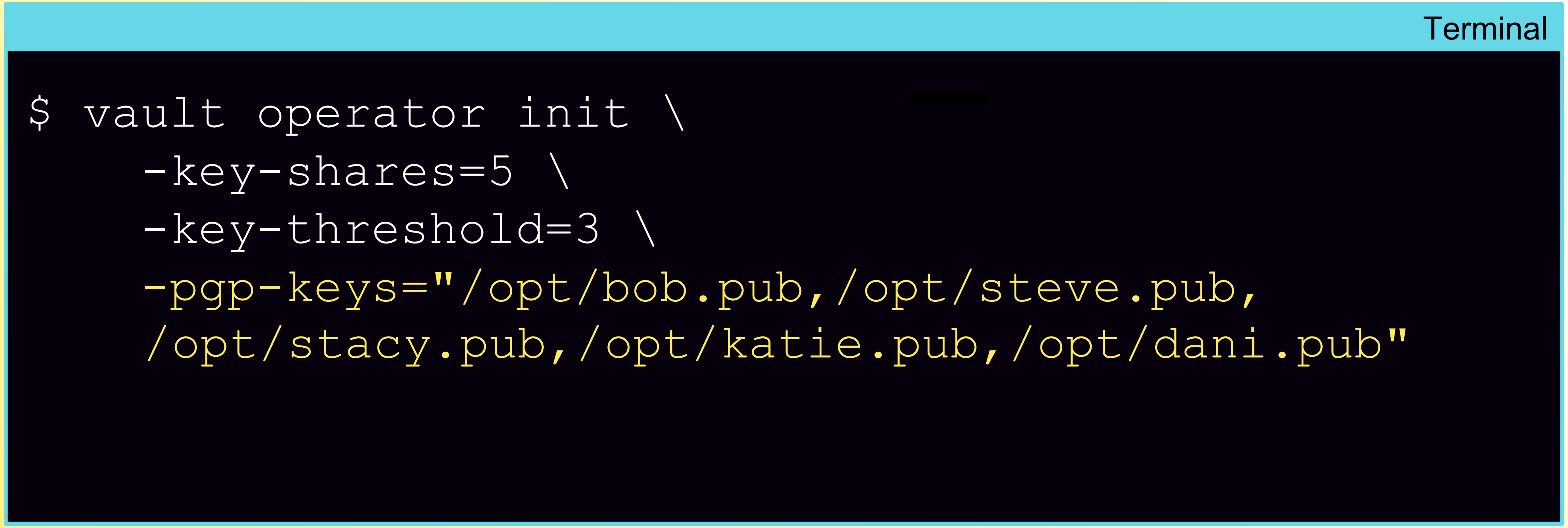
```
vault operator init
-pgp-keys=K,K,K,K,K
```

Encrypted
Recovery
Keys



Secure Vault Initialization

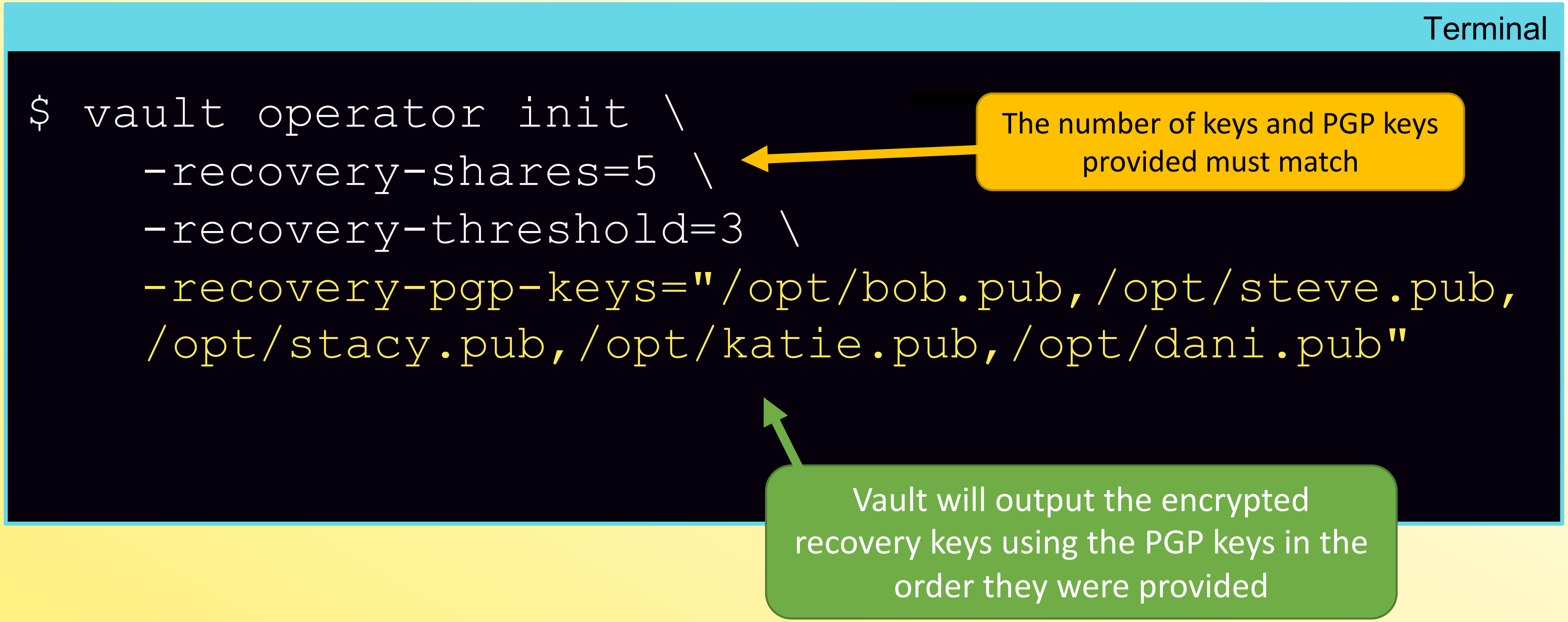
For Default Unseal Keys



```
$ vault operator init \
    -key-shares=5 \
    -key-threshold=3 \
    -pgp-keys="/opt/bob.pub,/opt/steve.pub,
    /opt/stacy.pub,/opt/katie.pub,/opt/dani.pub"
```

