HSM Auto-Unseal

ICT.TECHNOLOGY
INFRASTRUCTURE · CLOUD · TRANSITION

Montag, 6. Januar 2025

Was ist ein HSM?

Ein Hardware Security Module (HSM) ist:

- Ein netzwerkbasiertes Gerät (oder eine in einem Server verbaute PCI-Karte), welches Geheimnisse und Schlüssel sicher speichert
- Ein gegen unbefugten physikalischen Zugriff geschütztes Gerät (tamper resistance)
- Teuer.

Wo findet man HSMs?

Man kann sie finden:

- On-Premise bei Unternehmen, die hohe Anforderungen an die Sicherheit stellen (Behörden, Banken und Kreditkartenausgeber, Versicherungen, Krankenhäuser, usw.)

- Bei Cloud Providern, zum Beispiel:

  - Oracle Cloud Infrastructure (OCI Vault), sowohl softwarebasiert (sehr preiswert), als Hardwarepartition auf einem Shared HSM (teuer) oder dedicated HSM (sehr teuer)
  - Amazon Webservices: AWS KMS als Shared HSM (teuer), oder AWS CloudHSM als dedicated HSM (extrem teuer)
  - Manche Hersteller bieten ebenfalls cloudbasierte HSM-Lösungen an

Vault und HSMs

- Vault Root Keys im HSM speichern
- Auto-Unseal mit im HSM gespeichertem Key
- Seal Wrapping
- FIPS 140-2 Compliance (optional, seit Vault 1.10)
- Verbesserte Zufallswerte durch Entropy Augmentation von externem kryptografischen Modul

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. Initialisierung

Wie läuft die Initialisierung in der Praxis ab?

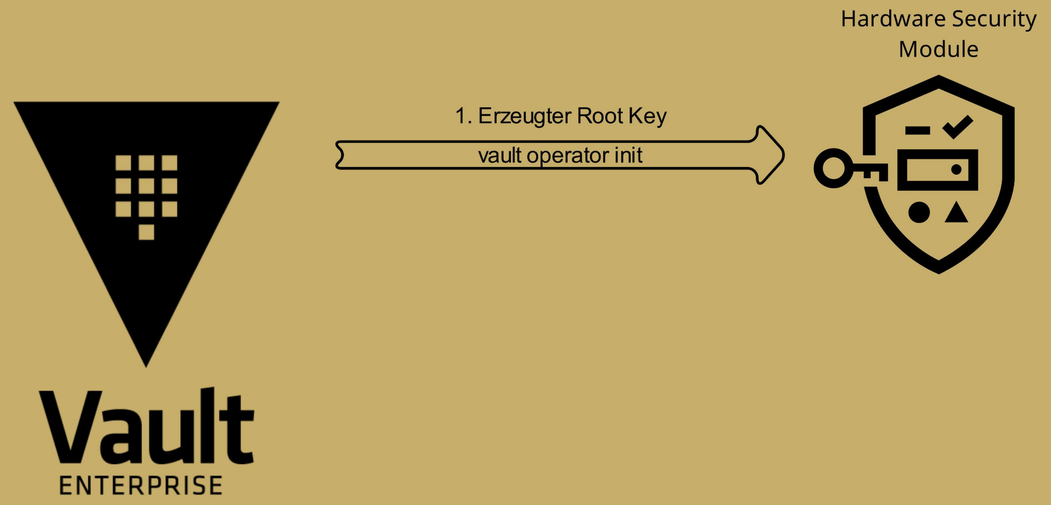
1. Initialisierung

Schritt 1:

Hardware Security Module

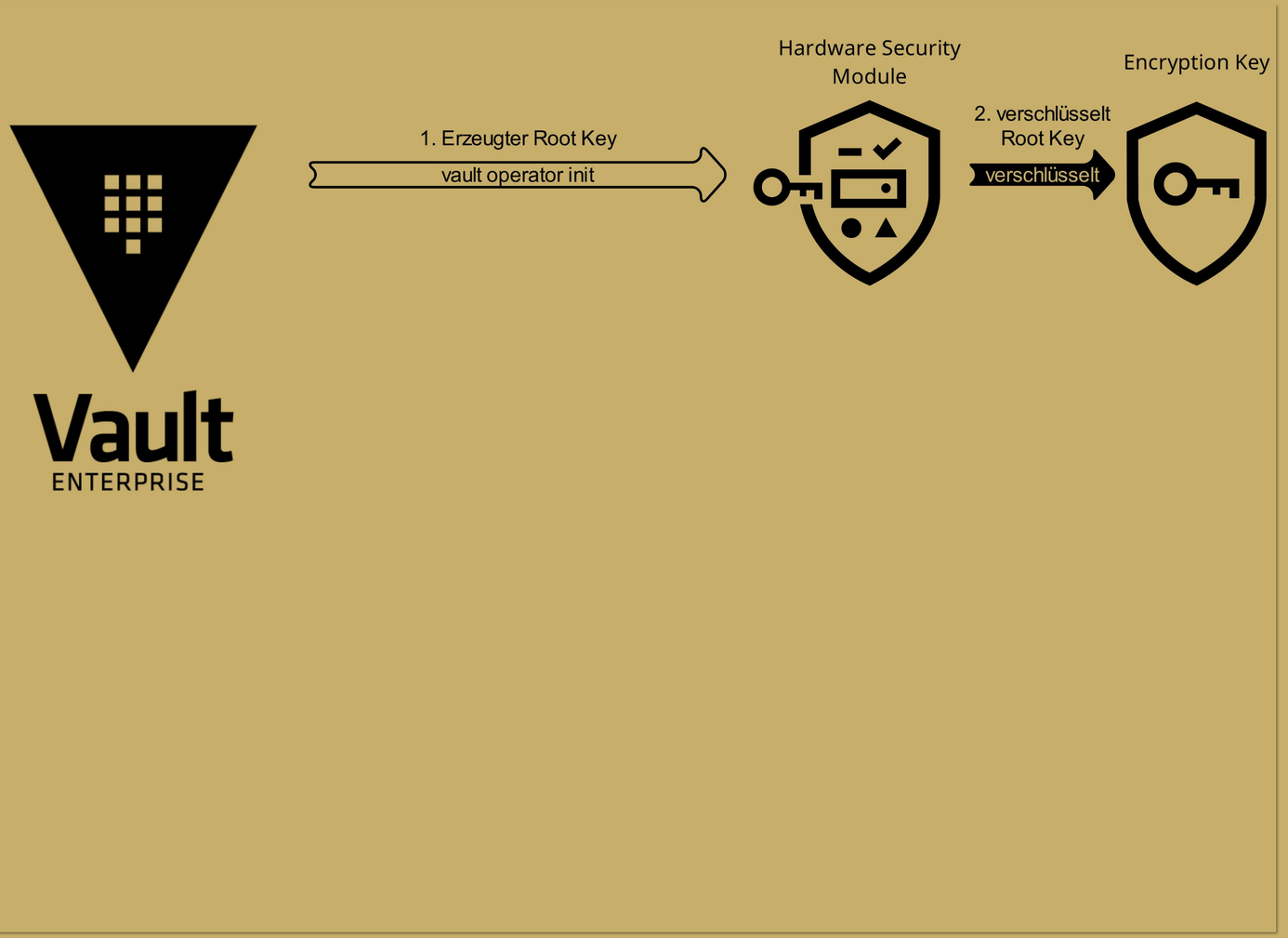
1. Initialisierung

Schritt 2:



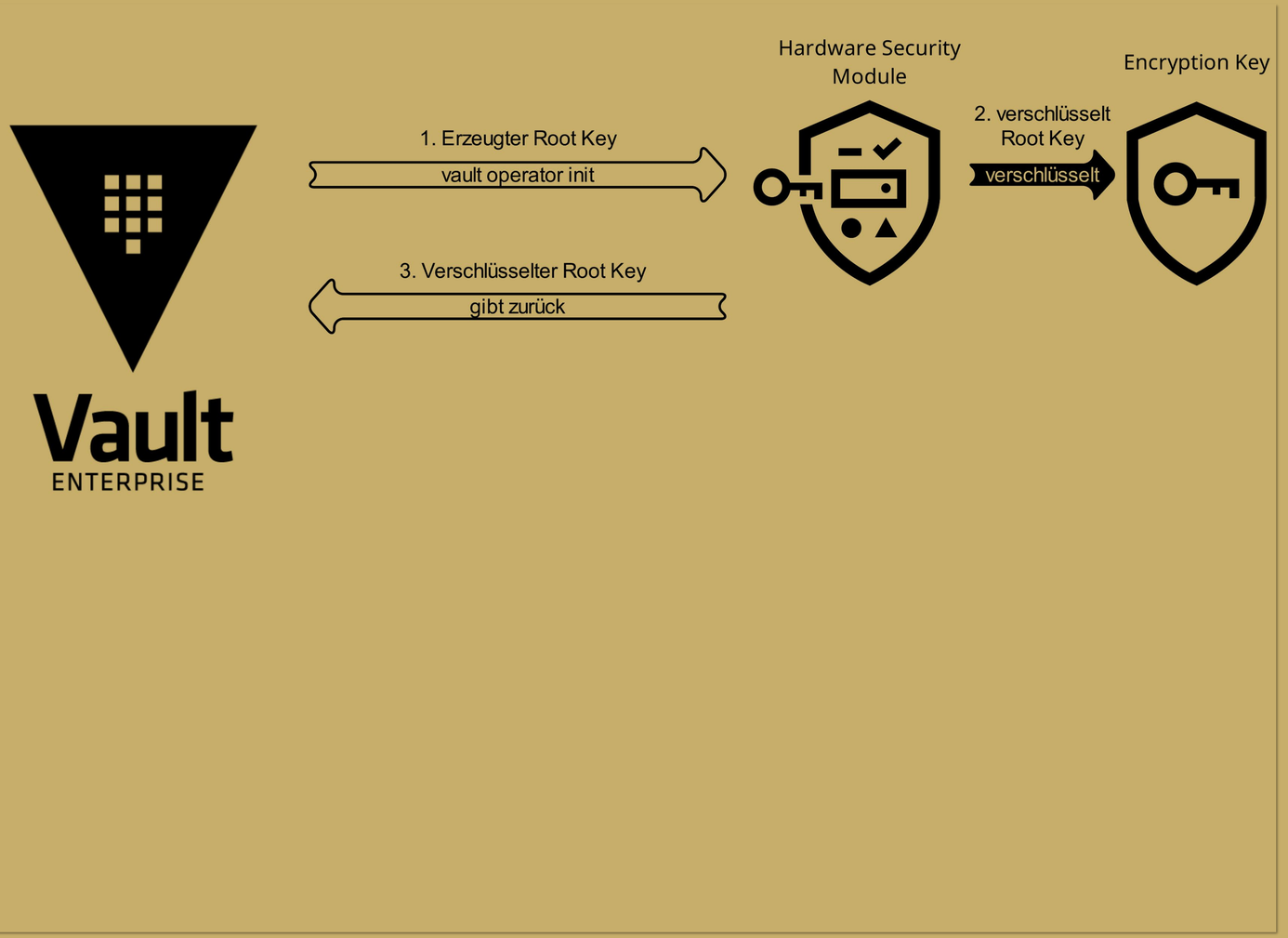
1. Initialisierung

Schritt 3:



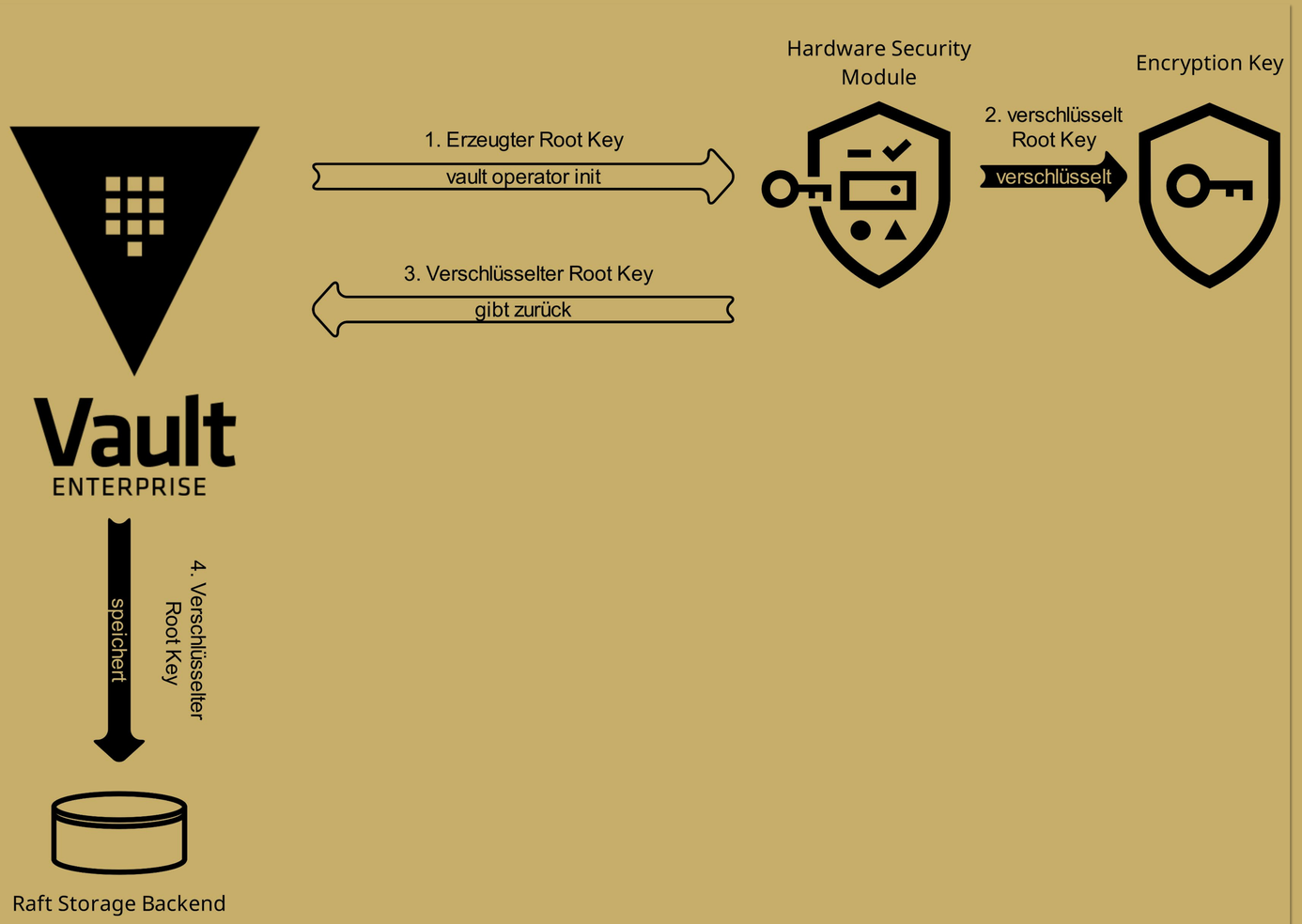
1. Initialisierung

Schritt 4:



1. Initialisierung

Schritt 5:



Demo

Highlight #1

Minimal-Konfiguration (mit HSM) von Vault vor erster Inbetriebnahme

Highlight #2

Initialisierung gegen HSM mittels *vault operator init*

Highlight #3

Wir erleben einen Auto-Unseal

Proof-of-Concept

Test Case #1

Zugriff auf Secrets ohne vorheriges HSM Auto-Unseal darf ***nicht*** möglich sein.

Test Case #2

Manueller Unseal mit Recovery Key Shares darf ***nicht*** funktionieren.

Test Case #3

Ohne das HSM darf Vault ***nicht*** starten.

Proof-of-Concept

Test Case #1

Zugriff auf Secrets ohne vorheriges HSM Auto-Unseal darf ***nicht*** möglich sein.

Proof-of-Concept

Test Case #2

Manueller Unseal mit Recovery Key
Shares darf ***nicht*** funktionieren.

Proof-of-Concept

Test Case #3

Ohne das HSM darf Vault ***nicht*** starten.

Proof-of-Concept

Test Case #1

Zugriff auf Secrets ohne vorheriges HSM Auto-Unseal darf ***nicht*** möglich sein.

Test Case #2

Manueller Unseal mit Recovery Key Shares darf ***nicht*** funktionieren.

Test Case #3

Ohne das HSM darf Vault ***nicht*** starten.

DANKE!

ICT.TECHNOLOGY

INFRASTRUCTURE · CLOUD · TRANSITION

https://ict.technology