UNIVERSITY OF CAMBRIDGE

Zero-Trust Storage Encryption From Application-Layer Operators to Infrastructure-Native CSI Drivers

Tunde Oyewo

Cloud Engineer

14/09/2026

UNIVERSITY OF CAMBRIDGE

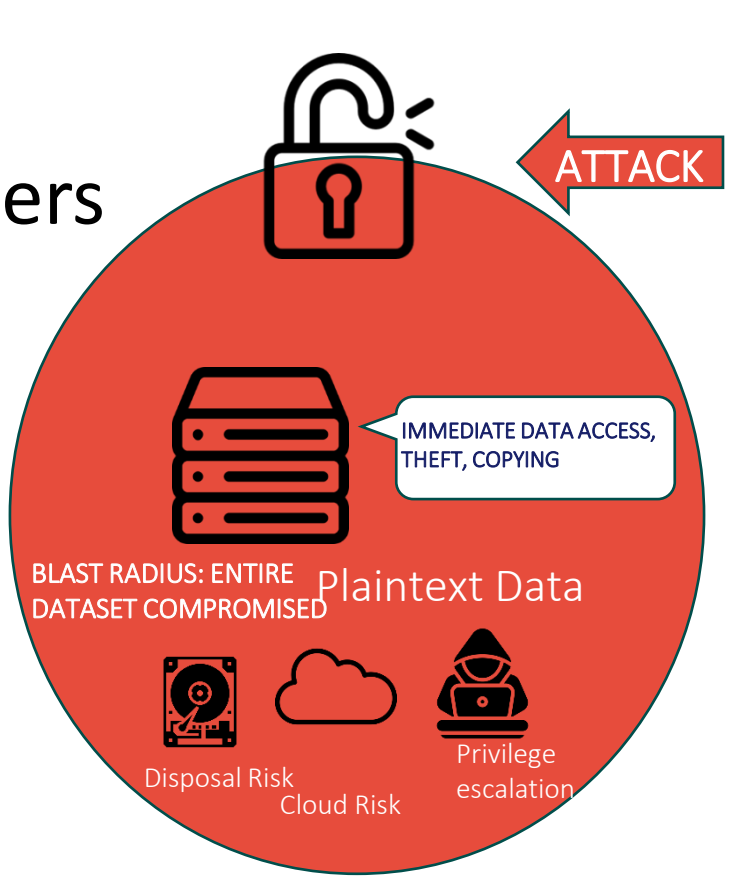
Key Objectives

- Exploration and Evaluation of automated encryption solutions for Kubernetes block storage in TREs, utilising technologies such as LUKS, HashiCorp Vault . Integrates OpenStack Cinder, via CSI driver with encryption keys securely stored in vault.
- Evaluate federated key ownership solutions, ensuring each institution maintains exclusive control over its encryption keys.
- Evaluate compliance, auditability, and operational security frameworks for encrypted storage, aligning with data security standards such as ISO27001, CAF, SATRE.
- Drive adoption and knowledge transfer through open-source deliverables, clear documentation, and engagement with the wider TRE community e.g. UK TRE, HDR UK, DARE UK.

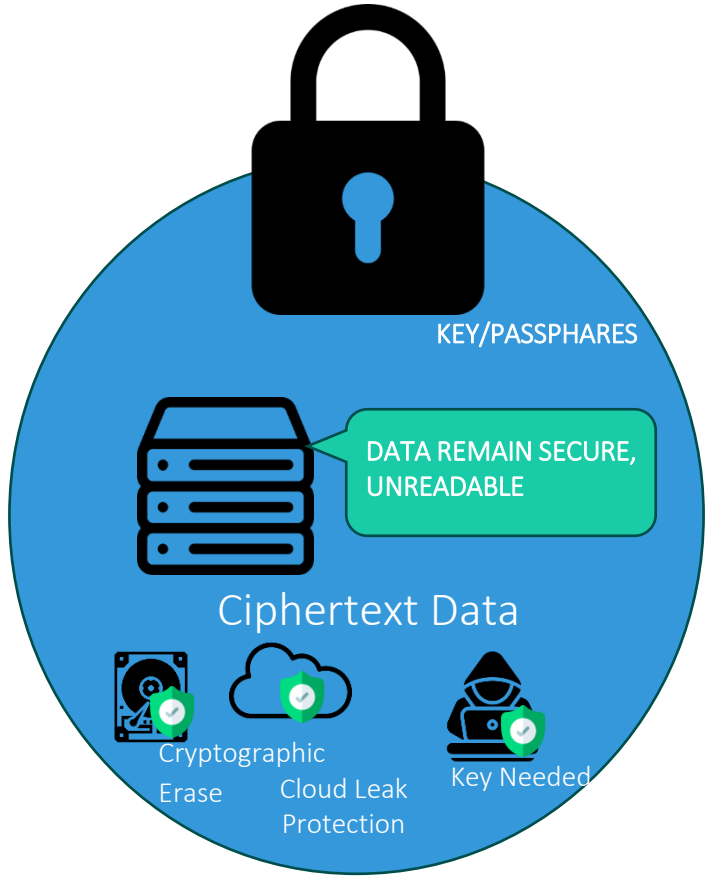
UNIVERSITY OF CAMBRIDGE

Why Encryption in TRE Matters

- TREs handles sensitive data
- Compliance with regulatory standards:
  - GDPR Article 32 mandates data encryption for confidentiality and resiliency.
  - NCSC Cloud Security Principles: All customer data should be encrypted at rest
  - NHS Secure Data Environment: Requires data to be encrypted at rest and in transit.



