Vault

CERTIFIED
OPERATIONS
PROFESSIONAL

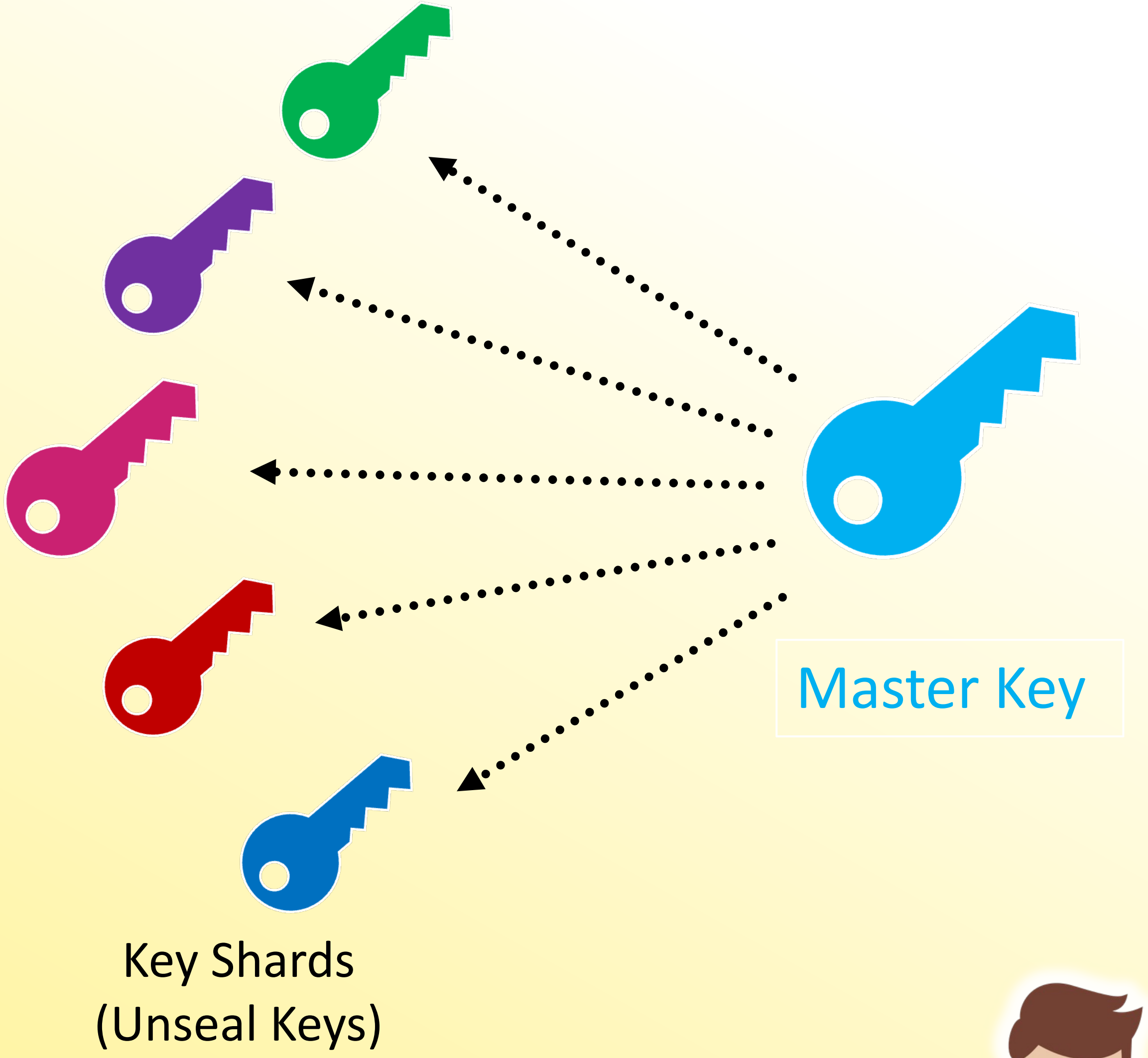
Rekey Vault and Rotate Encryption Keys

What is Rekey?

