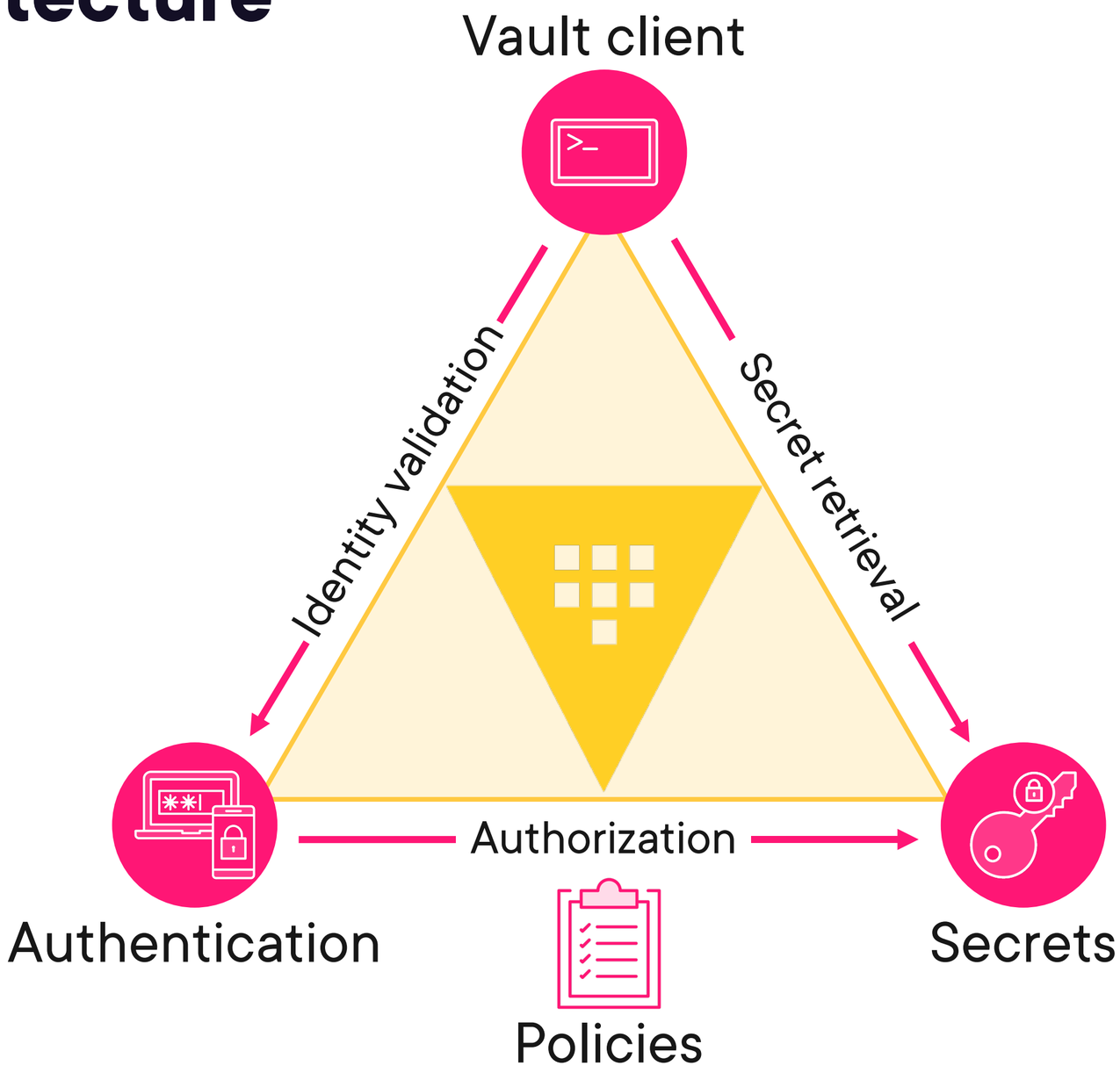
Vault Architecture Fundamentals for Vault Associate (003)