UNENCRYPTED STORAGE (HIGH RISK)

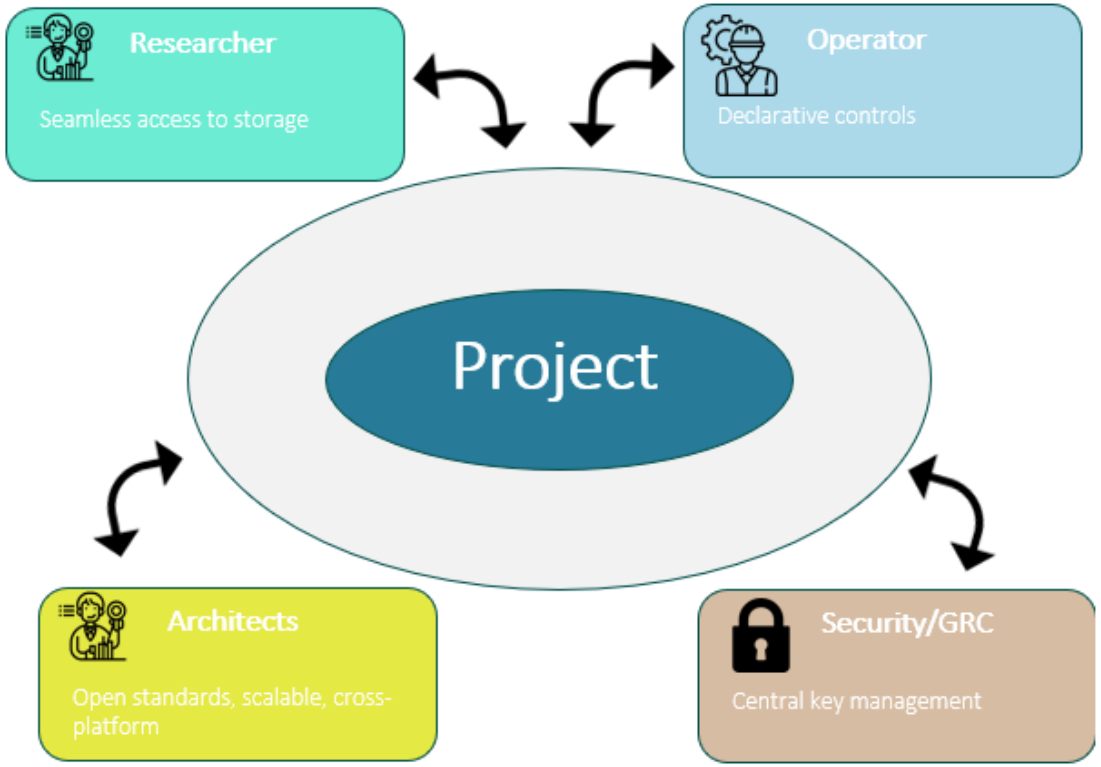


ENCRYPTED STORAGE (MITIGATED RISK)

UNIVERSITY OF CAMBRIDGE

Stakeholder Requirements

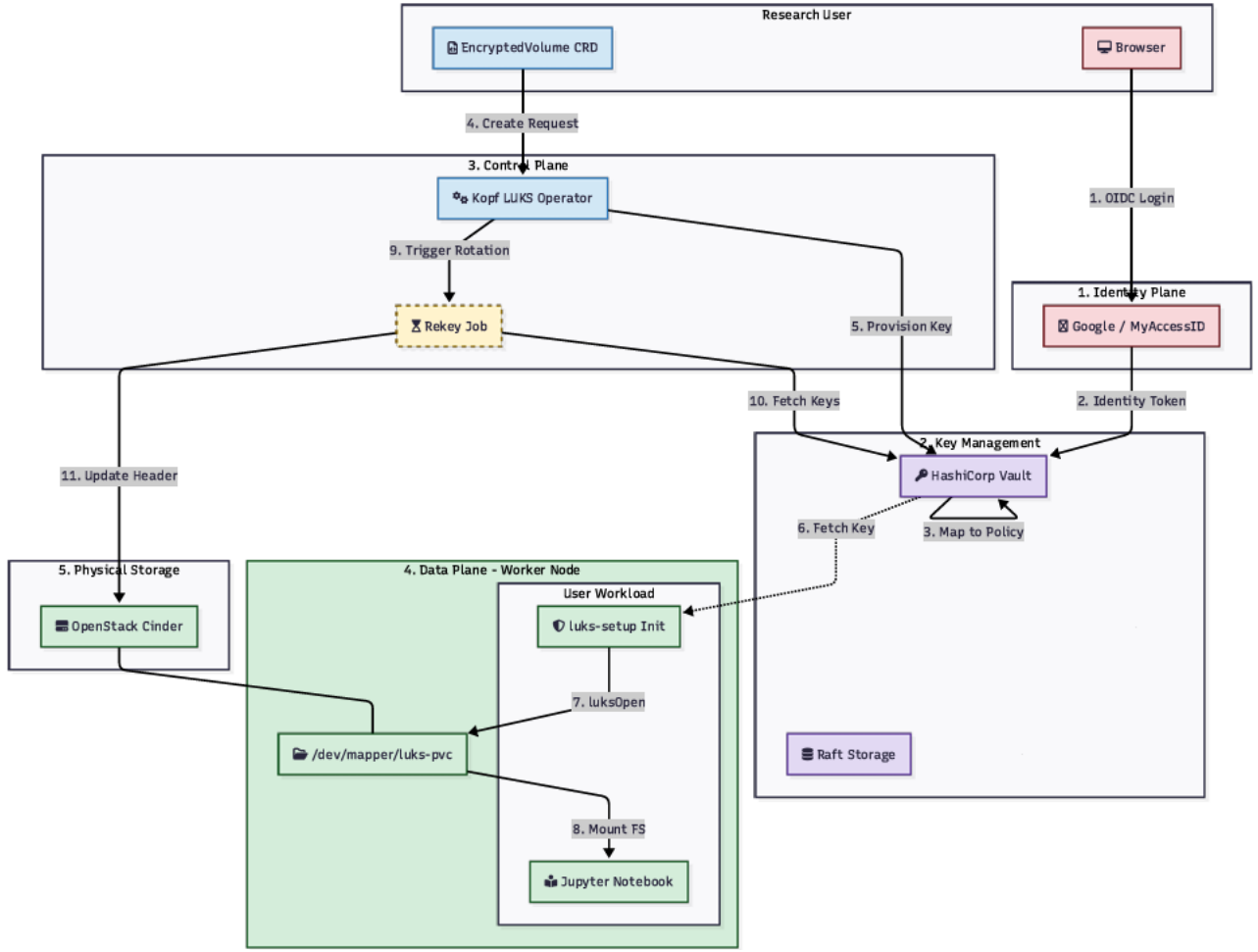
- Researchers
  - Seamless encryption with no cryptographic burden
- TRE Operator
  - Encryption enabled by default.
- Security/GRC
  - Centrally managed key, audit logs, key rotation
- Platform Engineer
  - Automated solution



