Managing Encryption and Master Keys

Ned Bellavance
MICROSOFT AZURE MVP

@ned1313 | nedinthecloud.com

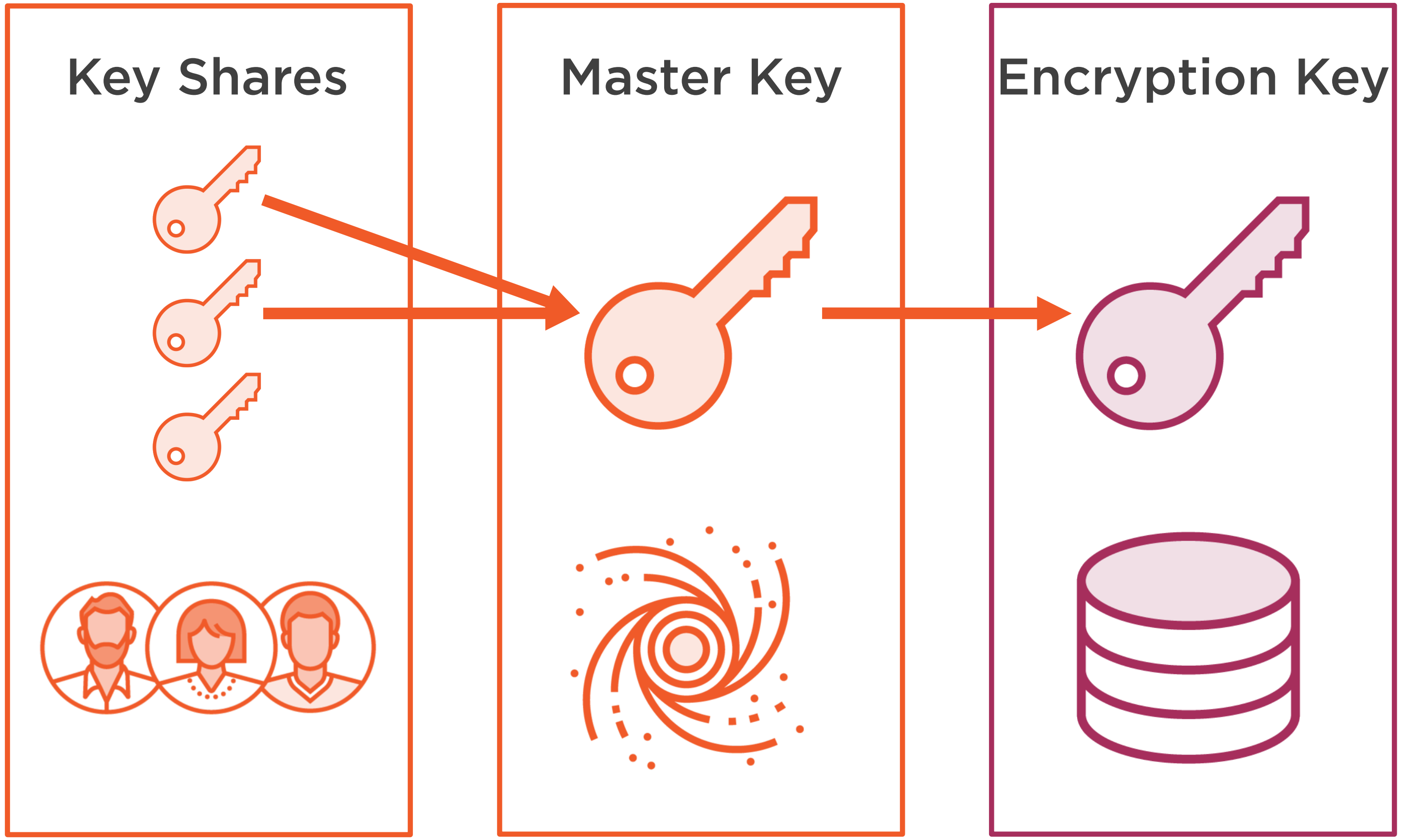
Overview

Managing the Vault seal

Root token best practices

Using auto unseal for Vault

Vault Seal



Master Key Options

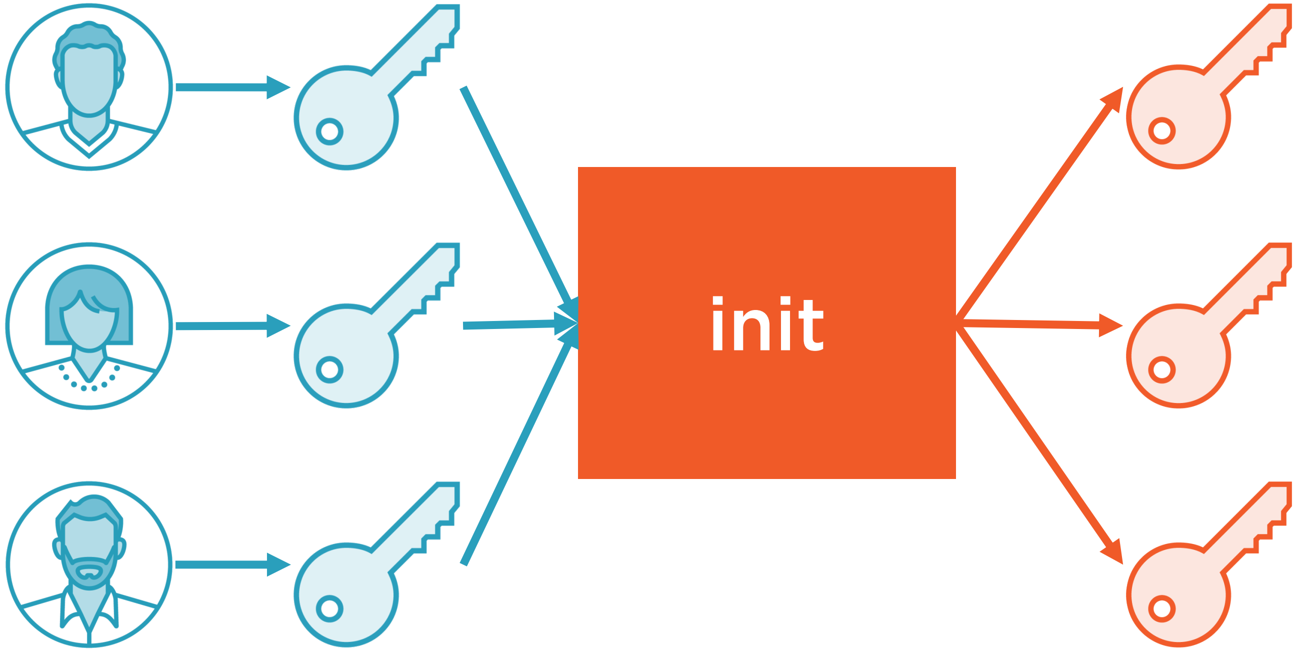
Key Shares

- PGP encrypted

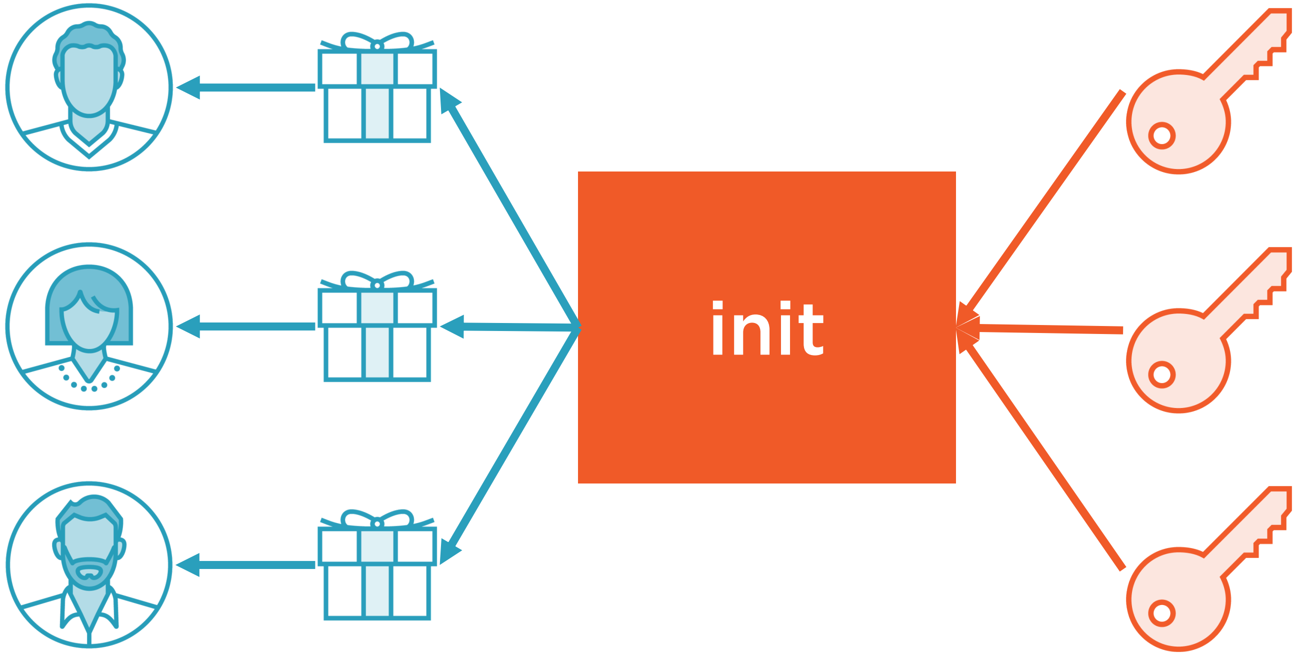
Cloud Vault

Hardware Security Module

Key Share Security