- Creates a new set of Vault recovery/unseal keys
- Allows you to specify the number of keys and threshold during the rekey process
- Requires a threshold of keys to successfully rekey (similar to an unseal or root token generation)
- Provides a nonce value to be given to key holders

Why Would I Need to Rekey?

- One or more keys are lost
- Employees leave the organization
- Your organization requires that you rekey after a period of time as a security measurement



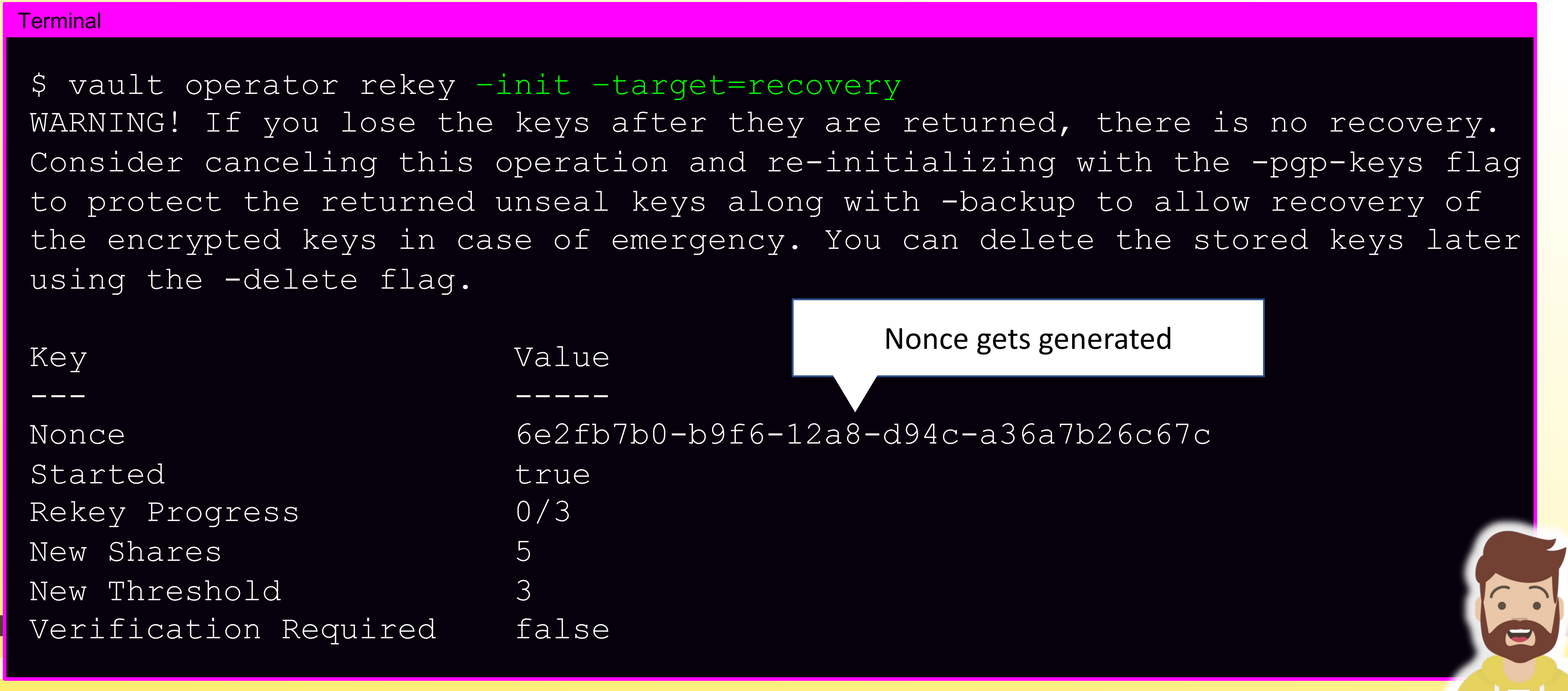
Rekey

To rekey Vault, use the `vault operator rekey` command:

Command Options	Description
-init	Initialize the rekey process
-key-shares=<num>	Specify the number of key shares
-key-threshold=<num>	Specify the threshold of keys needed to reconstruct the master key
-nonce	Pass the nonce value
-pgp-key=<keys>	Specify the PGP keys to encrypt the generated keys
-status	Print the status of the current rekey operation
-target=recovery	Specify that you want recovery keys if using HSM or Auto Unseal

Rekeying Vault

Step 1 – Initialize the Process



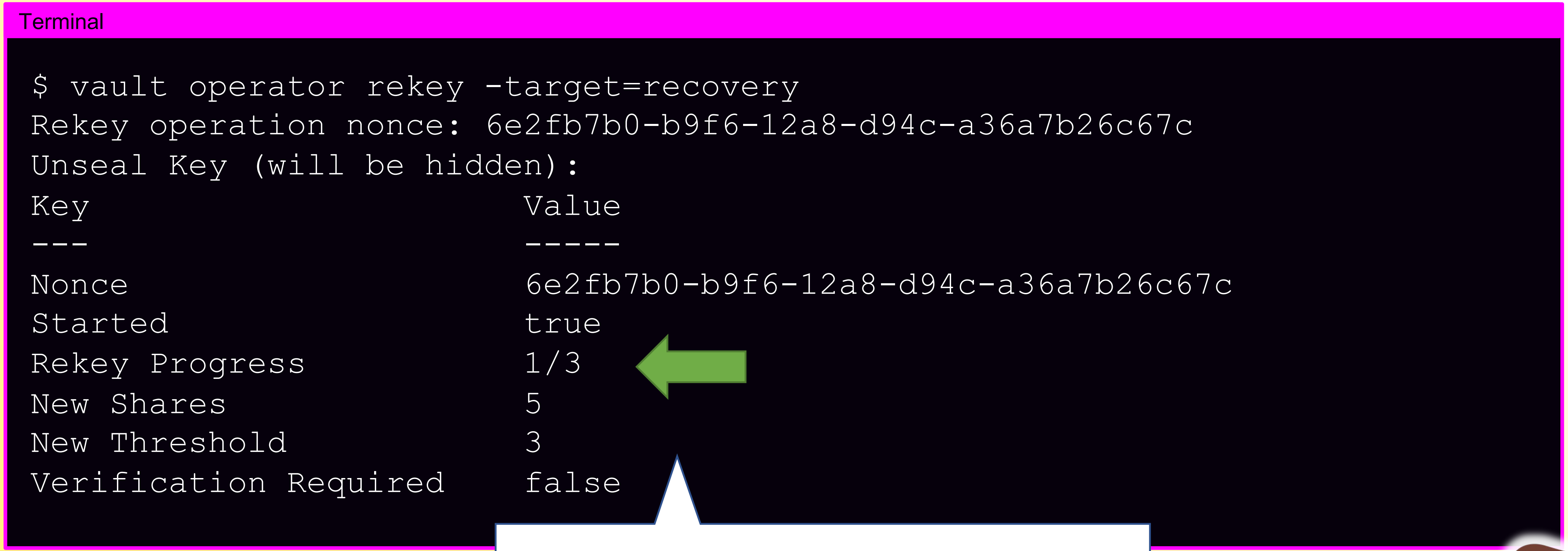
Terminal

```
$ vault operator rekey -init -target=recovery
WARNING! If you lose the keys after they are returned, there is no recovery.
Consider canceling this operation and re-initializing with the -pgp-keys flag
to protect the returned unseal keys along with -backup to allow recovery of
the encrypted keys in case of emergency. You can delete the stored keys later
using the -delete flag.

Key                     Value
---                     -----
Nonce                   6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Started                 true
Rekey Progress          0/3
New Shares              5
New Threshold           3
Verification Required   false
```