UNIVERSITY OF CAMBRIDGE

Application-Layer Blueprint (Kopf Operator Architecture)

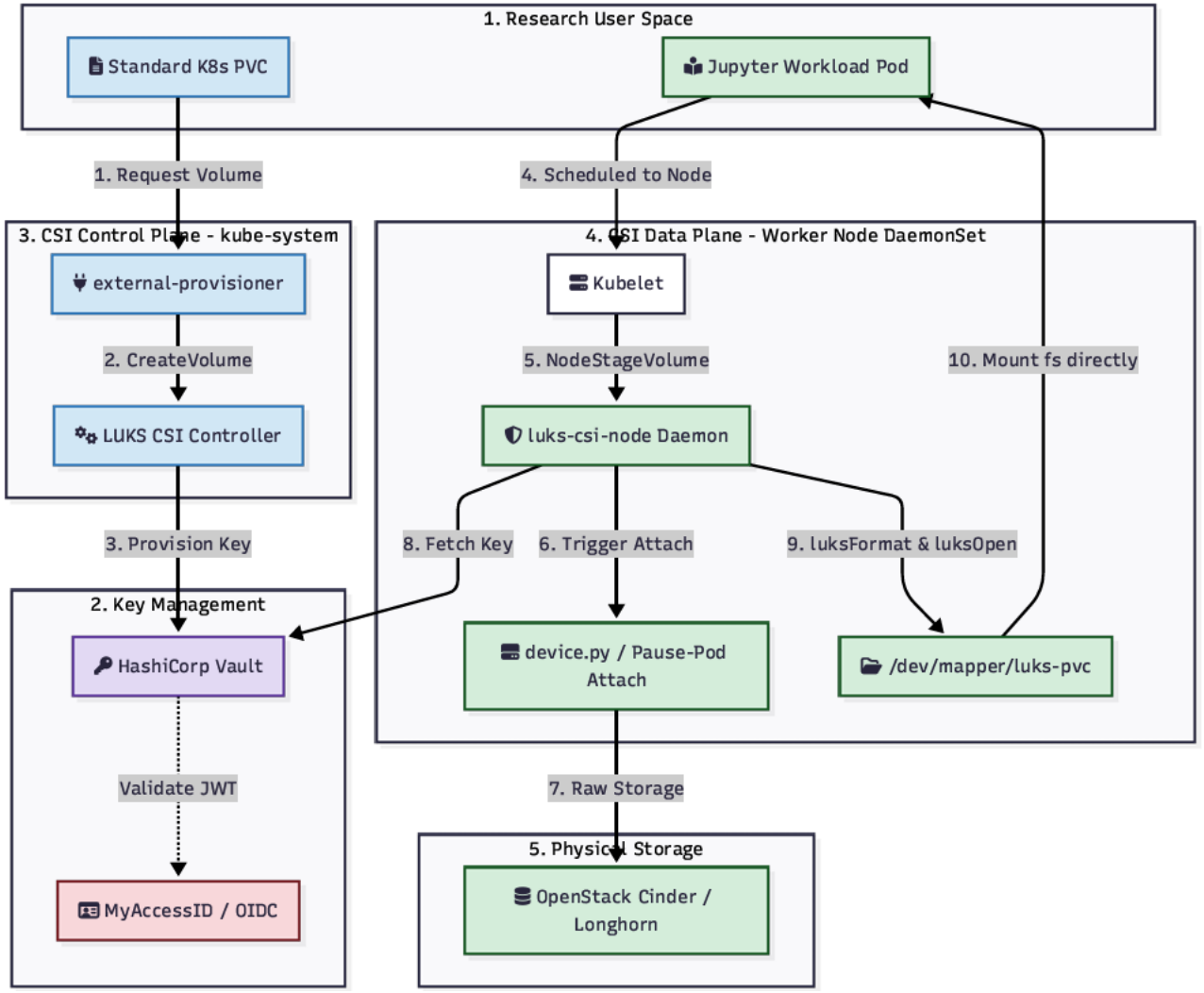
- Kubernetes Operator watches PVCs and Orchestrates LUKS encryption
- Works with OpenStack Cinder with CSI driver
- Keys stored securely in vault



UNIVERSITY OF CAMBRIDGE

Infrastructure-Native Blueprint (LUKS CSI Driver Architecture)

