HashiCorp Vault Integration Guide
# Table of Contents

- **INTRODUCTION** .................................................................................................................. 1
- **ABOUT CRYPTO4A TECHNOLOGIES** .................................................................................. 1
- **WHAT IS THE QXEDGE?** ..................................................................................................... 1
- **WHO IS THE QXEDGE FOR?** ............................................................................................. 2
- **INTEGRATING QXEDGE WITH HASHICORP VAULT** ............................................................ 3
  - **SUPPORTED FEATURES** ..................................................................................................... 3
  - **PREREQUISITES** ................................................................................................................. 4
  - **CONFIGURING THE QxEDGE** ........................................................................................... 4
  - **ACCESSING THE QXEDGE ENABLED VAULT** ................................................................... 5
  - **VALIDATING THE INTEGRATION** ....................................................................................... 5
  - **AUGMENTING ENTROPY** .................................................................................................. 5
  - **RUNNING AS A SYSTEM SERVICE ON QxEDGE** ........................................................... 6
- **CONTACTING SUPPORT** ....................................................................................................... 7
Introduction

This document describes how the HashiCorp Vault can be integrated with the Crypto4A Technologies QxEDGE™ - HSM as a Platform. The document provides an overview of Crypto4A itself, explains some of the benefits of the QxEDGE, and gives detailed instructions on how the HashiCorp Vault can be integrated with the QxEDGE.

About Crypto4A Technologies

Crypto4A Technologies Inc. is a cybersecurity company started in 2012 with a goal of making cybersecurity simple, scalable, and sustainable. Crypto4A solutions are quantum-ready and provide the highest level of security based on today’s standards.

Crypto4A’s world-class team has a track record of creating value with nearly 300 years of combined experience in the cybersecurity industry. The company was founded by four industry experts who were instrumental in designing the first and second generation of Hardware Security Modules (HSM) that underpin the security of today’s internet. Crypto4A provides enterprise, cloud providers, mobile application, and IoT developers with sophisticated hardware-based security to protect the digital keys and their machine identities that run commerce, banking, payments, logistics, and the entire digital economy from cybercriminals and nation state attackers.

What is the QxEDGE?

The QxEDGE is the next evolution of the HSM. It brings together security applications, a quantum-ready HSM, and the tools and level of integration required by development, security, and operations teams to develop, deploy, and manage their security applications at scale in a simple and sustainable way. It has the flexibility to support numerous applications that run in an environment that is familiar to DevOps teams by supporting modern cloud native tools and the technologies that they use every day.

Benefits of the QxEDGE include:

- Eliminates the complexity of securing an organization’s most important assets.
- Creates a safe environment for critical assets.
- Simplifies management of trust infrastructures.
- Allows flexibility in deployment and scalability/extensibility - from the datacenter to the cloud to the edge.
- Reduces the cost of developing, deploying, and managing trust infrastructure.

“We eliminate complexity in cyber security to enable agile, scalable, and cost-effective trust infrastructure to aid digital transformation.”
At the core of the QxEDGE, is Crypto4A’s next-generation HSM - the Quantum Assured Security Module (QASM™). The QASM delivers cryptographic agility, cryptographic adaptability, and quantum safety to ensure quantum computing readiness. The QASM leverages quantum-safe, hash-based signature (HBS) algorithms and key encapsulation mechanisms (KEM) to ensure quantum-safe platform updates and inter-QxEDGE communications for secure auto-scaling, High Availability (HA), and Disaster Recovery (DR).

Digital transformation marks a radical rethinking of how organizations use technology, people, and processes to fundamentally change business practices. Due to advancements in quantum computing, edge computing, hyper-converged infrastructure, 5G networks, AI, and the deployment of many billions of IoT devices, organizations need to rethink their approach to cybersecurity while facing an ever-worsening skills shortage.

Applications include:
- Public Key Infrastructure (PKI).
- PKI in a Box.
- PKI as a Service.
- Code Signing.
- Secrets Vault.
- Network-Attached Quantum-Ready HSM.
- Entropy Generation.
- Unified Key Management.
- And many more applications.

