Vault

CERTIFIED
OPERATIONS
PROFESSIONAL

Describe the Benefits of Auto Unsealing with HSM

What is an HSM?

- An HSM is a network-based physical device that can safeguard and manage digital keys
- These keys can be used for encryption and decryption functions, digital signatures, strong authentication, or other functions
- HSMs commonly have tamper resistance – meaning that detection of tampering could invoke a response such as deleting the keys so nobody can access them

- Large enterprise customers often deploy dedicated physical HSMs in a traditional data center
- Public cloud providers offer access to dedicated or shared HSM services as well.
  - AWS CloudHSM or Azure Dedicated HSM is an HSM service where the HSM is dedicated to a single customer
  - AWS KMS is an example of a shared HSM service, where multiple customers may use a service that is backed by the same HSM

General HSM Support

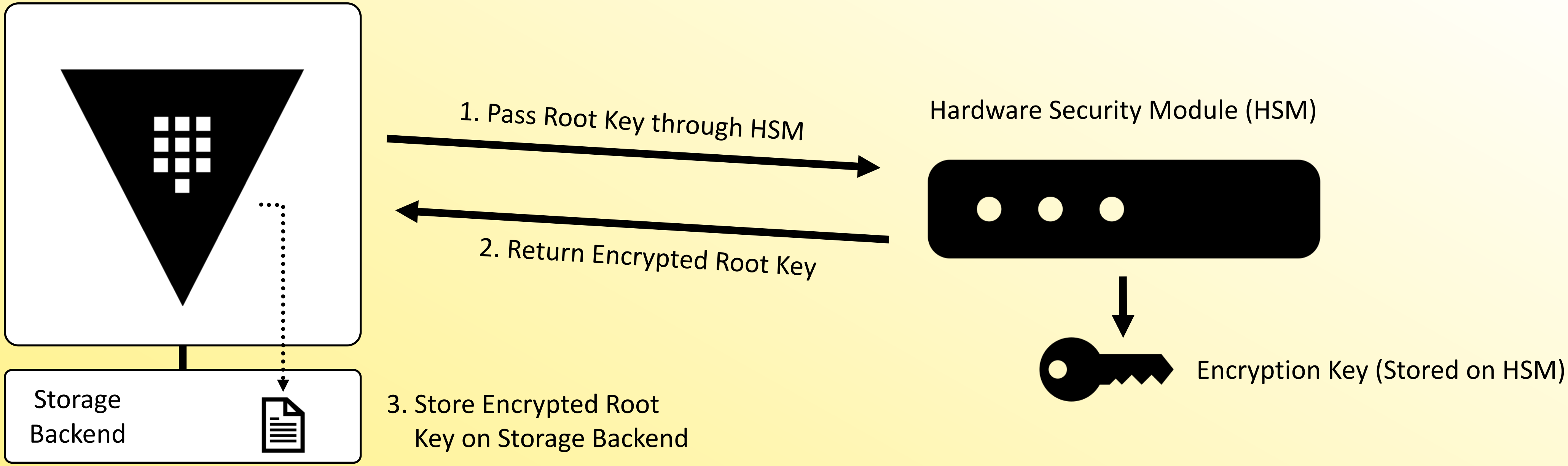
Vault Enterprise has multiple integrations with an HSM:

- Protect root key by using HSM to encrypt/decrypt root key
- Auto unseal Vault by storing wrapped key on local storage
- Seal wrapping to provide extra layer of protection for FIPS 140-2 compliance
- Entropy Augmentation to generate randomness for cryptographic operations