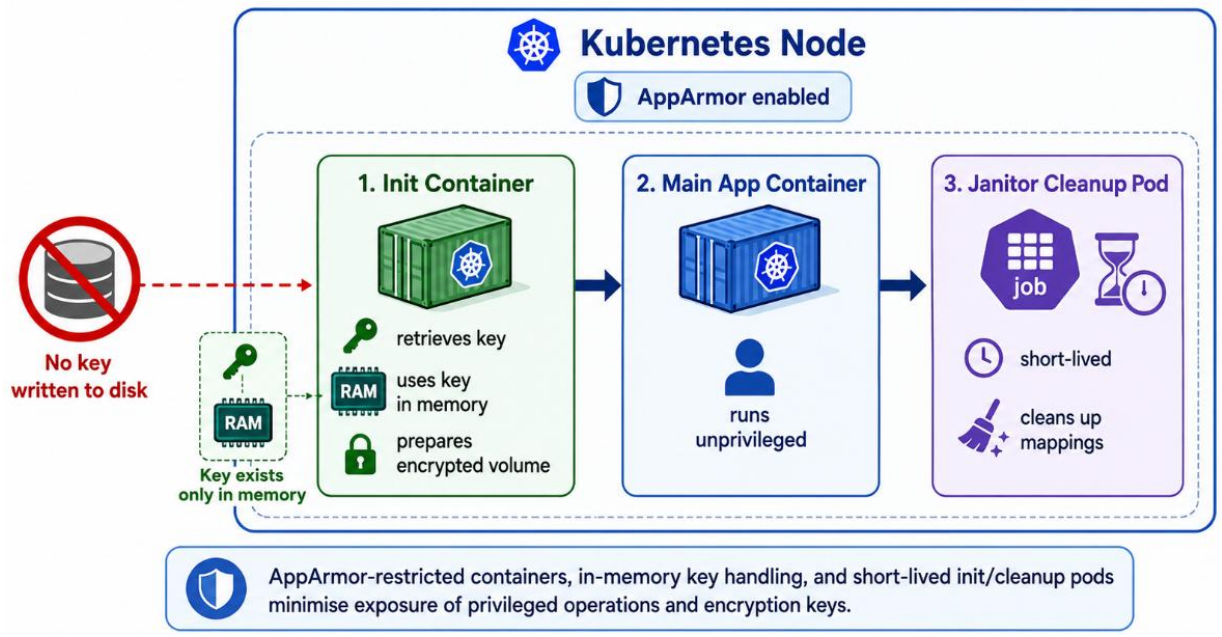
- Zero-Friction request
- Storage attachment and authentication (Node data plane)
- Transparent decryption and mounting



UNIVERSITY OF CAMBRIDGE

Security Consideration – Operator model

- Restricted AppArmor Profiles
- In-Memory Key Handling
- Node Isolation (Tainting)
- Short-Lived Execution:



UNIVERSITY OF CAMBRIDGE

When to use each approach

Scenario	Recommendation approach	Why
Production or multi-tenant cluster	CSI Driver	Native PVC integration and privileged operations remains within platform-managed components
Rapid PoC and workflow experimentation	Kopf Operator	Faster to modify for Vault, OIDC, key rotation and custom orchestration testing
No cluster-level access or privileged workload permitted	Neither	Both approaches require platform-level permissions and access to raw block devices

UNIVERSITY OF CAMBRIDGE

Project Team

Project Leads

Wojciech Turek (Cambridge)

Co-leads

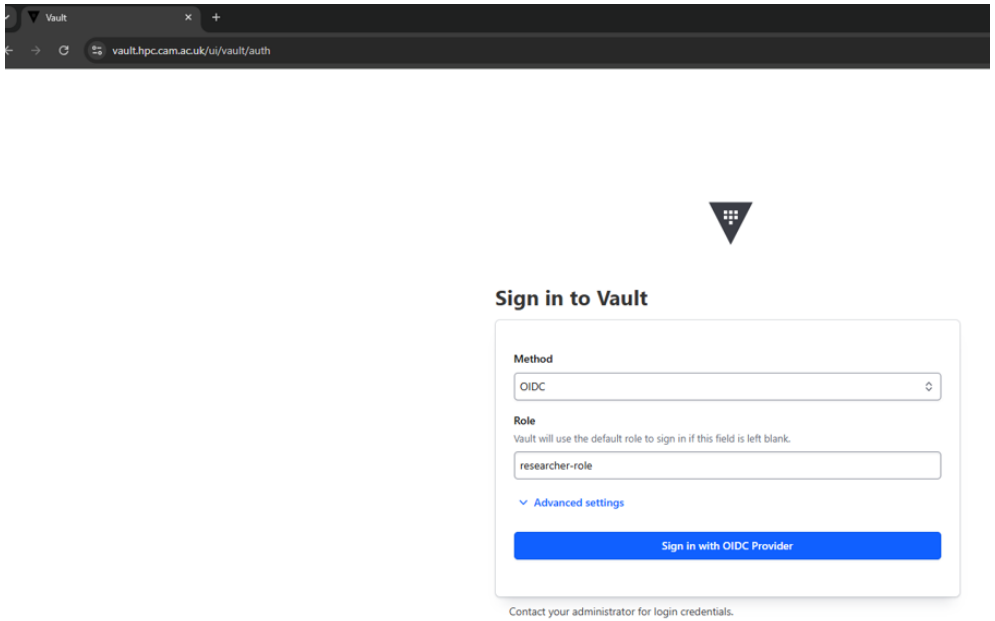
- Slyvie Da Graca Ramos (UCL)
- Thomas Green (BriCS)
- Matt Penn (KCL)