Key Share Security



Key and Seal Operations

```
#Seal and Master Key Operations

vault operator init
vault operator rekey
vault operator seal
vault operator unseal

#Encryption Key Operations

vault operator key-status
vault operator rotate
```

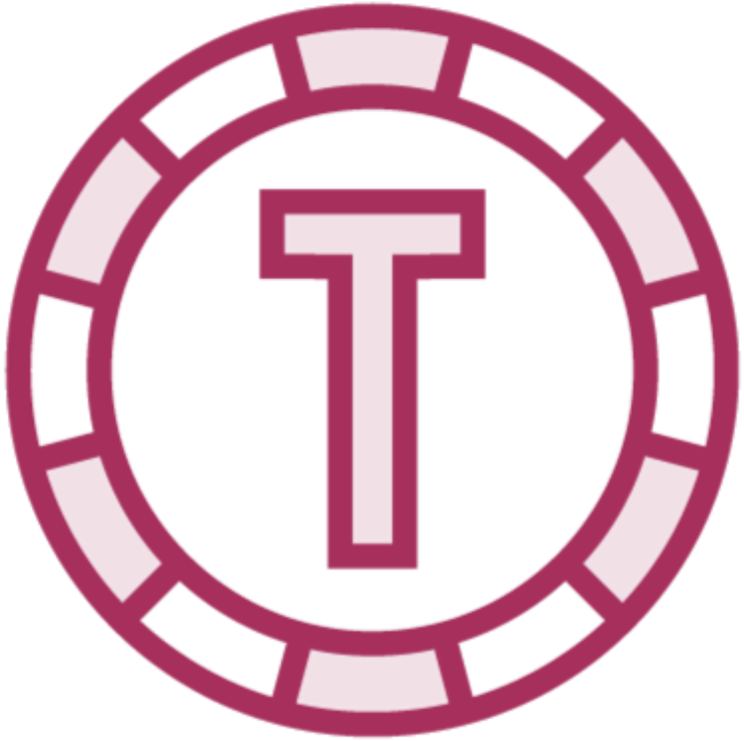
Globomantics Seal Update

Rekey Vault with PGP encrypted keys

Remove the root token

Enable auto unseal with Azure Key Vault

Root Token



Root token can do ANYTHING

Encrypt with PGP

Non-persistent root tokens

Generate using key shares

Auto Unseal

Master key stored in secure location

Cloud services and HSM

Key shares become recovery keys

Key shares still required

Auto Unseal Configuration

```
seal "azurekeyvault" {
  tenant_id     = "AZUREAD_TENANT_ID"


  client_id     = "AZUREAD_SPN_ID"
  client_secret = "AZUREAD_SPN_SECRET"


  vault_name    = "KEY_VAULT_NAME"
  key_name      = "KEY_NAME"

}
```