Nonce gets generated

Rekeying Vault

Step 2 – Provide the Existing Keys

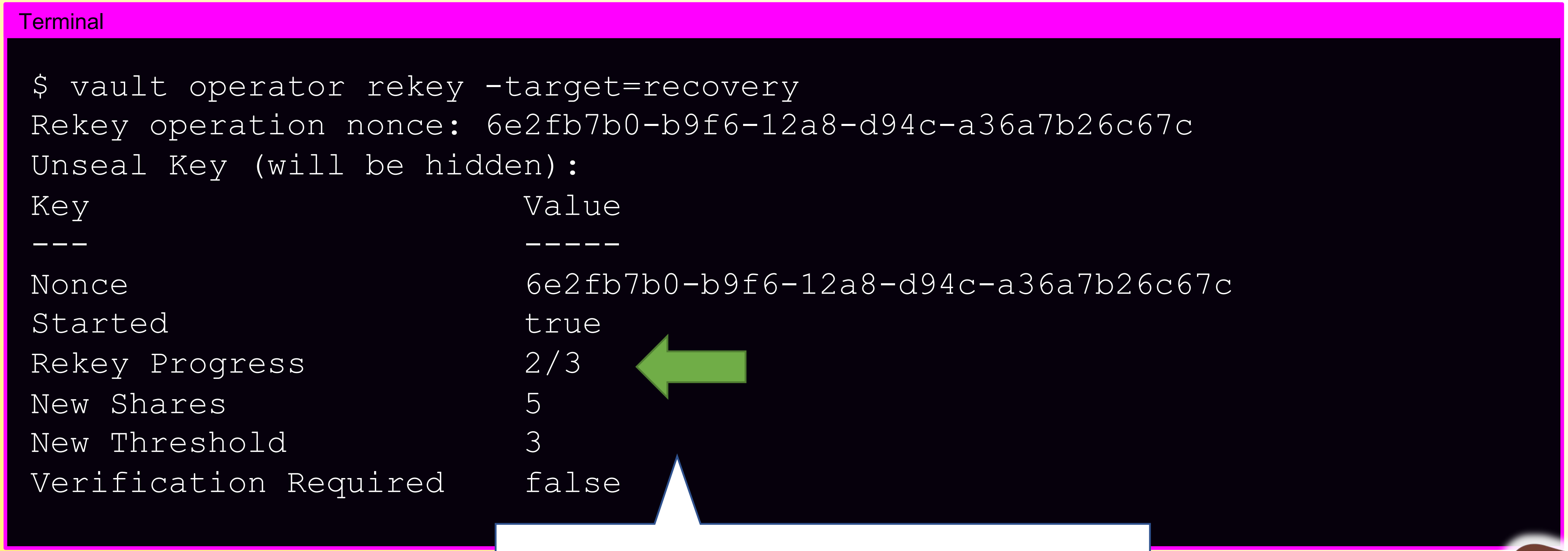


```
$ vault operator rekey -target=recovery
Rekey operation nonce: 6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Unseal Key (will be hidden):
Key                        Value
---                        -----
Nonce                      6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Started                    true
Rekey Progress             1/3
New Shares                 5
New Threshold              3
Verification Required      false
```