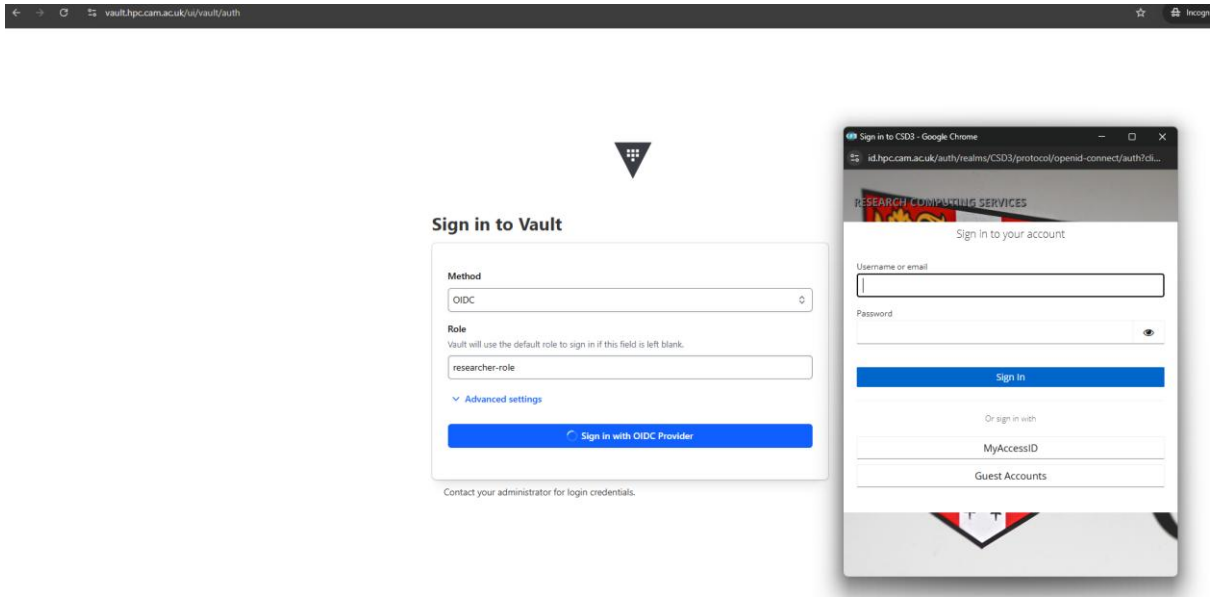
Project Team Members

- Paul Browne (Cambridge)
- Tunde Oyewo (Cambridge)
- Jake Watson (BriCS)
- Glyn Chudleigh (KCL)
- David Guzman (UCL)