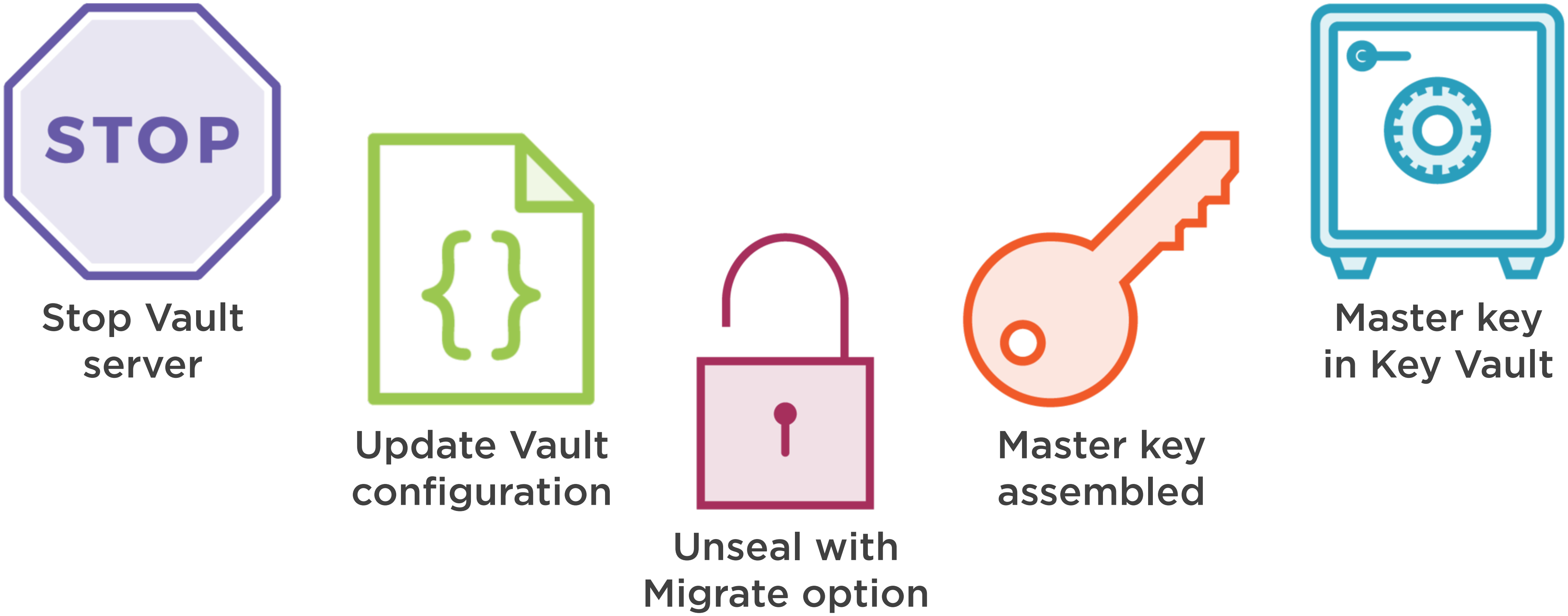
Auto Unseal Architecture

Azure VM

Azure AD MSI

Azure Key Vault

Master Key Migration



Stop Vault server

Update Vault configuration

Unseal with Migrate option

Master key assembled

Master key in Key Vault

Summary

Key shares are important

Root tokens are dangerous

Auto unseal is awesome

Coming up:

- Configuring Vault Server for High Availability