For HashiCorp Vault customers, the QxEDGE offers an extra level of security assurance as the Vault software can run on the platform itself thus ensuring that all communications between the Vault and the HSM are local and are never exposed to the greater company network.

**Who is the QxEDGE for?**

Integrating the QxEDGE with the HashiCorp Vault provides many different benefits for an organization.

For the security administrators, QxEDGE ensures that the organization’s most sensitive data and applications are protected by a world-class HSM platform.

For operators and stakeholders, QxEDGE’s virtual air gap and strong business continuity processes remove the need for expensive and complex in-person key orchestration.

For developers, the QxEDGE also provides a rich online support system and a comprehensive SDK. The platform fully supports cloud native technologies and makes it extremely simple to deploy applications directly to the platform itself so that they can run on a trusted computing platform in parallel with the HSM.
Integrating QxEDGE with HashiCorp Vault

QxEDGE can support the following integration paths for the HashiCorp Vault:

- HashiCorp Vault running on a standalone machine communicating directly with QxEDGE HSM as a Platform via the QxEDGE PKCS #11 shared library.
- HashiCorp Vault running in Docker on a QxEDGE Processing Engine.
- HashiCorp Vault running on a standalone machine communicating with the QxEDGE emulator.

**NOTE:** This mode is for development and integration testing purposes only.

The remainder of the document assumes that HashiCorp Vault is running on a standalone machine and communicating with the QxEDGE directly. For instructions on how to run the QxEDGE emulator or how to run HashiCorp Vault on a QxEDGE Processing Engine, please refer to the Crypto4A Technologies support portal or contact support@crypto4a.com.

**Supported Features**

The QxEDGE supports the following features:

- Master Key Wrapping.
- Auto-unseal.
- Seal Wrap.
- Entropy Augmentation with SP 800-90B Compliant Entropy Sources.
- Dockerized HashiCorp Vault running on QxEDGE Processing Engine.
Prerequisites

To complete the procedures detailed in this guide, the following prerequisites are needed:

- HashiCorp Vault Enterprise with HSM support and a valid license.
- QxEDGE Software Development Kit (SDK).
- QxEDGE HSM as a Platform.
- QxEDGE PKCS #11 shared library.
- Ubuntu 18.04LTS.

Configuring the QxEDGE

Use the following procedure to configure the QxEDGE.

1. Configure your QxEDGE HSM as a Platform and ensure it is running properly.
   - Optionally, if this is a test integration, configure and run the QxEDGE emulator.
   - For instructions on how to configure the QxEDGE HSM as a Platform or to run the QxEDGE emulator, please refer to the documentation on the Crypto4A QxEDGE support portal.
2. Install HashiCorp Vault Enterprise with HSM support.
3. Copy the QxEDGE PKCS #11 shared library (libpkcs11.so) from the QxEDGE SDK into the same directory as the vault application.
4. Create a configuration file called config.hcl in the same directory as the vault application. The values in <> and the addresses should be updated to the correct values for your system configuration.

```hcl
seal "pkcs11" {
    lib = "<vault_install_path>/libpkcs11.so"
    slot = "5"
    pin = "<pin>"
    key_label = "vault-hsm-key"
    hmac_key_label = "vault-hsm-hmac-key"
    generate_key = "true"
}

storage "raft" {
    path = "<vault_install_path>/data"
    node_id = "node1"
}

listener "tcp" {
    address = "127.0.0.1:8200"
    tls_disable = 1
}

api_addr = "http://127.0.0.1:8200"
```
cluster_addr = 'https://127.0.0.1:8201'
ui = true
disable_mlock = true
5. Open a terminal.
6. Navigate to the HashiCorp Vault installation directory.
7. Start HashiCorp Vault.
   ./vault server -config config.hcl

Accessing the QxEDGE Enabled Vault

Use the following procedure to access the QxEDGE enabled vault.