Requires HSM that supports PKCS11 standard

Initializing Vault

Vault
CERTIFIED
OPERATIONS
PROFESSIONAL



1. Pass Root Key through HSM

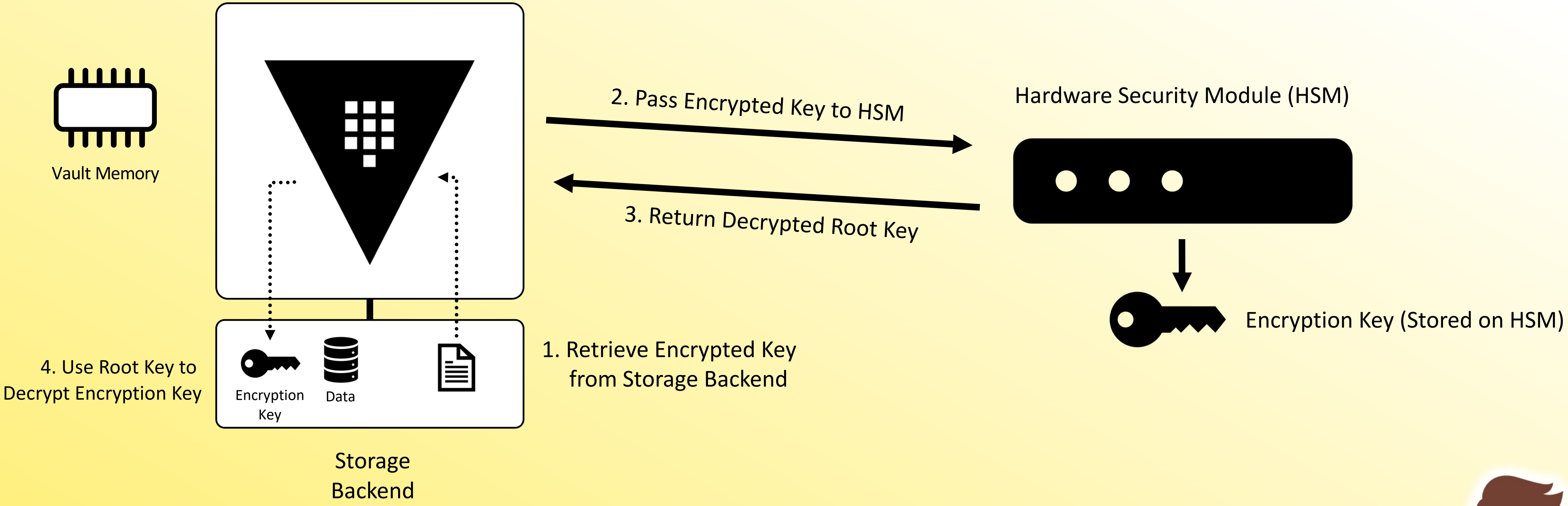
2. Return Encrypted Root Key

3. Store Encrypted Root Key on Storage Backend

Hardware Security Module (HSM)

Encryption Key (Stored on HSM)