Key holders each provide their key until you meet the threshold

Rekeying Vault

Step 2 – Provide the Existing Keys

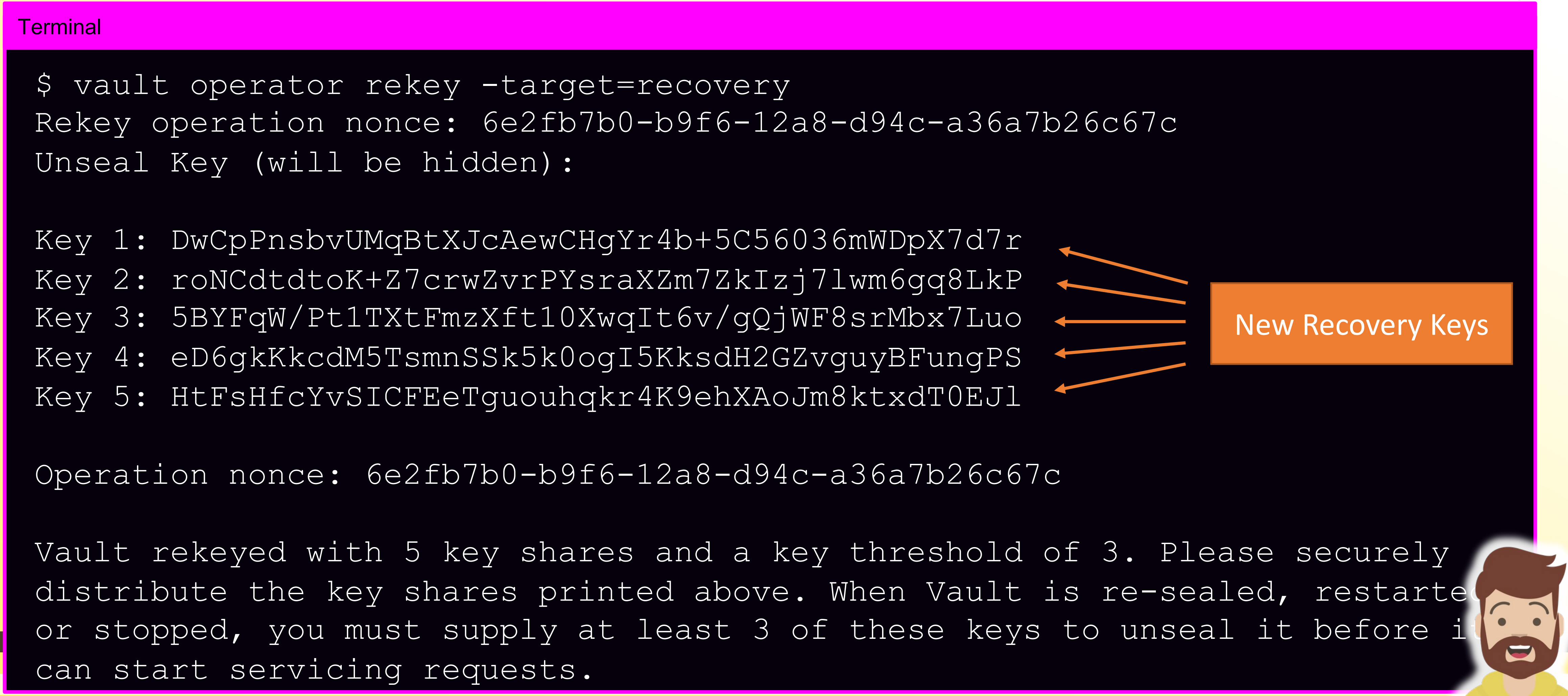


```
$ vault operator rekey -target=recovery
Rekey operation nonce: 6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Unseal Key (will be hidden):
Key                         Value
---                         ------
Nonce                       6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Started                     true
Rekey Progress              2/3
New Shares                  5
New Threshold               3
Verification Required       false
```