UNIVERSITY OF CAMBRIDGE

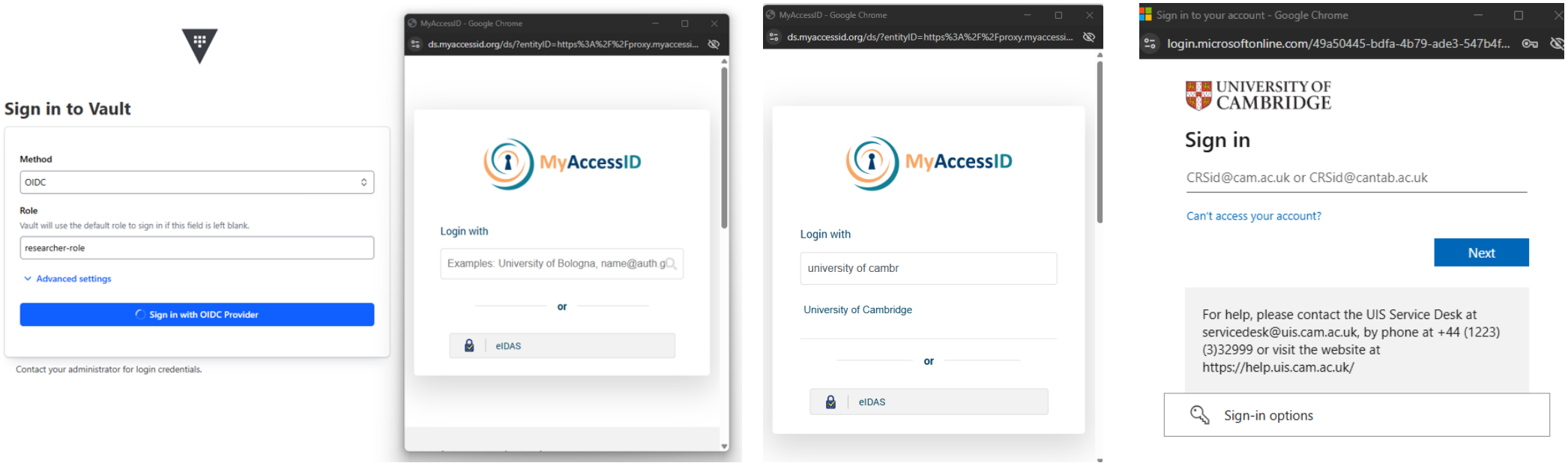
Demo





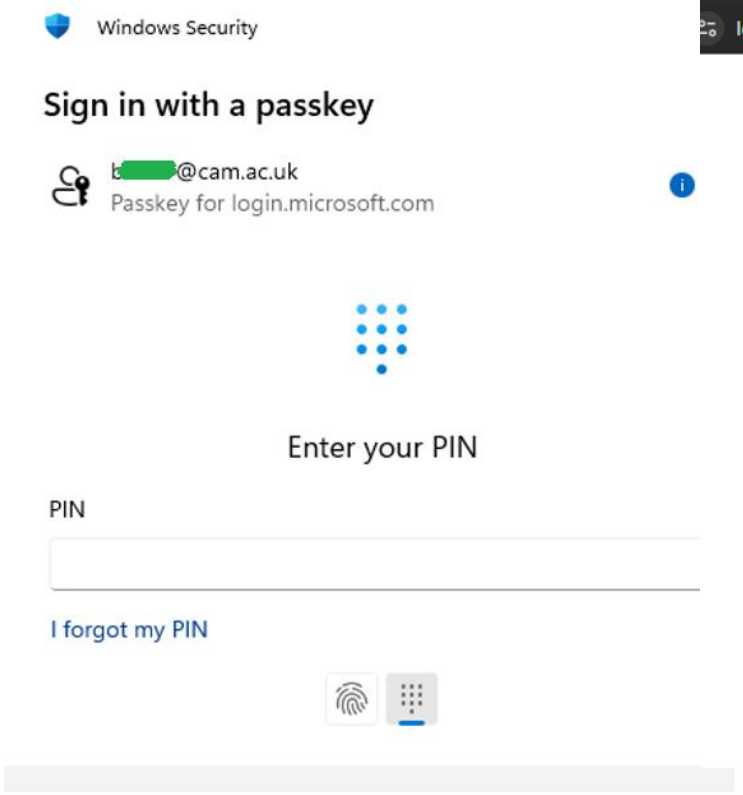
UNIVERSITY OF CAMBRIDGE

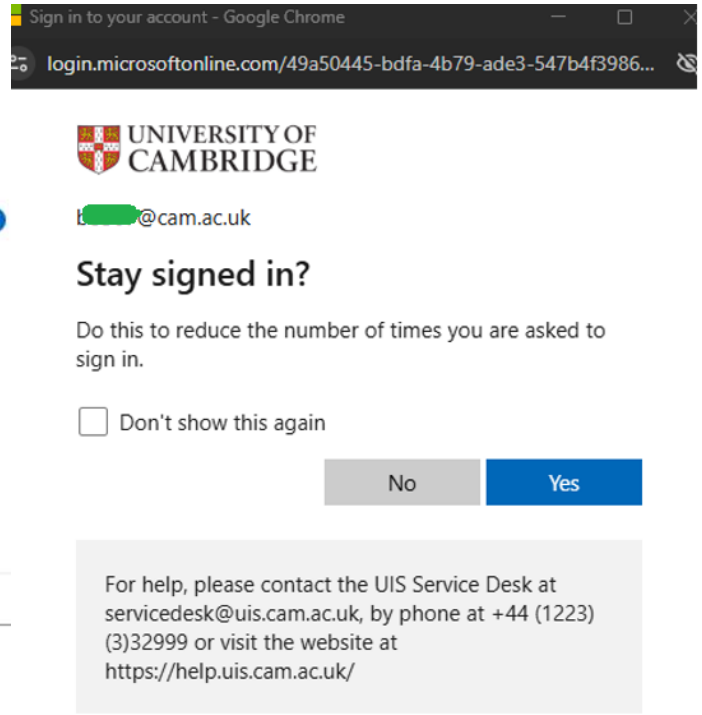
Demo

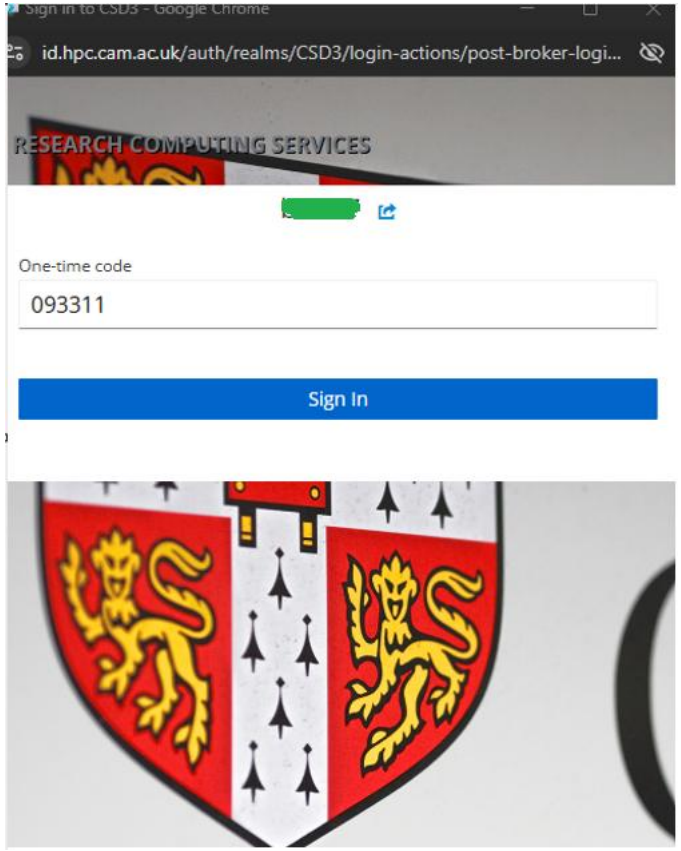


UNIVERSITY OF CAMBRIDGE

Demo

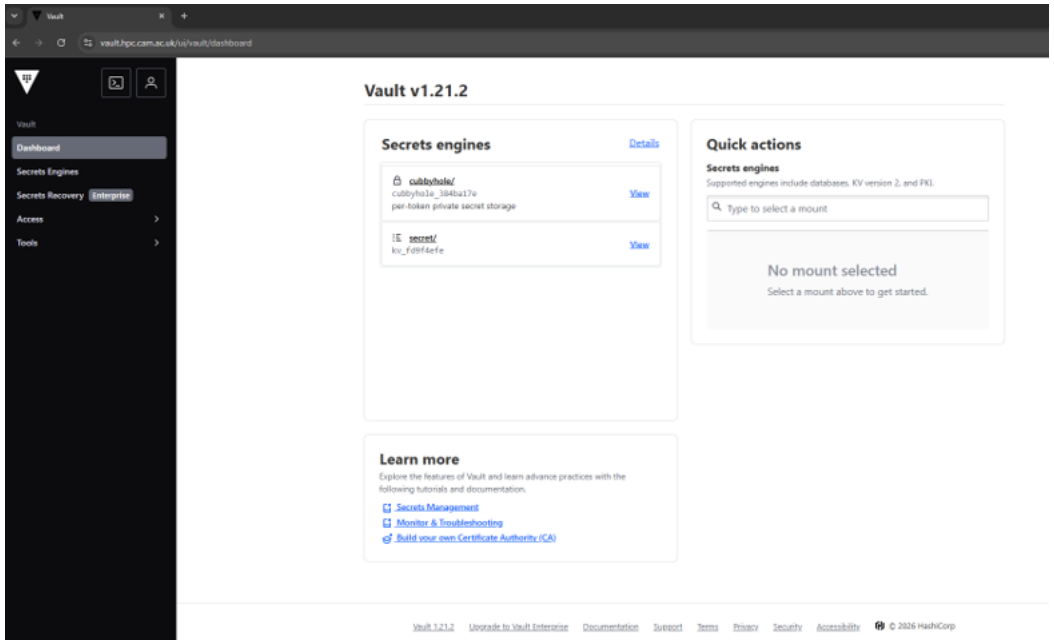


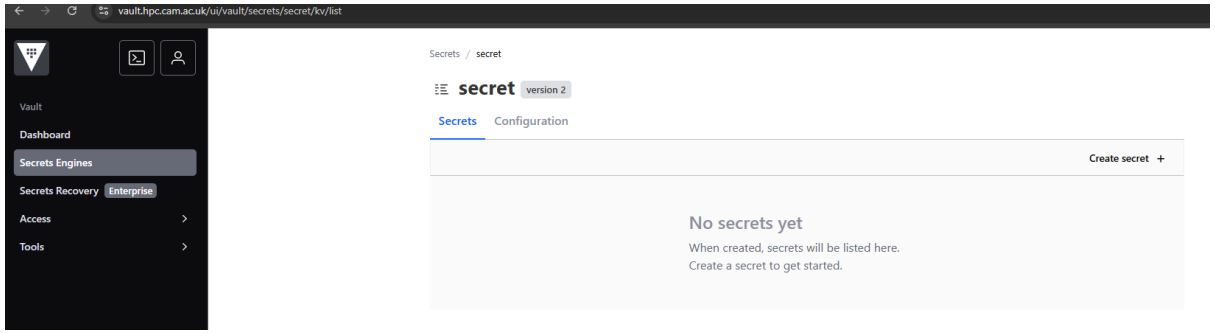




UNIVERSITY OF CAMBRIDGE

Demo





encrypted-volume-cr-vault.yaml

custom-resource > ! encrypted-volume-cr-vault.yaml > ...

```yaml
apiVersion: crypto.example.com/v1
kind: EncryptedVolume
metadata:
  name: luks-encrypted-volume-new
  namespace: default
spec:
  institution: "university-of-cambridge"
  pvcName: "csi-pvc-cinder-for-luks"
  mountPath: "/mnt/securefolder"
  size: "2Gi"
  deletionPolicy: "Delete"
  # deletionPolicy: "Retain"
  storageClassName: "cinder-sc" # change this if storageclass name is different

```

UNIVERSITY OF CAMBRIDGE

Demo

```
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$ kubectl apply -f custom-resource/encrypted-volume-cr-vault.yaml
encryptedvolume.crypto.example.com/luks-encrypted-volume-new created
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$ kubectl get EncryptedVolume
NAME                       AGE
luks-encrypted-volume-new   13s
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$ kubectl get pods -A | grep luks
default         encrypt-luks-encrypted-volume-new           2/2     Running   0             27s
default         luks-test-luks-operator-78b9fc8779-6nwkw    1/1     Running   0             16m
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$ kubectl get encryptedvolume,pvc -o wide
NAME                                                                AGE
encryptedvolume.crypto.example.com/luks-encrypted-volume-new   2m51s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE     VOLUMEMODE
persistentvolumeclaim/csi-pvc-cinder-for-luks       Bound    pvc-d38d24ca-5360-4bd2-a9a7-a1b253cf284b   2Gi        RWO            cinder-sc      <unset>                 2m50s   Block
