HSM Auto-Unseal

ICT.TECHNOLOGY
INFRASTRUCTURE · CLOUD · TRANSITION

Monday, January 6, 2025

What is a HSM?

A Hardware Security Module (HSM) is:

- A network-based device (or a PCI card in a server), which stores Secrets and keys securely
- A tamper-resistant device
- Expensive

Where to find HSMs?

You can find them:

- On-premise at enterprises with high requirements on security (Government, banks and credit card issuers, insurances, hospitals, etc.)

- At cloud providers, for example:

  - Oracle Cloud Infrastructure (OCI Vault), both software (very inexpensive), as hardware partition on a shared HSM (expensive) or dedicated HSM (very expensive)
  - Amazon Web Services: AWS KMS as shared HSM (expensive), oder AWS CloudHSM as dedicated HSM (extremely teuer)
  - Some manufacturers offer cloud-based HSM services

Vault and HSMs

- Store Vault root keys in a HSM
- Auto-Unseal with the key which is saved in the HSM
- Seal Wrapping
- FIPS 140-2 Compliance (optional, Vault 1.10+)
- Improved random values through Entropy Augmentation using external cryptographic modules

Vault and HSMs

Requirements:

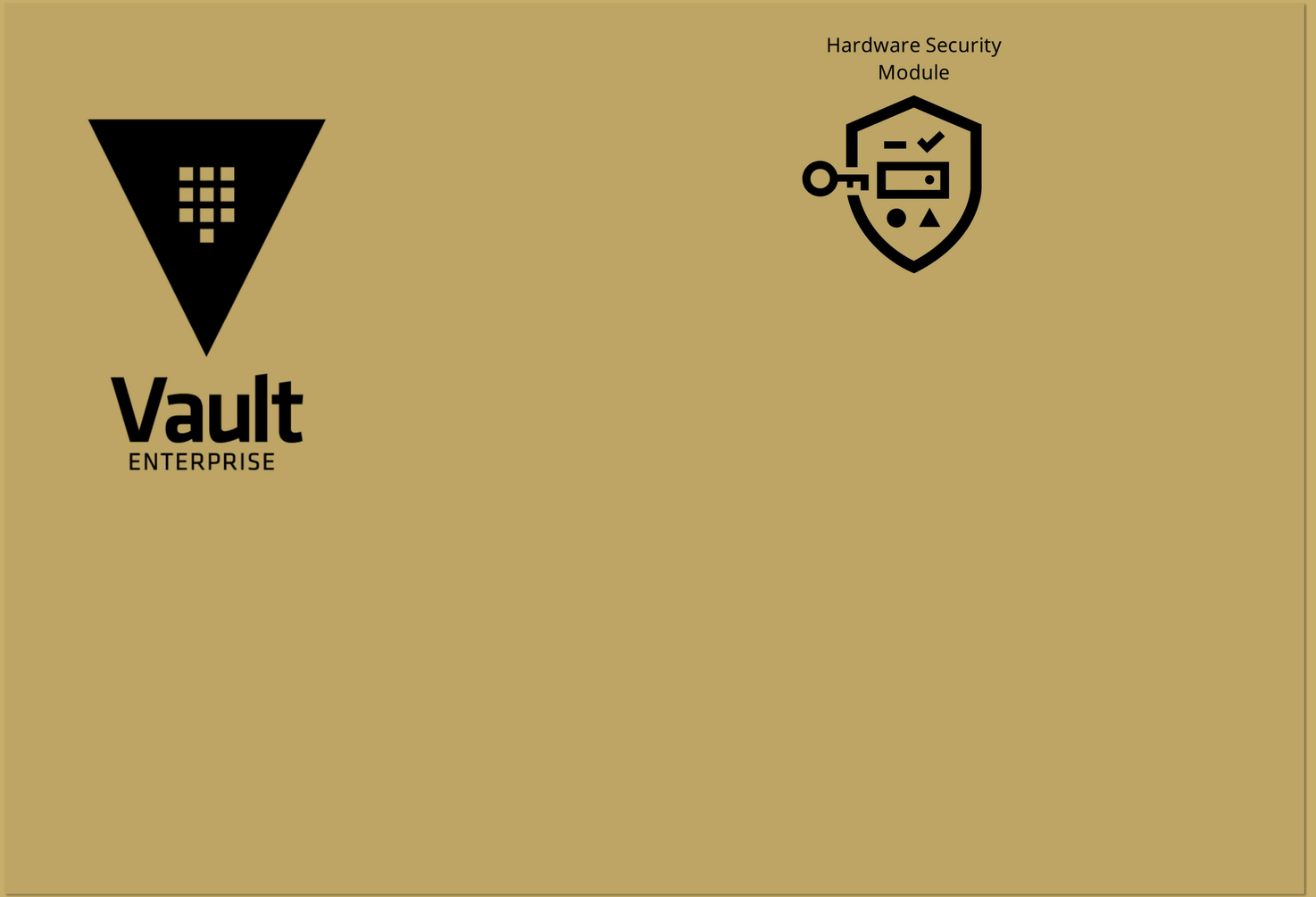
- Requires HashiCorp Vault Enterprise Plus as minimum
- HSM must support the PKCS#11 standard (Interfaces must support v2.20+, integration libraries must be Linux running on amd64)