Vault Data Encryption

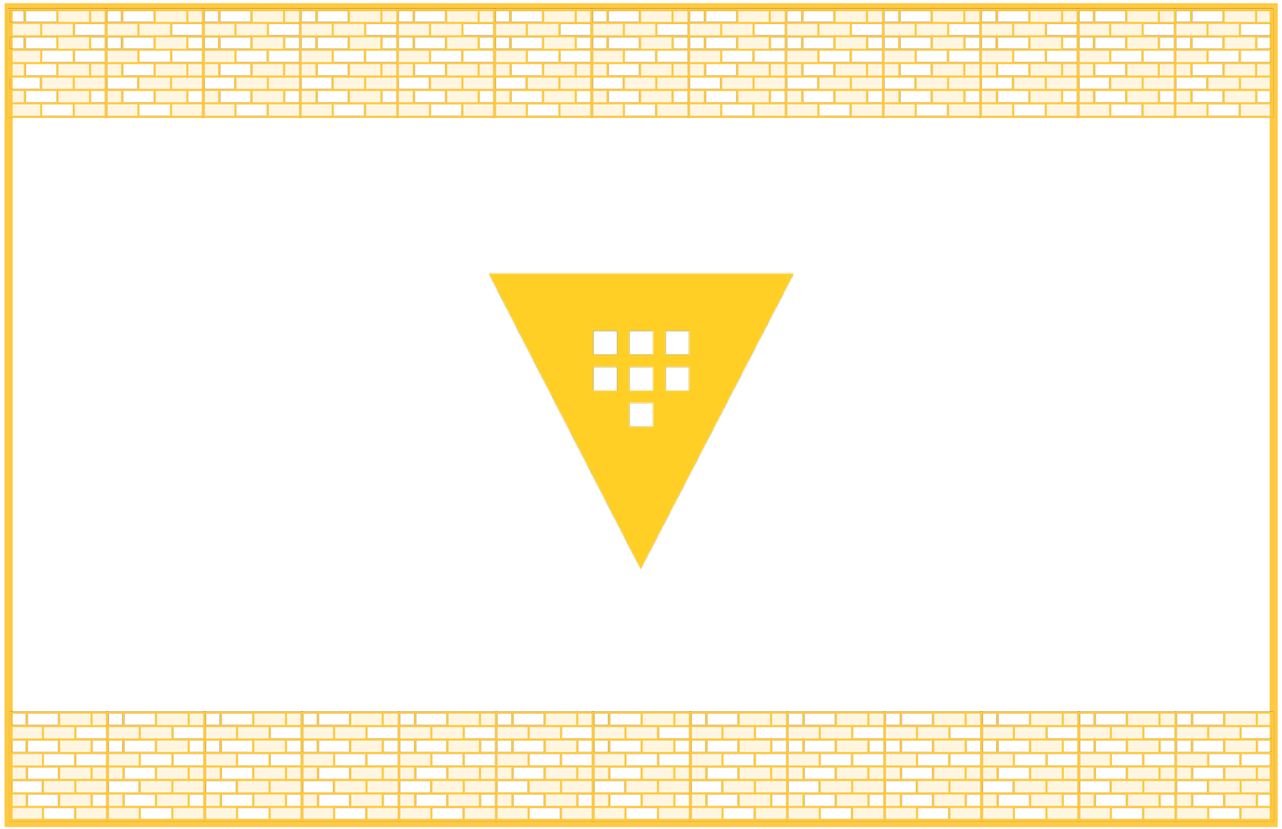
Ned Bellavance
HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