1. Verify that the HashiCorp Vault has successfully started.
2. Open a new terminal window.
3. Set the environment variable VAULT_ADDR.
   export VAULT_ADDR='http://127.0.0.1:8200'
4. Initialize Vault.
   ./vault operator init
   A number of keys, the root token, and a success message are returned.
5. Copy the recovery keys and the root token.
   ./vault login
7. Enter the root token when prompted.

Validating the Integration

The following procedure uses a tool in the QxEDGE SDK called spa-key-man to confirm that Vault has been successfully integrated with QxEDGE.

1. Run the following command to list the key metadata stored in QxEDGE.
   spa-key-man list
2. Ensure that the list contains entries similar to the following:
   ...
   903d20b5-0e13-684b-b684-7785878cf31e - SECRET_KEY vault-hsm-key
   ...
   956773c8-2029-5842-217e-e2004a66bb46 - SECRET_KEY vault-hsm-hmac-key
   ...

Augmenting Entropy

The QxEDGE provides a number of SP800-90B compliant entropy sources. Use the following procedure to augment HashiCorp Vault.

1. Update the config.hcl file and add the following lines.
   entropy "seal" {
     mode = "augmentation"
2. Restart Vault.
3. Open a terminal.
4. Navigate to the vault installation directory.
5. Run the following command:
   ```bash
   vault secrets enable -external-entropy-access transit
   ```
6. Validate that entropy augmentation has been enabled by running the following command:
   ```bash
   vault secrets list -detailed
   ```
7. Ensure that External Entropy Access is set to “true”.

### Running as a System Service on QxEDGE

If HashiCorp Vault is running on QxEDGE directly, it can be run as a System Service to enable automatic start on system boot. However, there are some special considerations that need to be followed in order to ensure proper execution as described in the following procedure.

1. Navigate to the vault installation.
2. Copy the vault executable to `/usr/local/bin`.
   ```bash
   sudo cp vault /usr/local/bin
   ```
3. Create a directory for the configuration file.
   ```bash
   sudo mkdir /etc/vault.d
   ```
4. Copy the configuration file to the newly created directory.
   ```bash
   cp config.hcl /etc/vault.d
   ```
5. Configure Vault to run on QxEDGE.
   ```bash
   sudo setcap cap_ipc_lock=+ep /usr/local/bin/vault
   sudo useradd --system --home /etc/vault.d --shell /bin/false vault
   sudo mkdir /var/lib/vault
   sudo chown vault:vault /var/lib/vault
   ```
6. Create a systemd service configuration file at
   ```bash
   /etc/systemd/system/vault.service
   ```
   with the following content:

   ```ini
   [Unit]
   Description="HashiCorp Vault - A tool for managing secrets"
   Documentation=https://www.vaultproject.io/docs/
   Requires=network-online.target
   After=network-online.target
   ConditionFileNotEmpty=/etc/vault.d/config.hcl
   StartLimitIntervalSec=60
   StartLimitBurst=3
   
   [Service]
   User=vault
   Group=vault
   ProtectSystem=full
   ProtectHome=read-only
   PrivateTmp=yes
   PrivateDevices=yes
   SecureBits=keep-caps
   AmbientCapabilities=CAP_IPC_LOCK
   ```
Capabilities=CAP_IPC_LOCK+ep
CapabilityBoundingSet=CAP_SYSLOG CAP_IPC_LOCK
NoNewPrivileges=yes
ExecStart=/usr/local/bin/vault server -config=/etc/vault.d/config.hcl
ExecReload=/bin/kill --signal HUP $MAINPID
KillMode=process
KillSignal=SIGINT
Restart=on-failure
RestartSec=5
TimeoutStopSec=30
StartLimitInterval=60
StartLimitIntervalSec=60
StartLimitBurst=3
LimitNOFILE=65536
LimitMEMLOCK=infinity

[Install]
WantedBy=multi-user.target

7. Enable the Vault service.
   sudo systemctl enable vault
8. Start the Vault service.
   sudo systemctl start vault

Contacting Support

If you require assistance or have any questions, please contact support@crypto4a.com.