persistentvolumeclaim/data-vault-0                  Bound    pvc-[redacted]                             10Gi       RWO            cinder-sc      <unset>                 84d     Filesystem
persistentvolumeclaim/data-vault-1                  Bound    pvc-32060a6d-38a6-4aaa-9dc7-16b57cd5e527   10Gi       RWO            cinder-sc      <unset>                 84d     Filesystem
persistentvolumeclaim/data-vault-2                  Bound    pvc-7ea67036-ff67-4110-9cbe-cde376631c0e   10Gi       RWO            cinder-sc      <unset>                 84d     Filesystem
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$
```

```
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$ kubectl logs  luks-test-luks-operator-78b9fc8779-6nwkw
[2026-07-13 15:58:29,003] kopf._core.reactor.r [DEBUG   ] Starting Kopf 1.36.0.
[2026-07-13 15:58:29,003] kopf._core.engines.a [INFO    ] Initial authentication has been initiated.
[2026-07-13 15:58:29,003] kopf.activities.auth [DEBUG   ] Activity 'login_via_client' is invoked.
[2026-07-13 15:58:29,005] kopf.activities.auth [DEBUG   ] Client is configured in cluster with service account.
[2026-07-13 15:58:29,005] kopf.activities.auth [INFO    ] Activity 'login_via_client' succeeded.
[2026-07-13 15:58:29,006] kopf._core.engines.a [INFO    ] Initial authentication has finished.
[2026-07-13 15:58:29,021] kopf._cogs.clients.w [DEBUG   ] Starting the watch-stream for customresourcedefinitions.v1.apiextensions.k8s.io cluster-wide.
[2026-07-13 15:58:29,355] kopf._cogs.clients.w [DEBUG   ] Starting the watch-stream for namespaces.v1 cluster-wide.
[2026-07-13 15:58:29,355] kopf._cogs.clients.w [DEBUG   ] Starting the watch-stream for encryptedvolumes.v1.crypto.example.com in 'default'.
[2026-07-13 15:58:29,356] kopf._cogs.clients.w [DEBUG   ] Starting the watch-stream for pods.v1 in 'default'.
```

