Vault

Vault and HSM Integration

TAM Workshop
Peter Souter

What is an HSM?

Hardware Security Module

“A hardware security module (HSM) is a secure physical device designed to generate [with a TRNG], store, and protect digital, high-value cryptographic keys. It is a secure crypto-processor that often comes in the form of a plug-in card with built-in tamper protection”

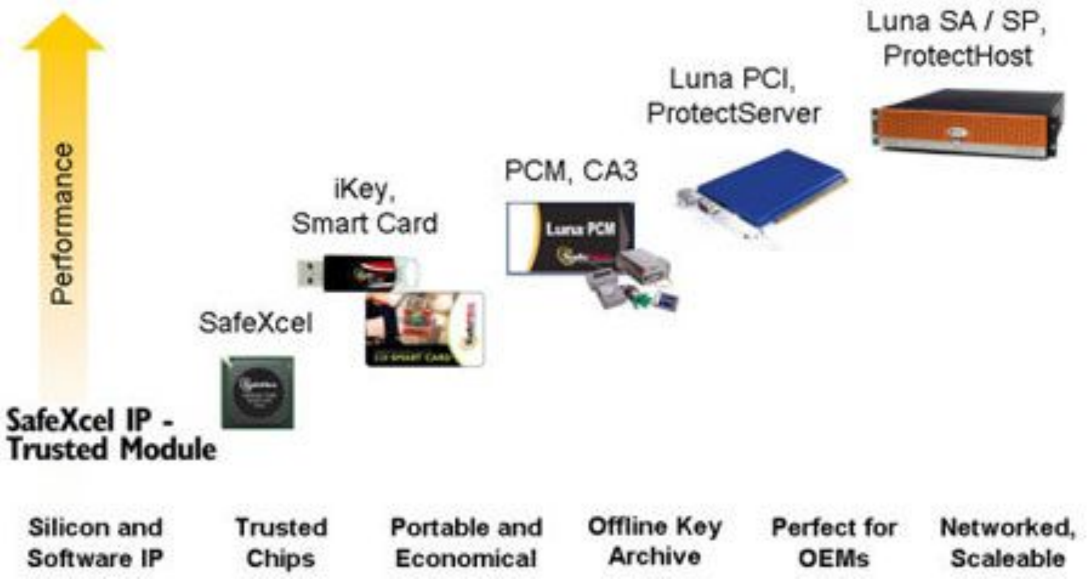
https://www.f5.com/pdf/solution-profiles/hardware-security-module-sp.pdf

HSM’s from the big to the small…

https://www.zdnet.com/article/yubico-launches-yubihsm-2-the-smallest-cheapest-hardware-security-module-hsm/

https://dymarjaya.co.id/product/safenet-luna-network-hsm/

HSM's come in many varieties...



http://www.pericosecurity.com/hardware-security-module-hsm.75162.en.html

Does an HSM replace Vault?

Or vice-versa?

“Vault doesn't replace an HSM. Instead, they can be complementary; a compliant HSM can protect Vault's master key to help Vault comply with regulatory requirements, and Vault can provide easy client APIs for tasks such as encryption and decryption.

For many companies' security requirements, Vault alone is enough. For companies that can afford an HSM or with specific regulatory requirements, it can be used with Vault to get the best of both worlds”

https://www.vaultproject.io/docs/vs/hsm.html#vault-vs-hsms

What are the features of Vault and HSM integration?

1. Master Key Wrapping and Automatic Unsealing
2. Seal Wrapping
3. Entropy Augmentation

Master Key Wrapping and Automatic Unsealing

What?

Vault protects its master key and transits it through the HSM for encryption rather than splitting into key shares

Why?

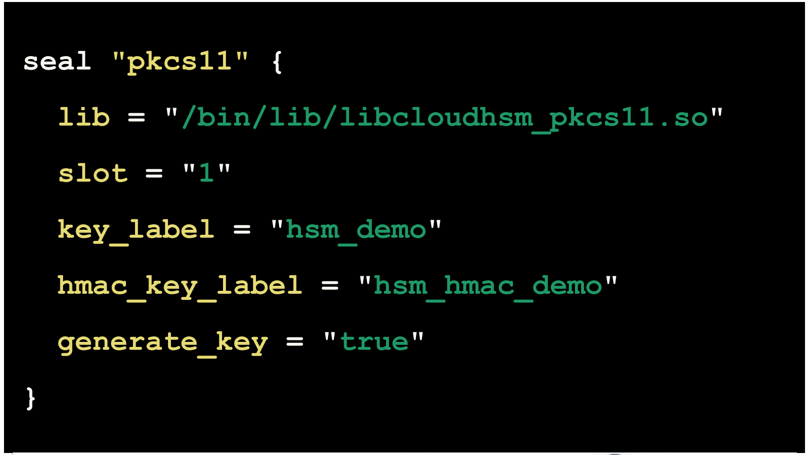
In some large organizations, there is a fair amount of complexity in designating key officers, who might be available to unseal Vault installations as the most common pattern is to deploy Vault immutably. As such automating unseal using an HSM provides a simplified yet secure way of unsealing Vault nodes as they get deployed.

