HSM Auto-Unseal

ICT.TECHNOLOGY
INFRASTRUCTURE · CLOUD · TRANSITION

Lundi 6 janvier 2025

Qu'est-ce qu'un HSM?

Un Hardware Security Module (HSM) est:

- Un dispositif réseau (ou une carte PCI installée dans un serveur) qui vous permet de stocker de manière sécurisée vos secrets et vos clés
- Un dispositif protégé contre tout accès physique non autorisé (tamper resistance)
- Coûteux.

•Oracle Cloud Infrastructure (OCI Vault), disponible en version logicielle (très économique), en tant que partition matérielle sur un HSM partagé (coûteux) ou en HSM dédié (très coûteux)
•Amazon Webservices : AWS KMS en HSM partagé (coûteux), ou AWS CloudHSM en HSM dédié (extrêmement coûteux)
•Certains fabricants vous proposent également des solutions HSM basées sur le cloud

Où pouvez-vous trouver les HSMs ?

Vous pouvez les trouver :

- Sur site dans les entreprises ayant des exigences élevées en matière de sécurité (administrations, banques et émetteurs de cartes de crédit, assurances, hôpitaux, etc.)

- Chez les fournisseurs Cloud, par exemple :

  - Oracle Cloud Infrastructure (OCI Vault), disponible en version logicielle (très économique), en tant que partition matérielle sur un HSM partagé (coûteux) ou en HSM dédié (très coûteux)
  - Amazon Web Services : AWS KMS en HSM partagé (coûteux), ou AWS CloudHSM en HSM dédié (extrêmement coûteux)
  - Certains fabricants vous proposent également des solutions HSM basées sur le cloud

•Seal Wrapping
•Conformité FIPS 140-2 (optionnel, depuis Vault 1.10)
•Valeurs aléatoires améliorées par augmentation d'entropie depuis un module cryptographique externe

Vault et HSMs

- Stockage des Vault Root Keys dans le HSM
- Auto-Unseal avec la clé stockée dans le HSM
- Seal Wrapping
- Conformité FIPS 140-2 (optionnel, depuis Vault 1.10)
- Valeurs aléatoires améliorées par augmentation d'entropie depuis un module cryptographique externe

Vault und HSMs

Anforderungen:

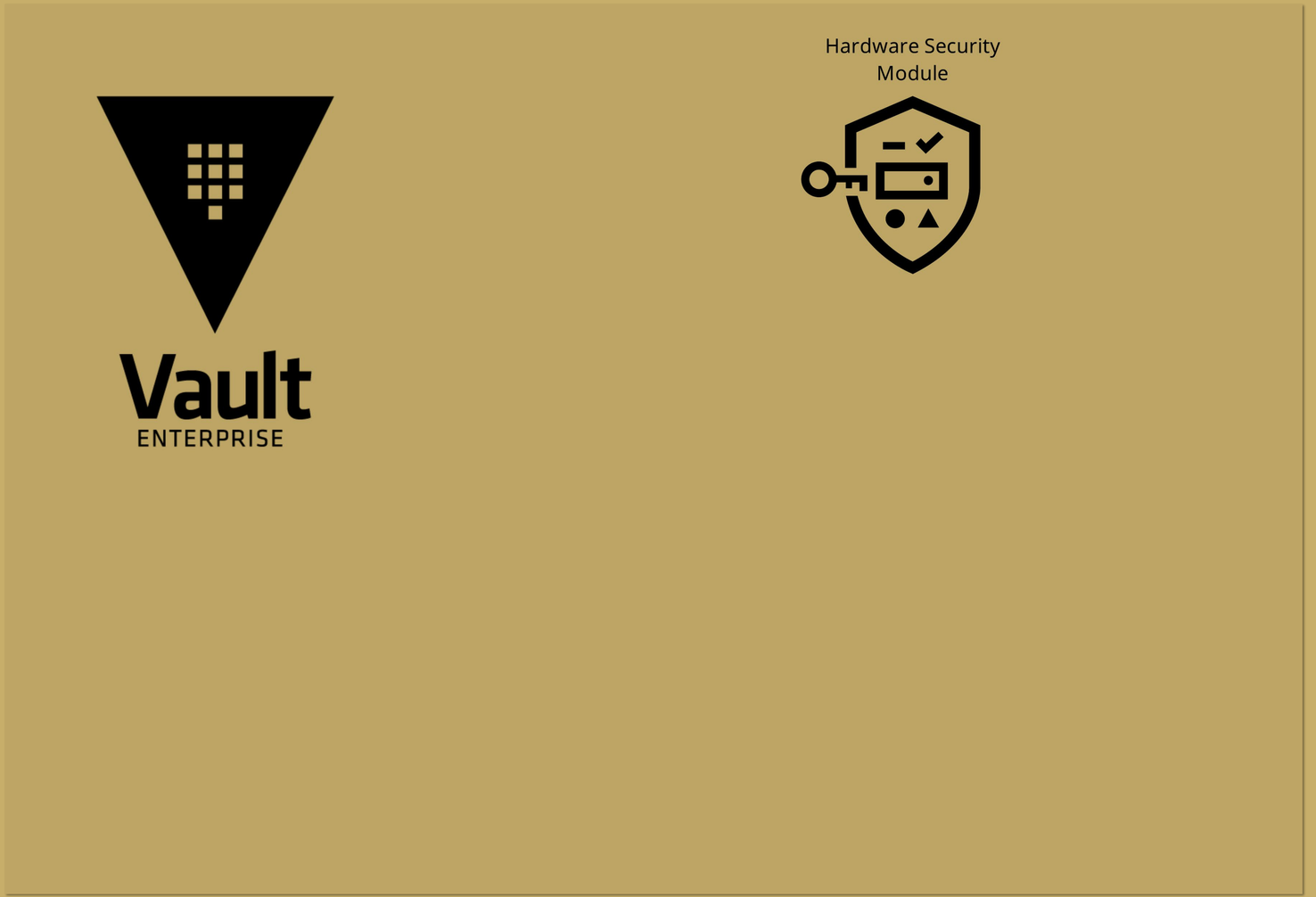
- Erfordert mindestens HashiCorp Vault Enterprise Plus
- HSM muss PKCS#11-Standard unterstützen (Interfaces entsprechend Version 2.20+, Integration Libraries für Linux auf amd64)

1. Initialisation

Comment se déroule l'initialisation en pratique ?