Key holders each provide their key until you meet the threshold

Rekeying Vault

Receive New Recovery Keys



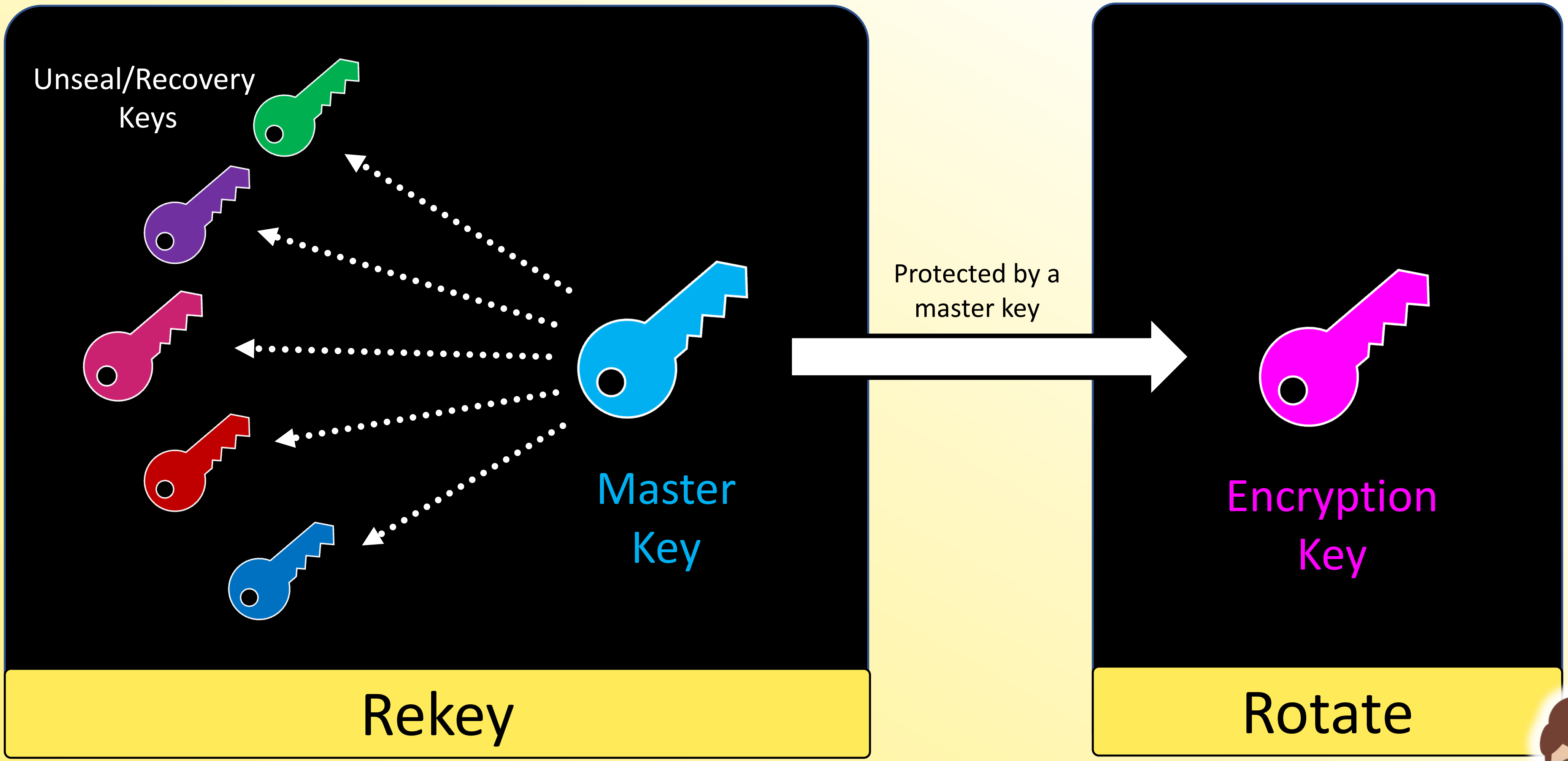
Terminal

```
$ vault operator rekey -target=recovery
Rekey operation nonce: 6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c
Unseal Key (will be hidden):

Key 1: DwCpPnsbvUMqBtXJcAewCHgYr4b+5C56036mWDpX7d7r
Key 2: roNCdtdtoK+Z7crwZvrPYsraXZm7ZkIzj7lwm6gq8LkP
Key 3: 5BYFqW/Pt1TXtFmzXft10XwqIt6v/gQjWF8srMbx7Luo
Key 4: eD6gkKkcdM5TsmnSSk5k0ogI5KksdH2GZvguyBFungPS
Key 5: HtFsHfcYvSICFEeTguouhqkr4K9ehXAoJm8ktxdT0EJl

Operation nonce: 6e2fb7b0-b9f6-12a8-d94c-a36a7b26c67c

Vault rekeyed with 5 key shares and a key threshold of 3. Please securely
distribute the key shares printed above. When Vault is re-sealed, restarte
or stopped, you must supply at least 3 of these keys to unseal it before i
can start servicing requests.
```

Impact to Production?

- The Rekey operation is an online operation and can be done anytime
- This means no downtime for performing this operation
- Vault continues to service requests during the rekey operation

Rekey vs. Key Rotation



What is Key Rotation?