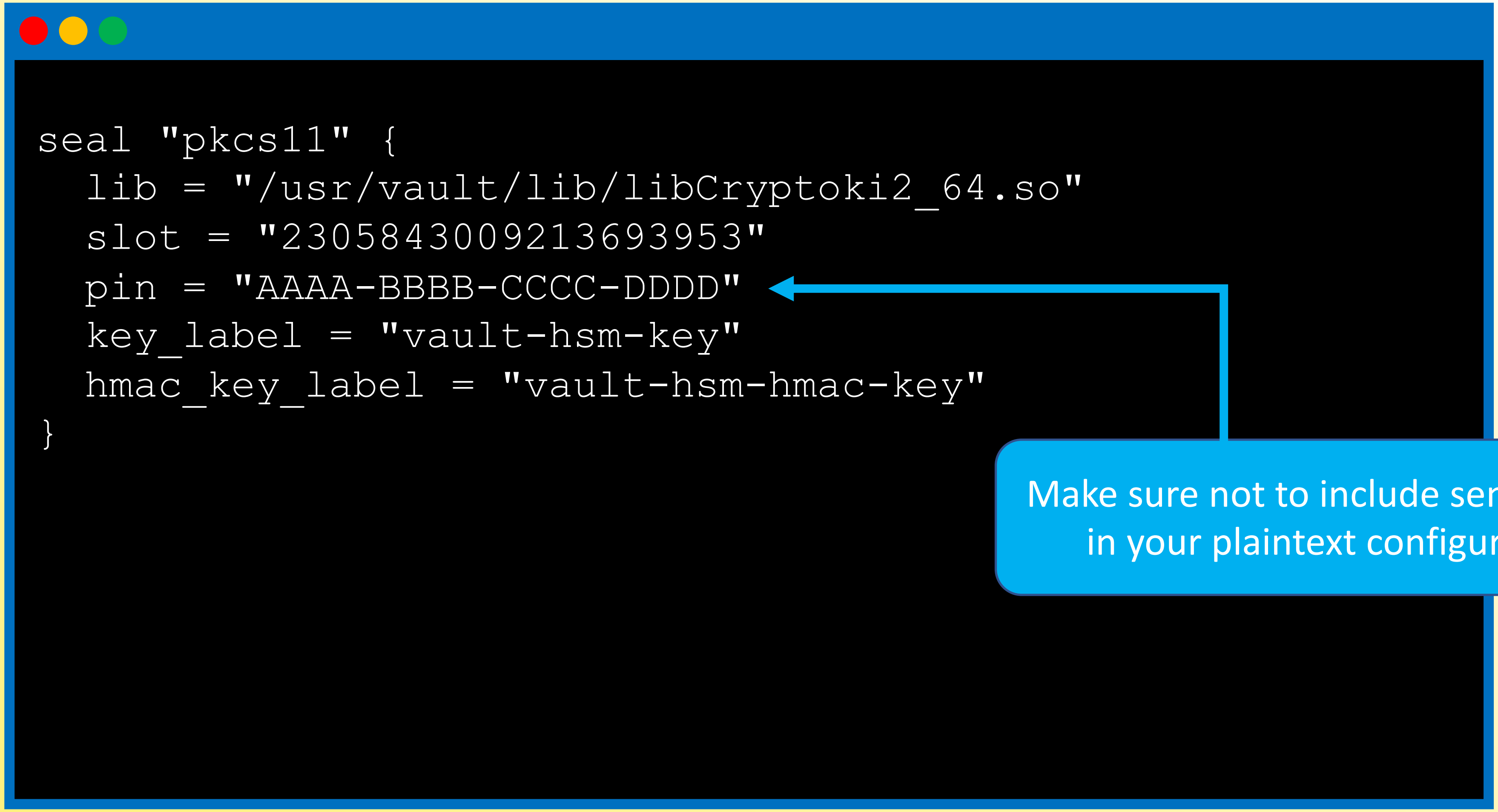
Auto Unseal with HSM



Vault Memory
2. Pass Encrypted Key to HSM
Hardware Security Module (HSM)
3. Return Decrypted Root Key
Encryption Key (Stored on HSM)
4. Use Root Key to Decrypt Encryption Key
Encryption Key
Data
1. Retrieve Encrypted Key from Storage Backend
Storage Backend

Configuration

Vault CERTIFIED OPERATIONS PROFESSIONAL



```
seal "pkcs11" {
  lib = "/usr/vault/lib/libCryptoki2_64.so"
  slot = "2305843009213693953"
  pin = "AAAA-BBBB-CCCC-DDDD"
  key_label = "vault-hsm-key"
  hmac_key_label = "vault-hsm-hmac-key"
}
```

Make sure not to include sensitive values in your plaintext configuration file

pkcs11 Environment Variables

- VAULT_HSM_LIB
- VAULT_HSM_TYPE
- VAULT_HSM_SLOT
- VAULT_HSM_TOKEN_LABEL
- VAULT_HSM_PIN
- VAULT_HSM_KEY_LABEL
- VAULT_HSM_DEFAULT_KEY_LABEL
- VAULT_HSM_KEY_ID
- VAULT_HSM_HMAC_KEY_LABEL
- VAULT_HSM_HMAC_DEFAULT_KEY_LABEL
- VAULT_HSM_HMAC_KEY_ID
- VAULT_HSM_MECHANISM
- VAULT_HSM_HMAC_MECHANISM
- VAULT_HSM_GENERATE_KEY
- VAULT_HSM_RSA_ENCRYPT_LOCAL
- VAULT_HSM_RSA_OAEP_HASH
- VAULT_HSM_FORCE_RW_SESSION

You do NOT need to memorize these for the exam