Vault pulls its encrypted master key from storage and transits it through the HSM for decryption via PKCS #11 API. Once the master key is decrypted, Vault uses the master key to decrypt the storage key to resume with Vault operations.

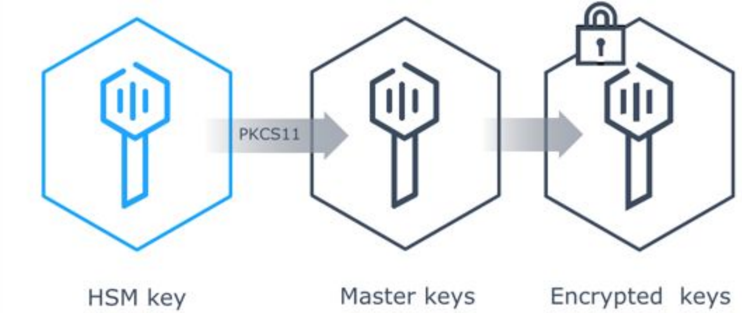
Links

https://www.vaultproject.io/docs/configuration/seal/pkcs11.html
https://www.vaultproject.io/docs/enterprise/hsm/behavior.html#unseal-master-key
https://learn.hashicorp.com/vault/operations/ops-seal-wrap

How?



```
seal "pkcs11" {
  lib = "/bin/lib/libcloudhsm_pkcs11.so"
  slot = "1"
  key_label = "hsm_demo"
  hmac_key_label = "hsm_hmac_demo"
  generate_key = "true"
}
```



Seal Wrapping

What?

Vault wraps your secrets with an extra layer of encryption leveraging the HSM encryption and decryption.

Why?

We wrap the data and HMAC the wrapped data with a key in the HSM. This allows us to detect tampering of the encrypted wrapped data

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. Government computer security standard used to accredit cryptography modules.

Aside from doing business with U.S. government, an organization may care about FIPS which approves various cryptographic ciphers for hashing, signature, key exchange, and encryption for security.

Links

https://www.vaultproject.io/docs/enterprise/sealwrap/index.html
https://learn.hashicorp.com/vault/operations/ops-seal-wrap

How?

```
seal "pkcs11" {
  lib = "/bin/lib/libcloudhsm_pkcs11.so"
  slot = "1"
  key_label = "hsm_demo"
  hmac_key_label = "hsm_hmac_demo"
  generate_key = "true"
}
```

```
$ vault secrets enable -path=kv-seal-wrapped -seal-wrap
$ vault secrets list -detailed
Path               Plugin    Accessor        Seal Wrap
----               ------    --------        ----------
kv-seal-wrapped/   kv        kv_fe02767b     true
```

Entropy Augmentation

What?

Entropy augmentation enables Vault to sample entropy from an external cryptographic modules.

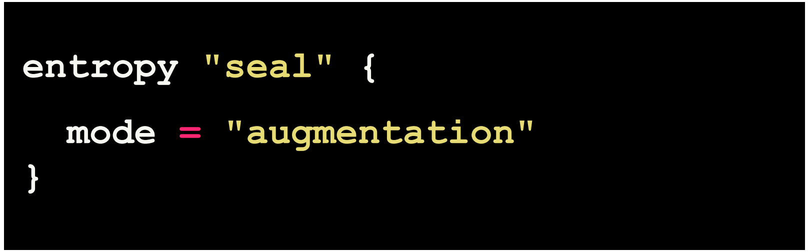
Why?

While the system entropy used by Vault is more than capable of operating in most threat models, there are some situations where additional entropy from hardware-based random number generators is desirable. For example, complying with regulations which require augmented entropy from external sources such as hardware true random number generators.

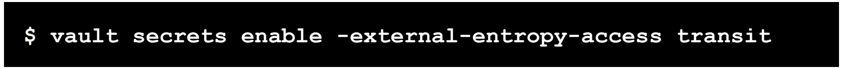
Links

https://www.vaultproject.io/docs/configuration/entropy-augmentation/index.html
https://www.vaultproject.io/docs/enterprise/entropy-augmentation/index.html
https://learn.hashicorp.com/vault/operations/hsm-entropy

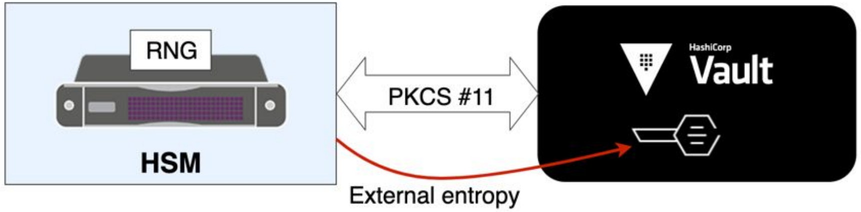
How?



```
entropy "seal" {
  mode = "augmentation"
}
```



```
$ vault secrets enable -external-entropy-access transit
```



Demo

HSM Autounseal with SoftHSM