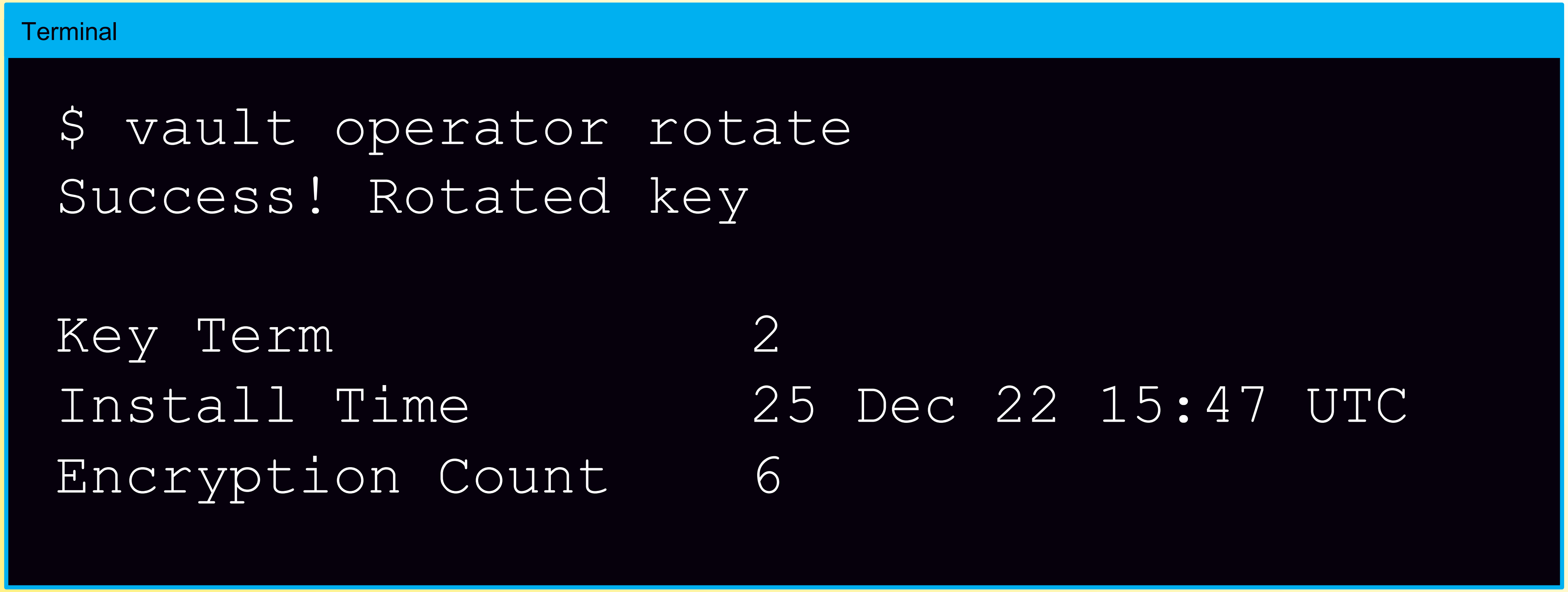
- Rotates the encryption key that is used to protect data on the storage backend
- Since the encryption key is never available to users or operators, it does NOT require a threshold of key holders to rotate
- New keys are added to the keyring - old values can still be decrypted with the old key

Encryption Key

Rotate

Rotating the Encryption Key

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL



```
$ vault operator rotate
Success! Rotated key

Key Term               2
Install Time           25 Dec 22 15:47 UTC
Encryption Count       6
```

Permissions Needed for Key Rotation

- The `sys/rotate` endpoint is a root protected API endpoint
  - This means that you either need a **root token** or **sudo** privileges on the `sys/rotate` path

Terminal

```
path "sys/rotate" {
  capabilities = ["update","sudo"]
}
path "sys/key-status" {
  capabilities = ["read"]
}
```

Needed to read the status of the key after rotating it, not to rotate it