Secure Vault Initialization

For Auto Unsealed Clusters



```
$ vault operator init \
    -recovery-shares=5 \
    -recovery-threshold=3 \
    -recovery-pgp-keys="/opt/bob.pub,/opt/steve.pub,
    /opt/stacy.pub,/opt/katie.pub,/opt/dani.pub"
```

The number of keys and PGP keys provided must match

Vault will output the encrypted recovery keys using the PGP keys in the order they were provided

Protecting the Root Token

Initialize

Unseal or
Recovery Keys

Initial Root Token

Protecting the Root Token

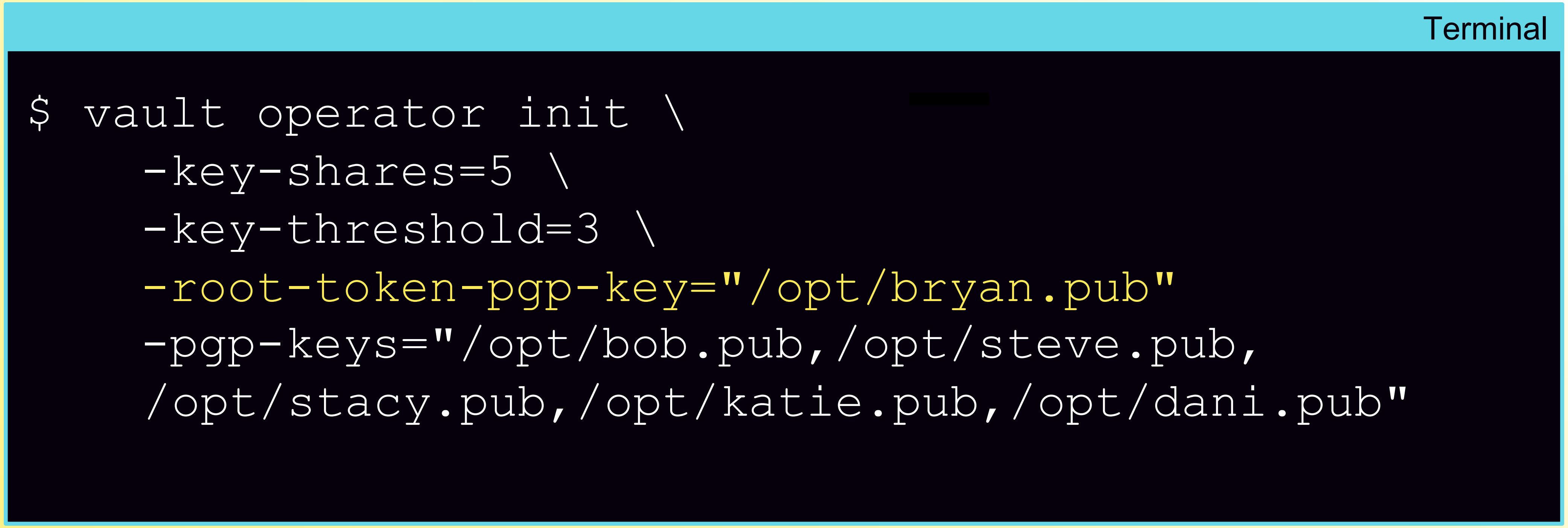
Option for: `vault operator init`

Encrypt the Root Token with Provided PGP Key

```
-root-token-pgp-key=<key>
```

Secure Vault Initialization

For Default Unseal Keys



```
$ vault operator init \
    -key-shares=5 \
    -key-threshold=3 \
    -root-token-pgp-key="/opt/bryan.pub"
    -pgp-keys="/opt/bob.pub,/opt/steve.pub,
    /opt/stacy.pub,/opt/katie.pub,/opt/dani.pub"
```