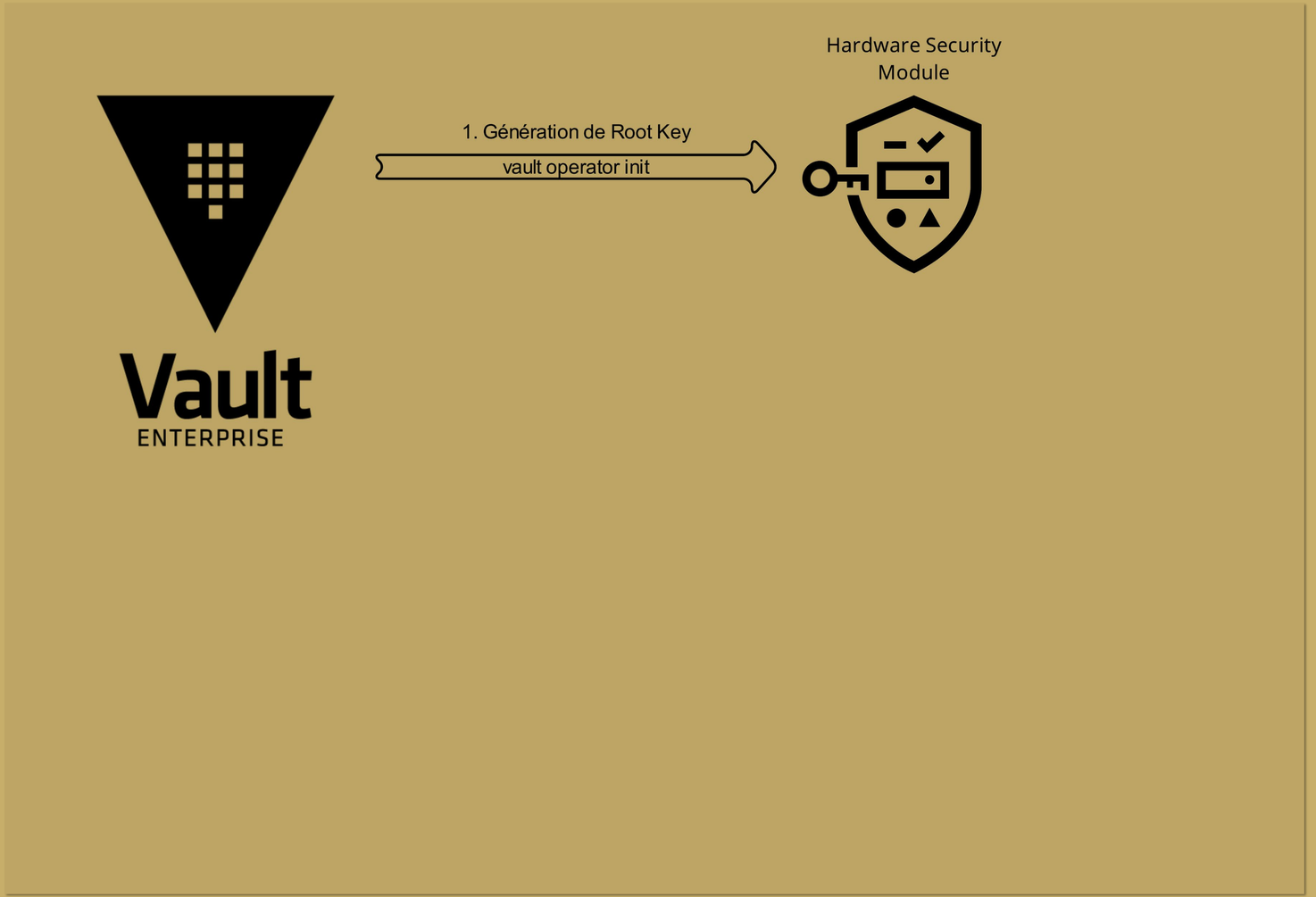
1. Initialisation

Étape 1:



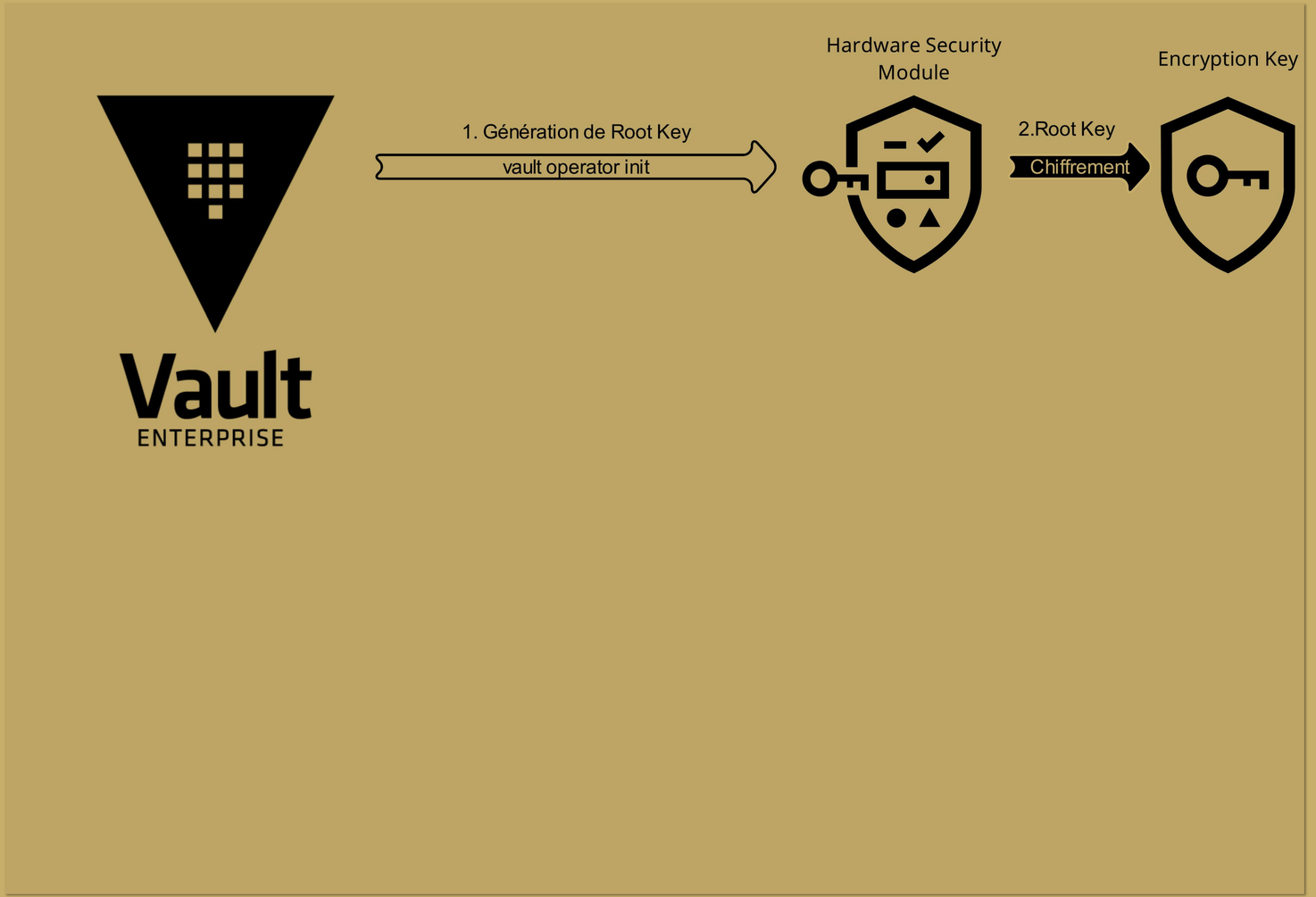
1. Initialisation

Étape 2:



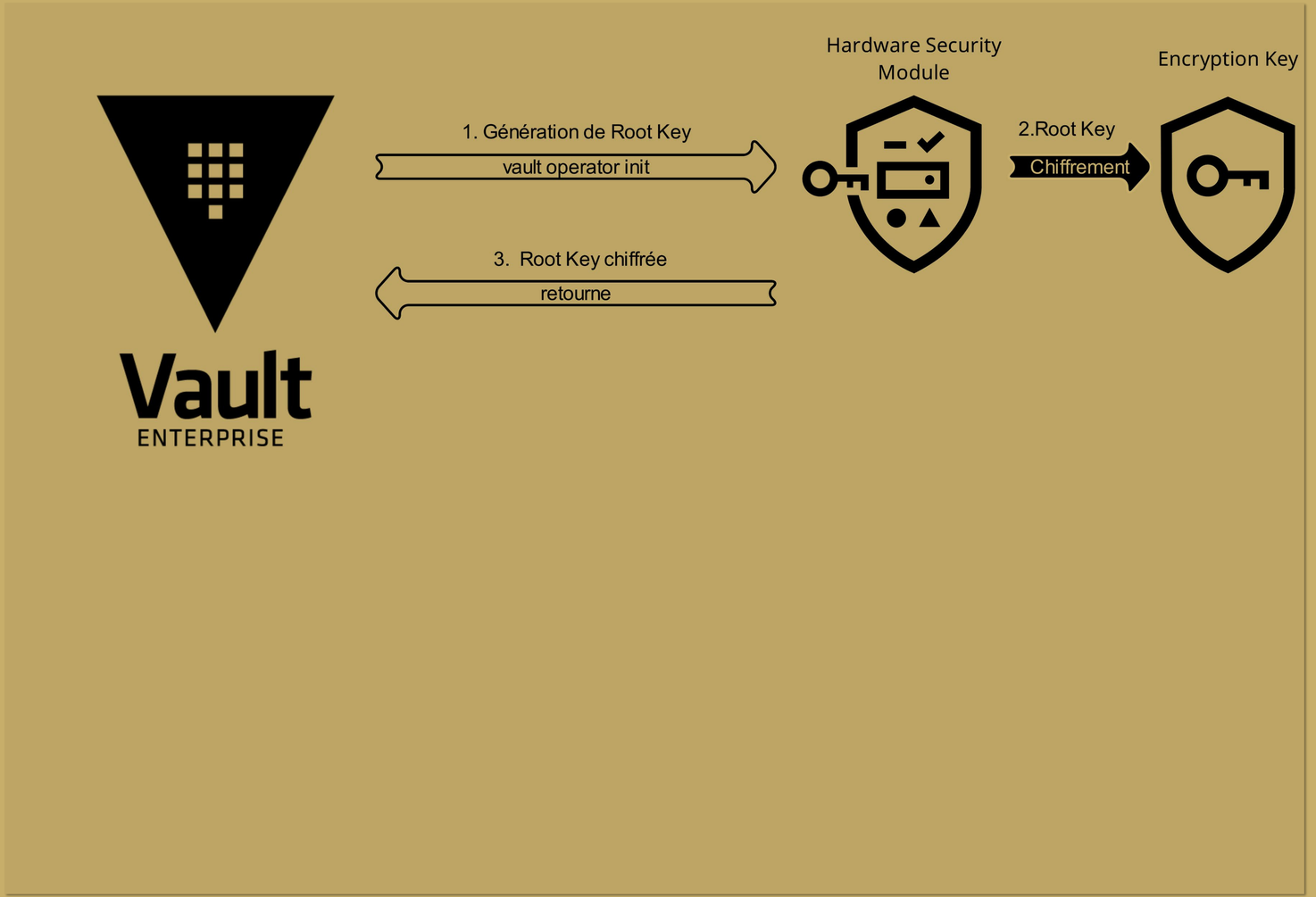
1. Initialisation

Étape 3:



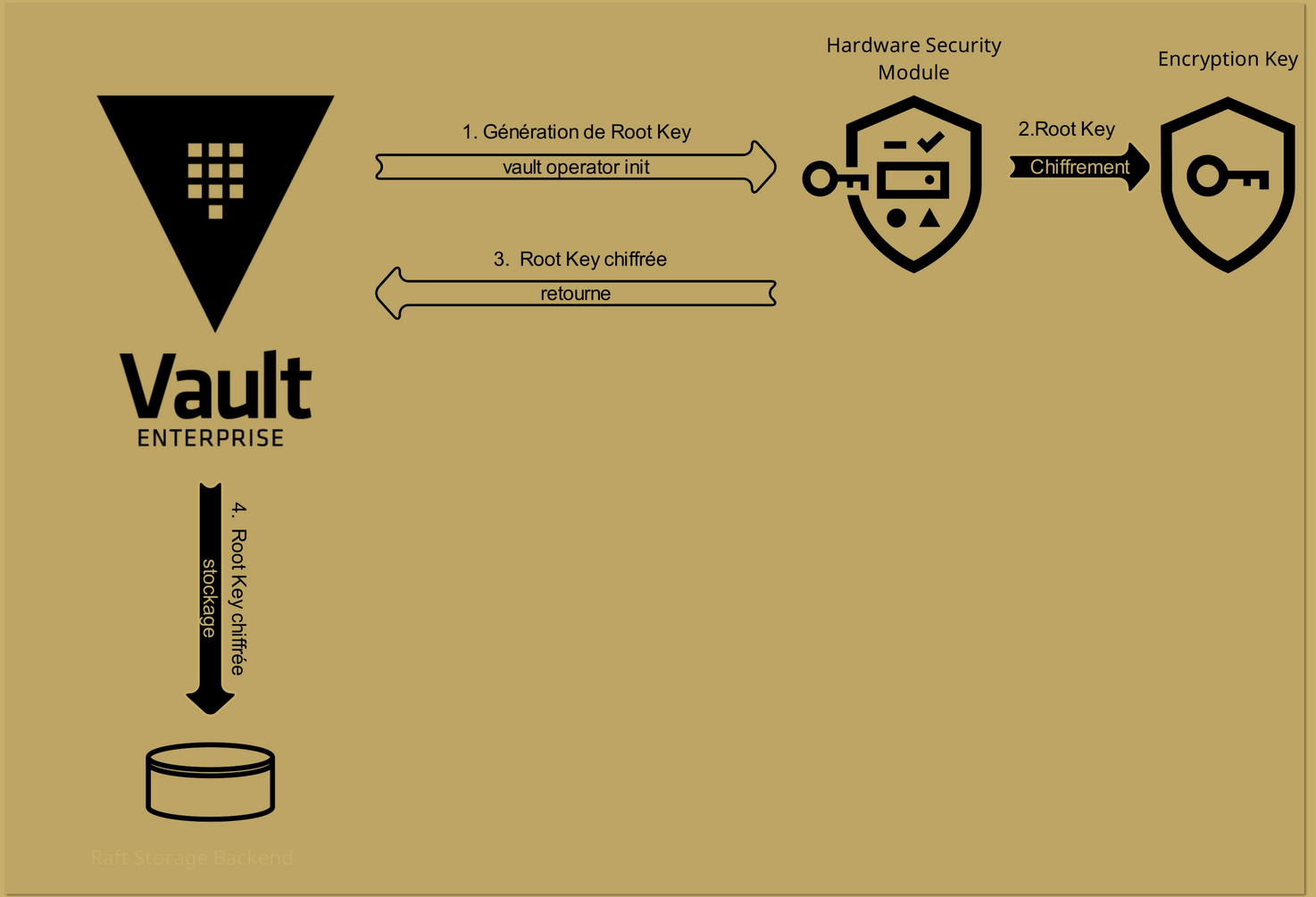
1. Initialisation

Étape 4:



1. Initialisation

Étape 5:



Démonstration

Point important #1

:Configuration minimale (avec HSM) de Vault avant la première mise en service

Point important #2

:Initialisation avec HSM via *vault operator init*

Point important #3 :

Nous observons un Auto-Unseal

Preuve de concept

Test Case #1

L'accès aux secrets sans Auto-Unseal HSM préalable *ne doit pas* être possible.

Test Case #2

Le déverrouillage manuel avec les Recovery Key Shares ***ne doit pas*** fonctionner.

Test Case #3

Vault ***ne doit pas*** démarrer sans le HSM.

Proof-of-Concept

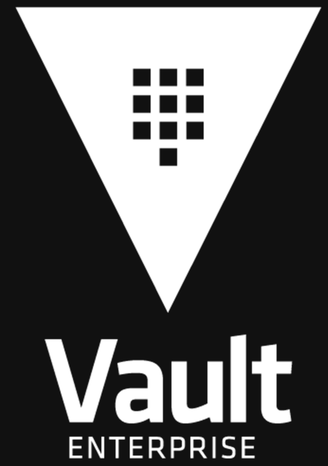
Test Case #1

L'accès aux secrets sans Auto-Unseal HSM préalable ***ne doit pas*** être possible.

Proof-of-Concept

Test Case #2

Le déverrouillage manuel avec les Recovery Key Shares ***ne doit pas*** fonctionner.



Proof-of-Concept

Test Case #3

Vault ***ne doit pas*** démarrer sans le HSM.

Preuve de concept

Test Case #1

L'accès aux secrets sans Auto-Unseal HSM préalable *ne doit pas* être possible.

Test Case #2

Le déverrouillage manuel avec les Recovery Key Shares ***ne doit pas*** fonctionner.

Test Case #3

Vault ***ne doit pas*** démarrer sans le HSM.

Merci !

ICT.TECHNOLOGY

INFRASTRUCTURE · CLOUD · TRANSITION

https://ict.technology