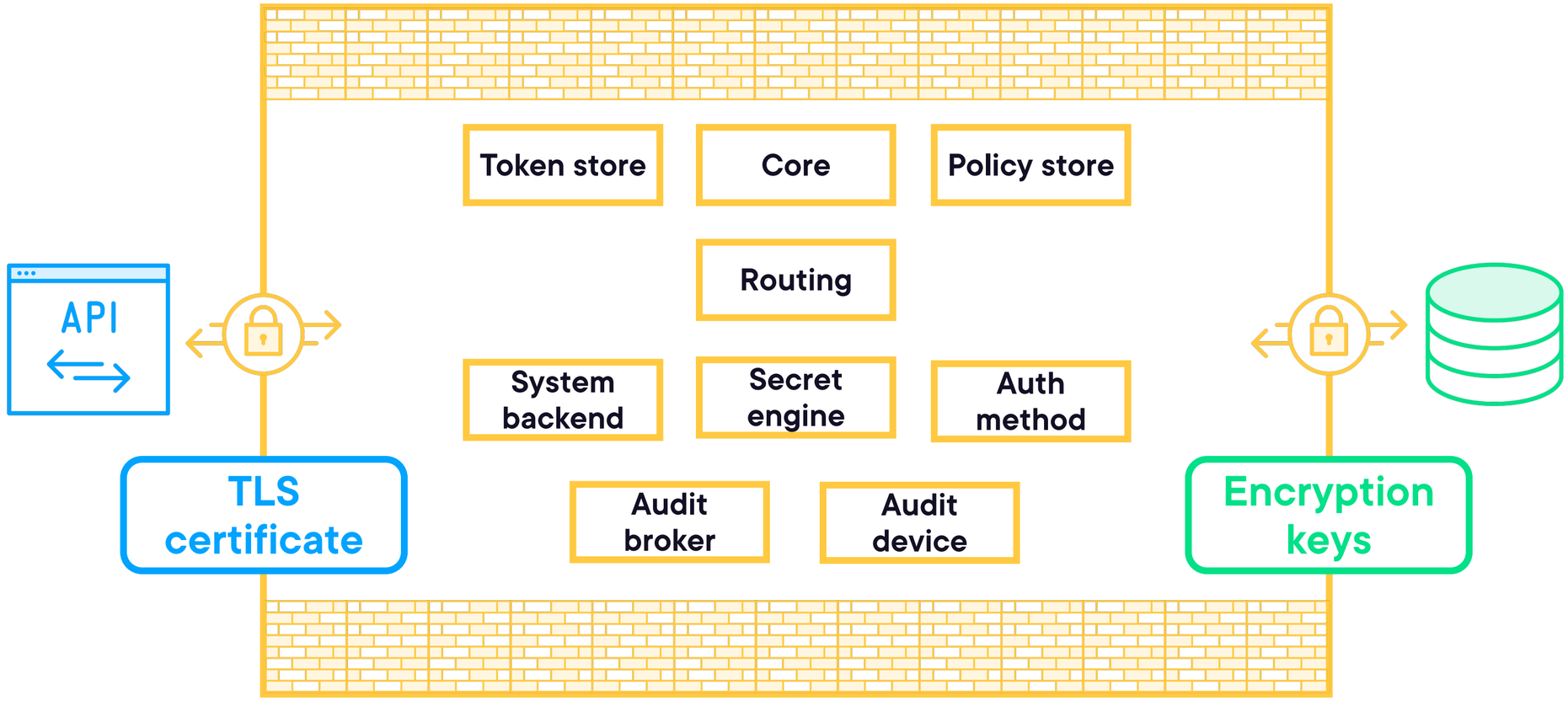
Vault Architecture



Vault Architecture

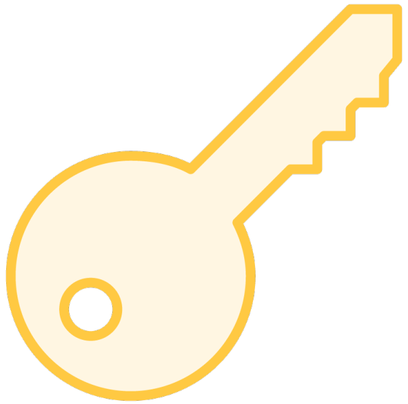


Vault Architecture

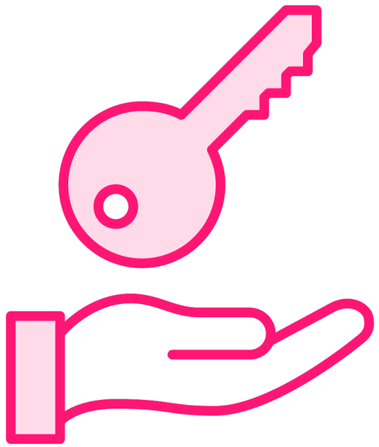


Encryption Keys

Encryption keys
Protect data written to storage
Stored on disk

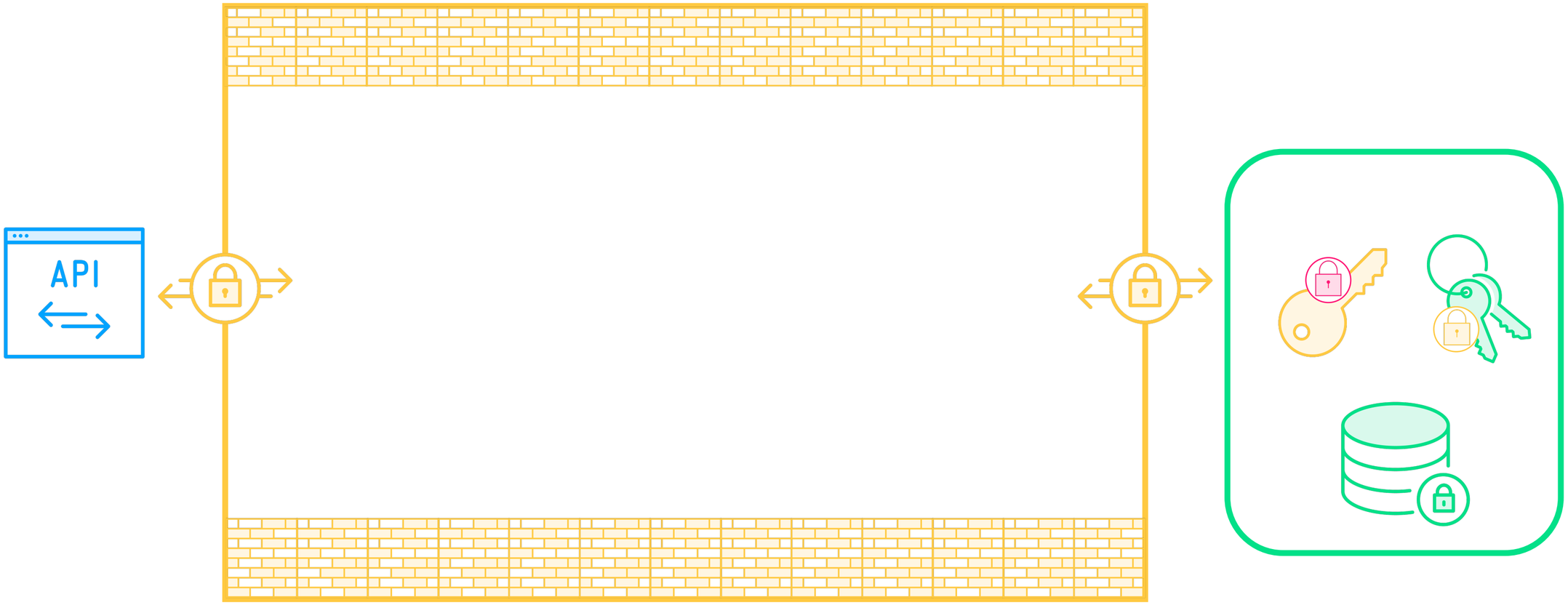


Root key
Protects encryption keys
Stored on disk

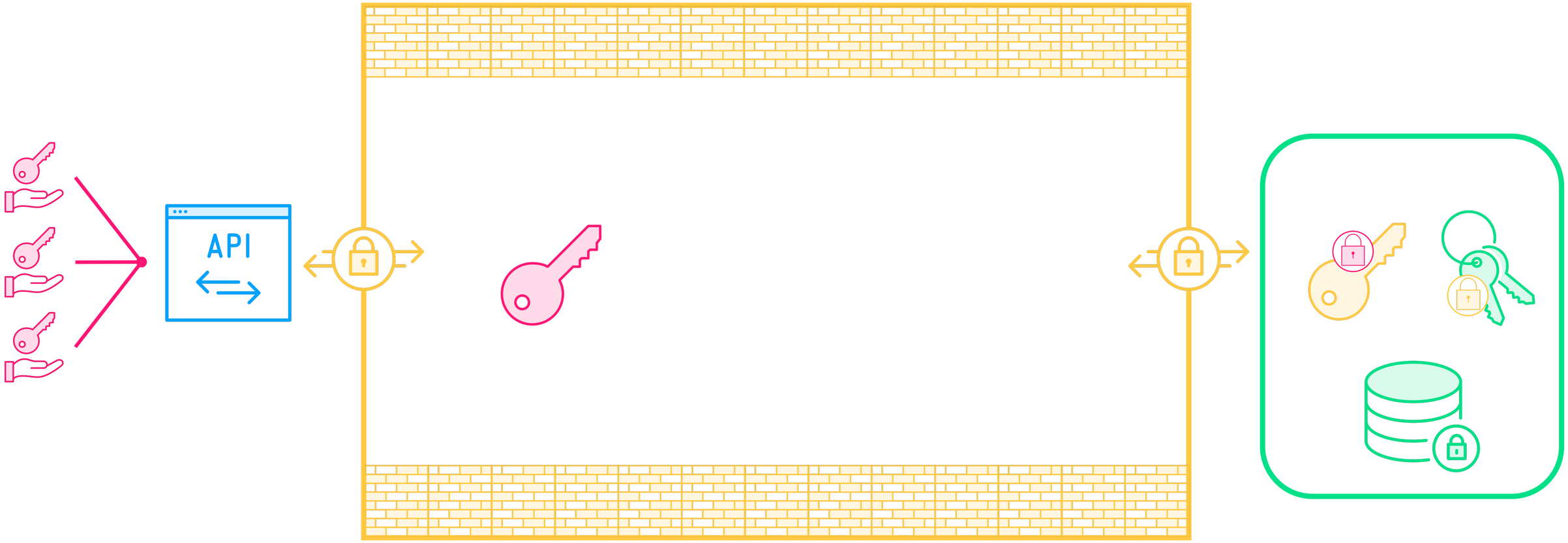


Unseal key