1. Initialisation

What happens when initialising Vault?

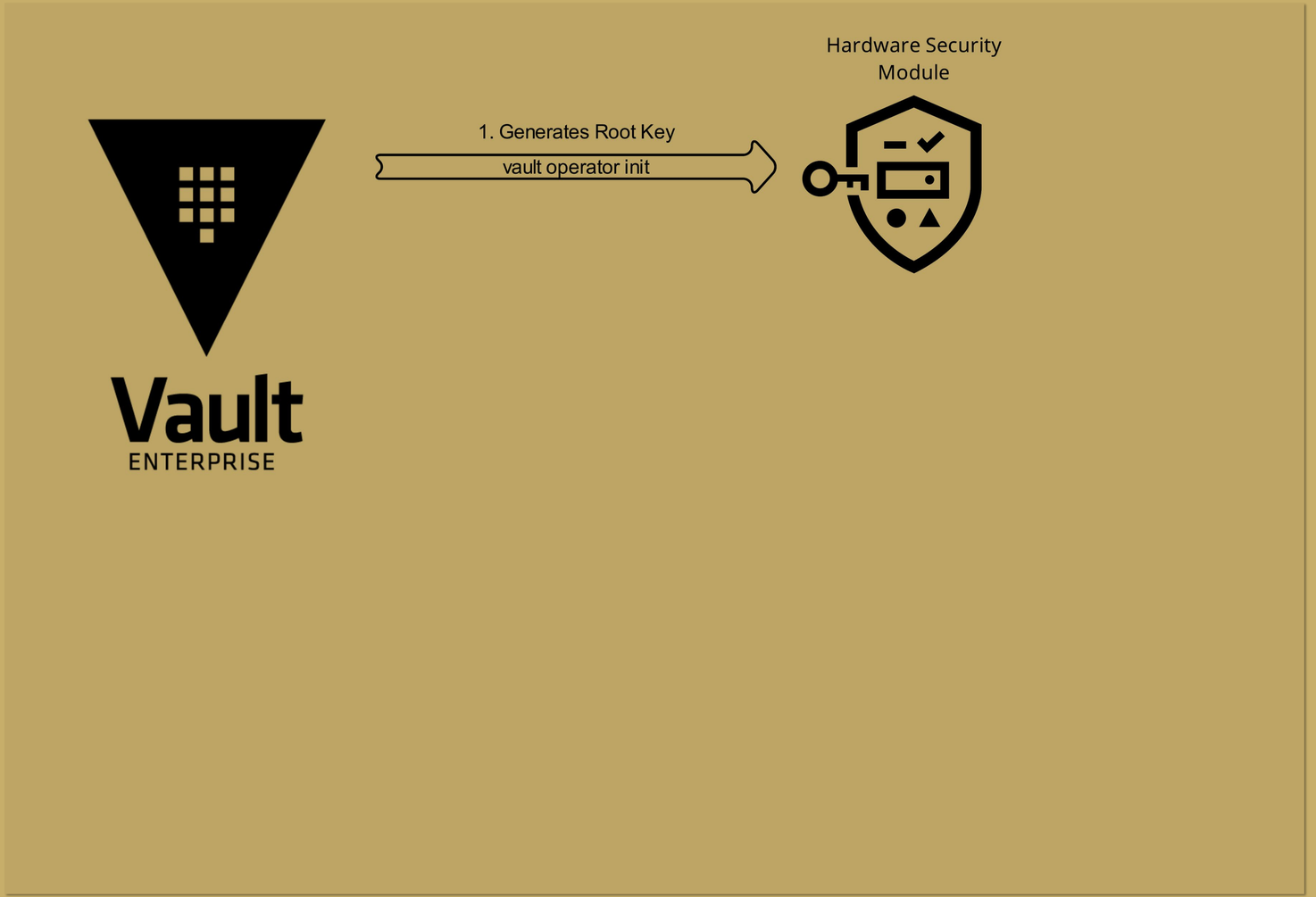
1. Initialisation

Step 1:



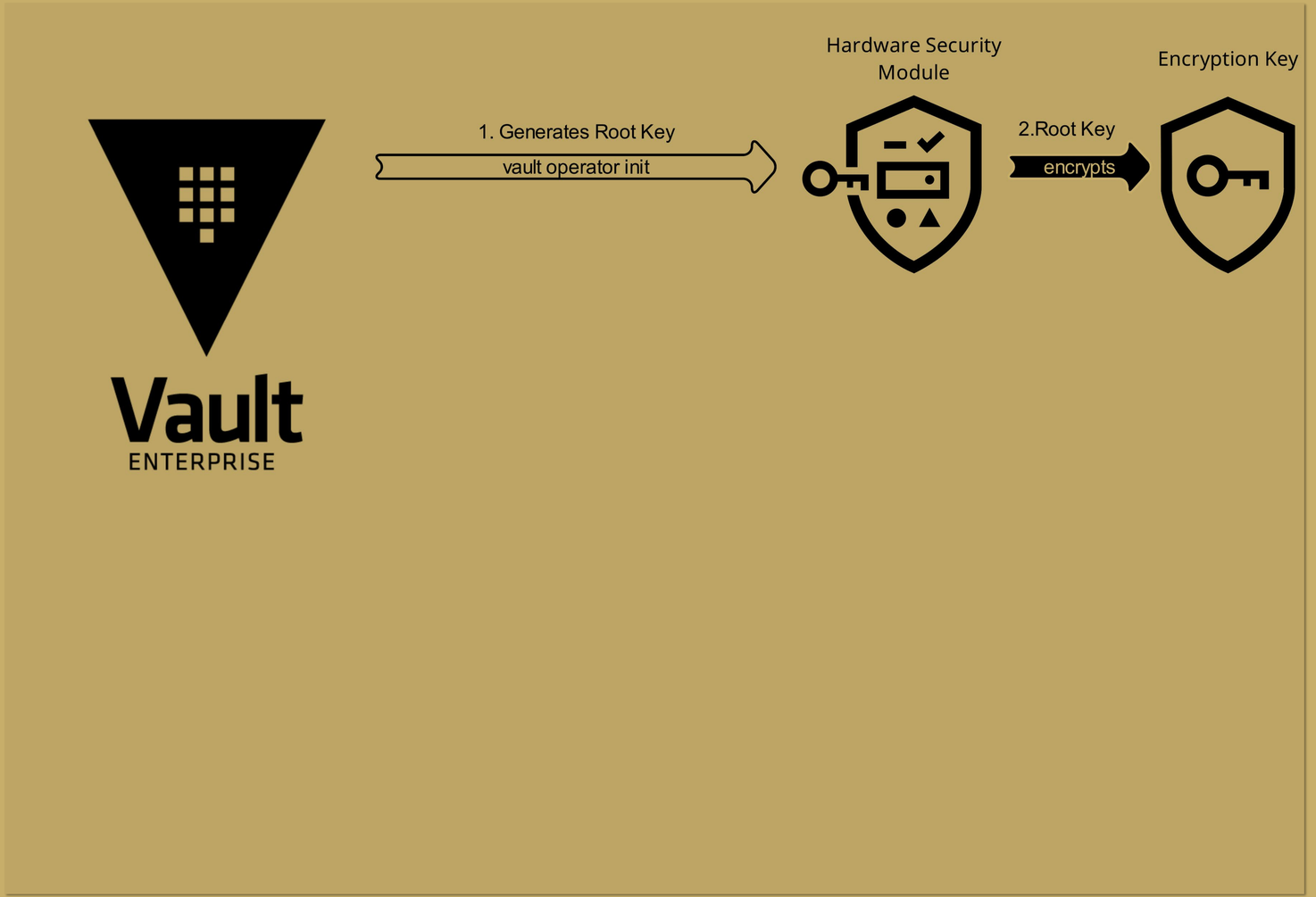
1. Initialisation

Step 2:



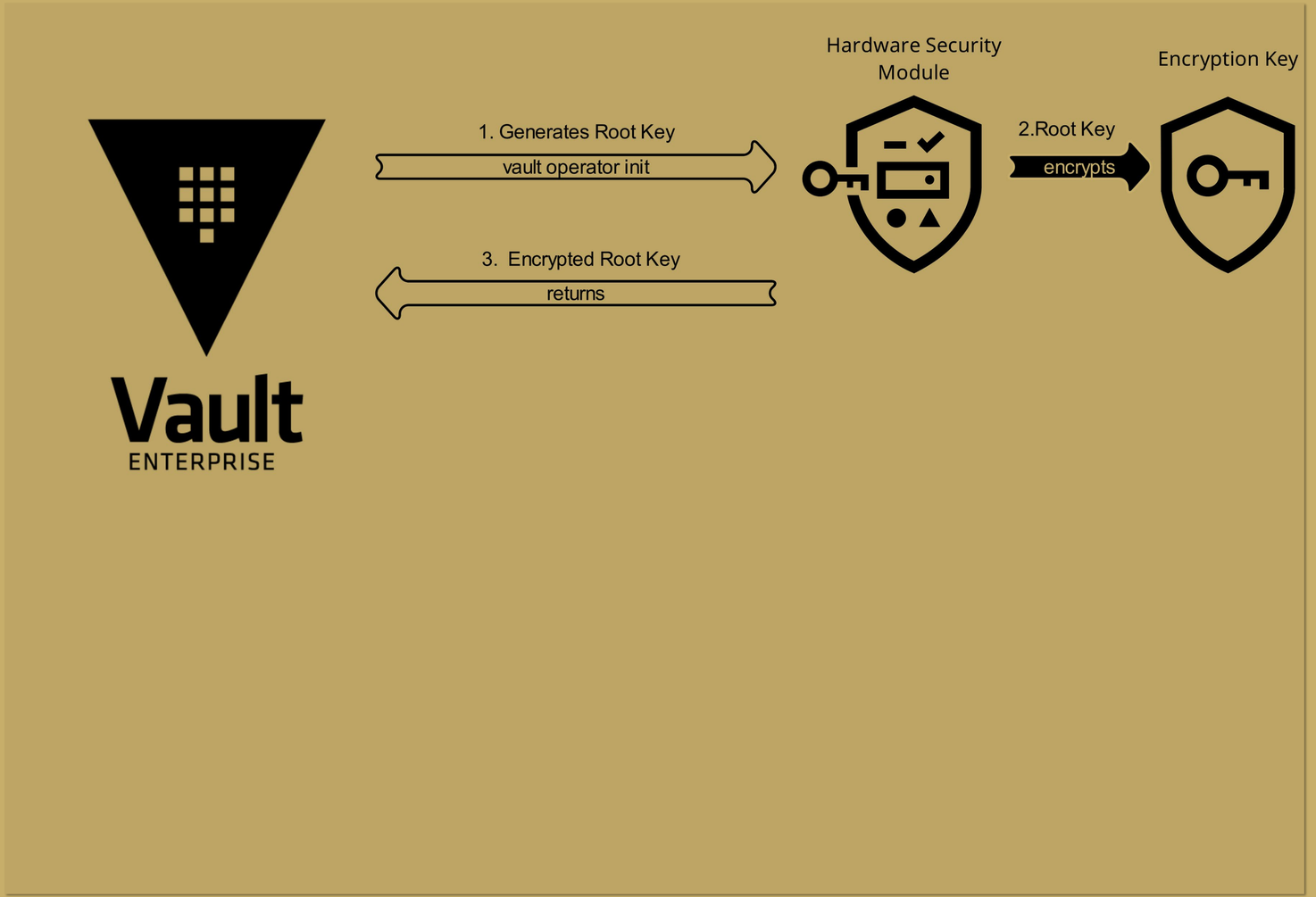
1. Initialisation

Step 3:



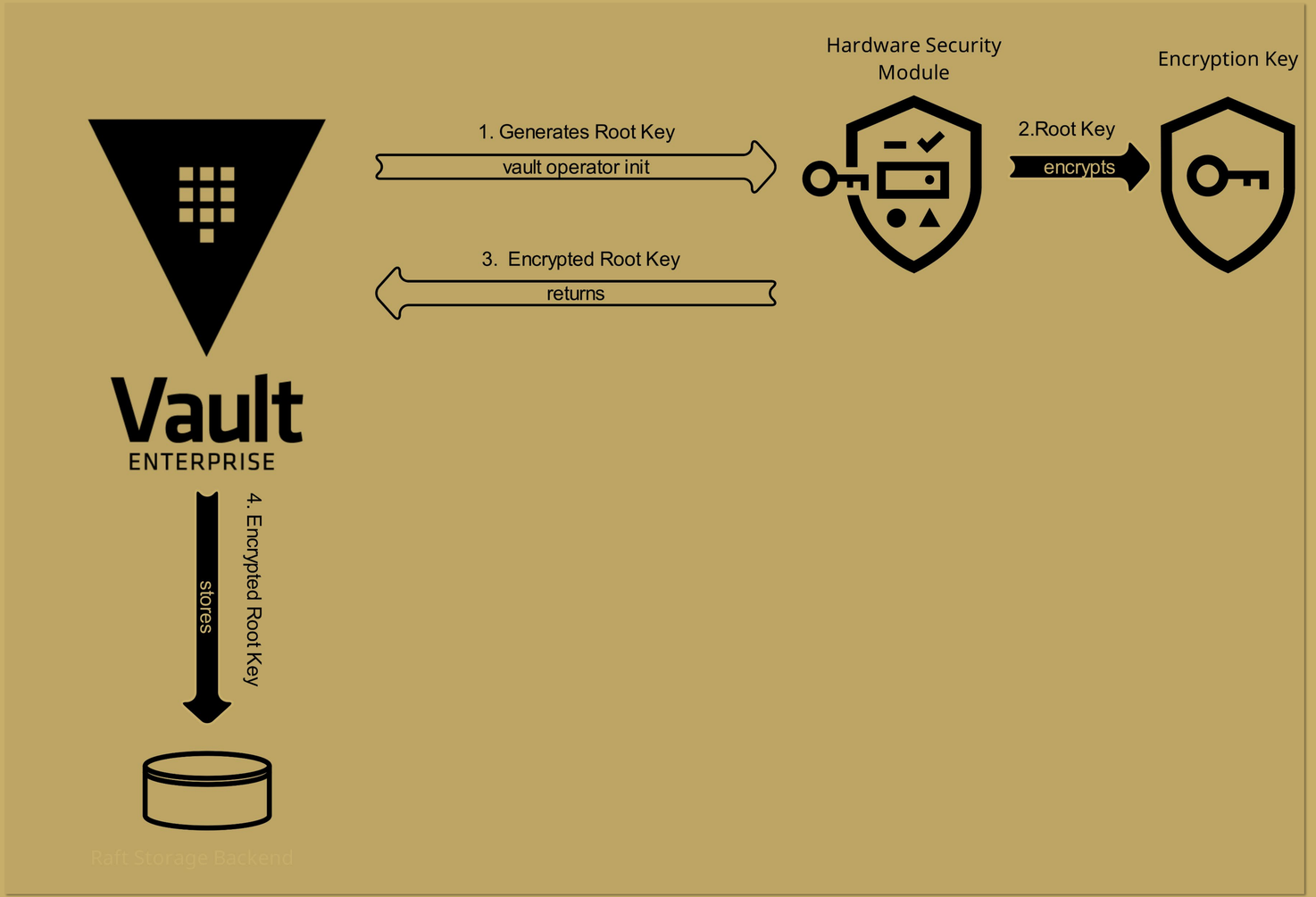
1. Initialisation

Step 4:



1. Initialisation

Step 5:



Demonstration

Highlight #1

Minimal configuration (\w HSM) of Vault before first use

Highlight #2

Initialisation against HSM using *vault operator init*

Highlight #3

We see an Auto-Unseal first hand

Proof-of-Concept

Test Case #1

Accessing secrets without previous HSM Auto-Unseal ***must not*** be possible.

Test Case #2

Manual unsealing with Recovery Key Shares ***must not*** be possible.

Test Case #3

Vault ***must not*** start up without the HSM.

Proof-of-Concept

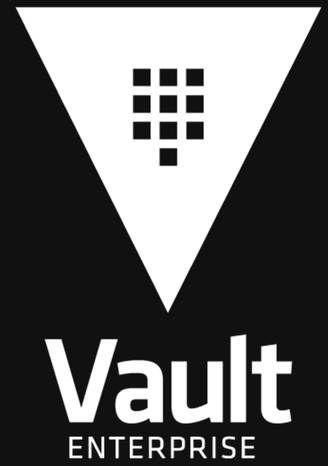
Test Case #1

Accessing secrets without previous HSM Auto-Unseal ***must not*** be possible.

Proof-of-Concept

Test Case #2

Manual unsealing with Recovery Key Shares ***must not*** be possible.



Proof-of-Concept

Test Case #3

Vault ***must not*** start up without the HSM.

Proof-of-Concept

Test Case #1

Accessing secrets without previous HSM Auto-Unseal ***must not*** be possible.

Test Case #2

Manual unsealing with Recovery Key Shares ***must not*** be possible.

Test Case #3

Vault ***must not*** start up without the HSM.

Thanks!

ICT.TECHNOLOGY

INFRASTRUCTURE · CLOUD · TRANSITION

https://ict.technology