Protects root key
Stored externally

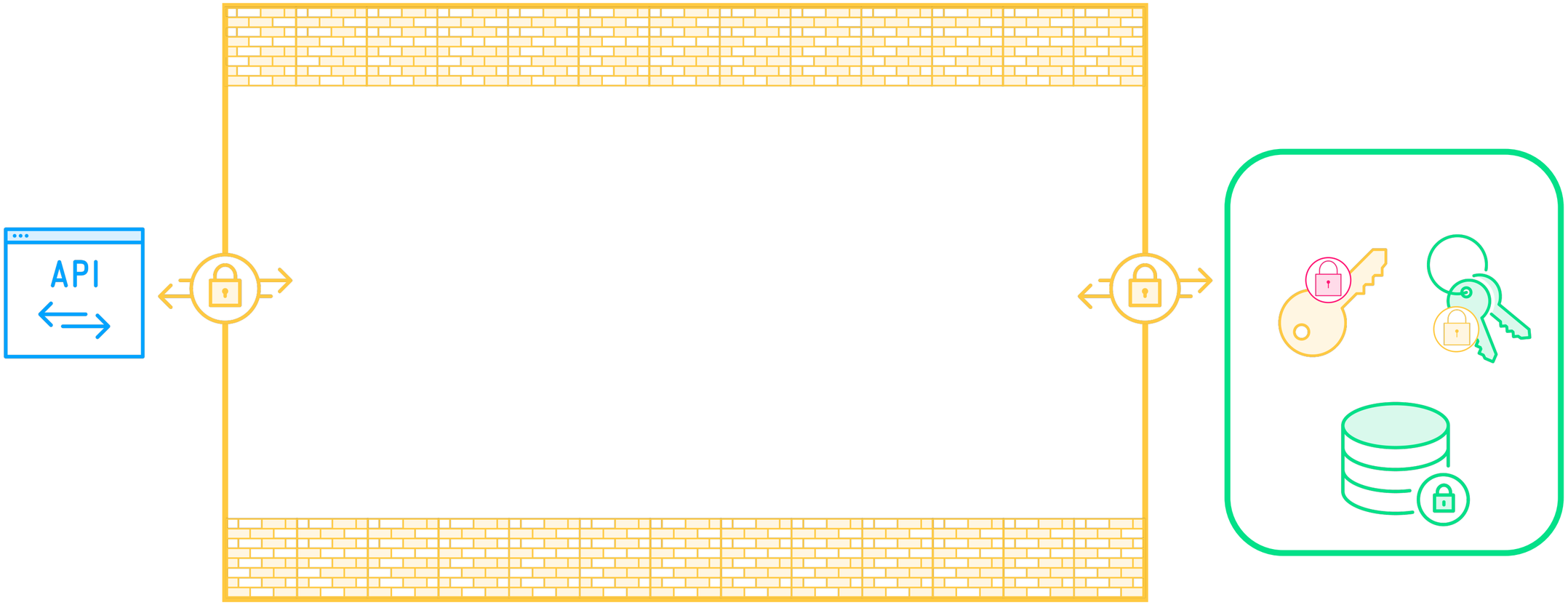
Unsealing Vault



Unsealing Vault



Unsealing Vault

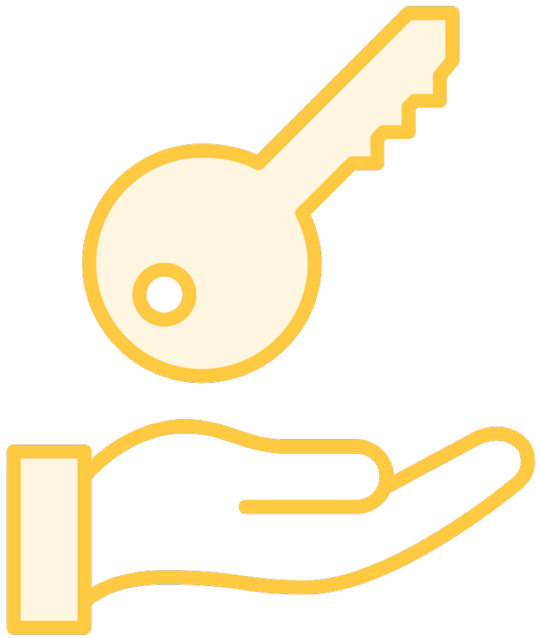


Seal Options

Shamir secret sharing

External KMS

Shamir Secret Sharing



Divide a cryptographic secret into shares

Reconstruct using a threshold of shares

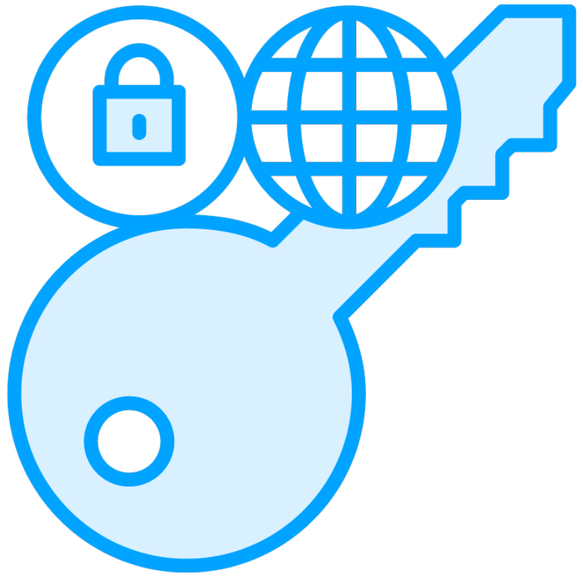
Unseal key constructed during initialization

- Set share count and threshold

Keys shares used for elevated actions

- Root tokens, new unseal key, DR and recovery tokens

External Key Management Service



Supports cloud KMS

- Azure Key Vault, AWS KMS, GCP Cloud KMS

Supports local KMS

- HSM or Transit engine

Uses asymmetric key on KMS

Automatic unsealing of Vault

Recovery keys created during initialization

If you lose access to the unseal key, you cannot recover your data from Vault

Initializing Vault

```
# Initialize vault with key shares
vault operator init [options]
vault operator init -key-shares=3 -key-threshold=2

# Response output
Unseal Key 1: FOtMzfM9dylemigqaqrMX5yYY3XKgRkuSPxLAPa+kwjC
Unseal Key 2: hOCZT1ImEl9rksusQoFOO0OZdAoZr4btlWDIzBuvI0hM
Unseal Key 3: NnNxIDQYCaFfSV8j2FMhGAChcRdhpUc4pumfasQ60MoY

Initial Root Token: hvs.Z0bzUKMKPdmtDq8Pp6jEqM54
```