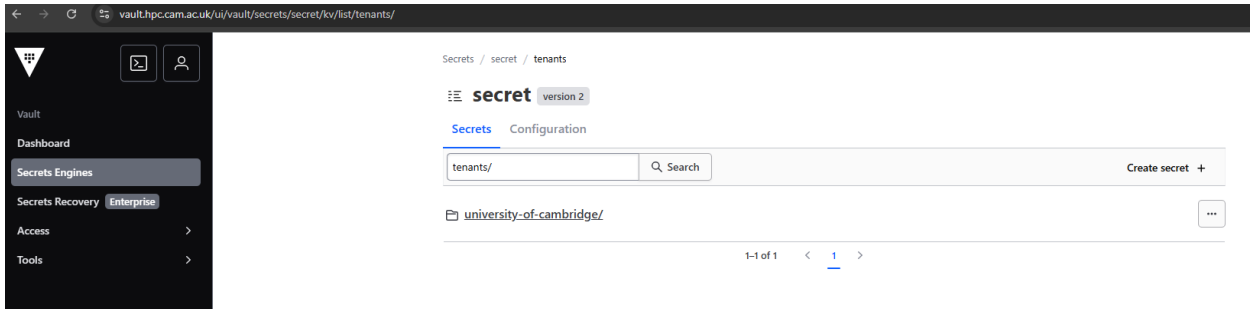
```
[2026-07-13 16:19:09,514] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Check client: <hvac.v1.Client object at 0x7f533efa2590>
[2026-07-13 16:19:09,519] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Timer found Vault v1. Synced to 'vaultversion' annotation.
[2026-07-13 16:19:09,519] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Timer 'sync_vault_version' succeeded.
[2026-07-13 16:19:09,520] kopf.objects         [DEBUG   ] [default/luks-encrypted-volume-new] Patching with: {'metadata': {'annotations': {'vaultversion': '1'}}, 'status': {'current_vault_version': 1}}
(base) b[redacted]:~/pulumi-nfcs-k8s-staging$
```

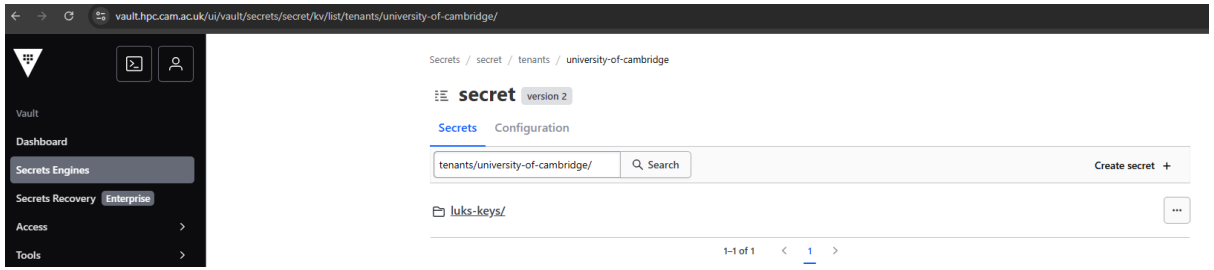
```
ubuntu@stage-nfcs-k8s-node1:~$ lsblk -o NAME,FSTYPE,TYPE,MOUNTPOINT
NAME                        FSTYPE    TYPE  MOUNTPOINT
loop0                       squashfs  loop  /snap/core20/2769
loop1                       squashfs  loop  /snap/core20/2866
loop2                                 loop
loop3                       squashfs  loop  /snap/lxd/38800
loop4                       squashfs  loop  /snap/core22/2411
loop5                       squashfs  loop  /snap/snapd/26865
loop6                       squashfs  loop  /snap/snapd/27406
loop7                       squashfs  loop  /snap/lxd/40115
sda                                   disk
├─sda1                      ext4      part  /
├─sda14                               part
└─sda15                     vfat      part  /boot/efi
sdb                                   disk
└─luks-luks-encrypted-volume-new
                            ext4      crypt /var/lib/kubelet/pods/5fb8d39c-b4eb-48ca-86fa-c383e35ce521/volume-subpaths/shared-data/jupyter-notebook/0
sdc                         ext4      disk  /var/lib/kubelet/pods/02f26db5-4f5a-4c28-aa67-aaa7e6bfe65b/volumes/kubernetes.io~csi/pvc-32060a6d-38a6-4aaa-9dc7-16b57cd5e527/mount
ubuntu@stage-nfcs-k8s-node1:~$
```

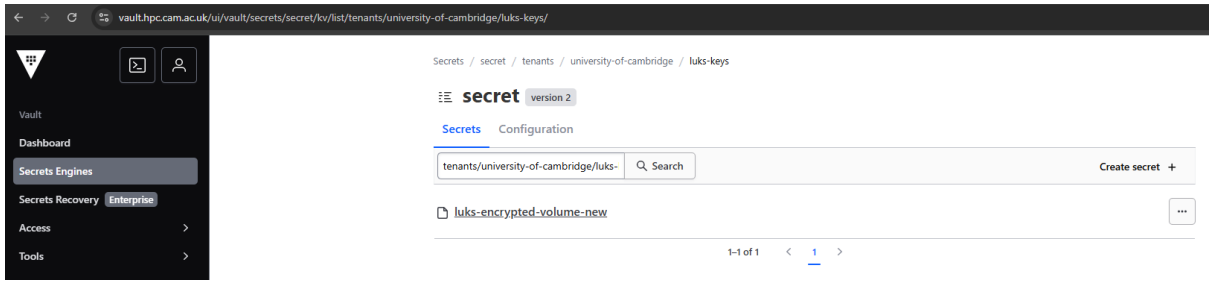
```
ubuntu@stage-nfcs-k8s-node1:~$ sudo cryptsetup status luks-luks-encrypted-volume-new
/dev/mapper/luks-luks-encrypted-volume-new is active and is in use.
  type:    LUKS2
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device:  /dev/sdb
  sector size:  512
  offset:  32768 sectors
  size:    4161536 sectors
  mode:    read/write
ubuntu@stage-nfcs-k8s-node1:~$
```

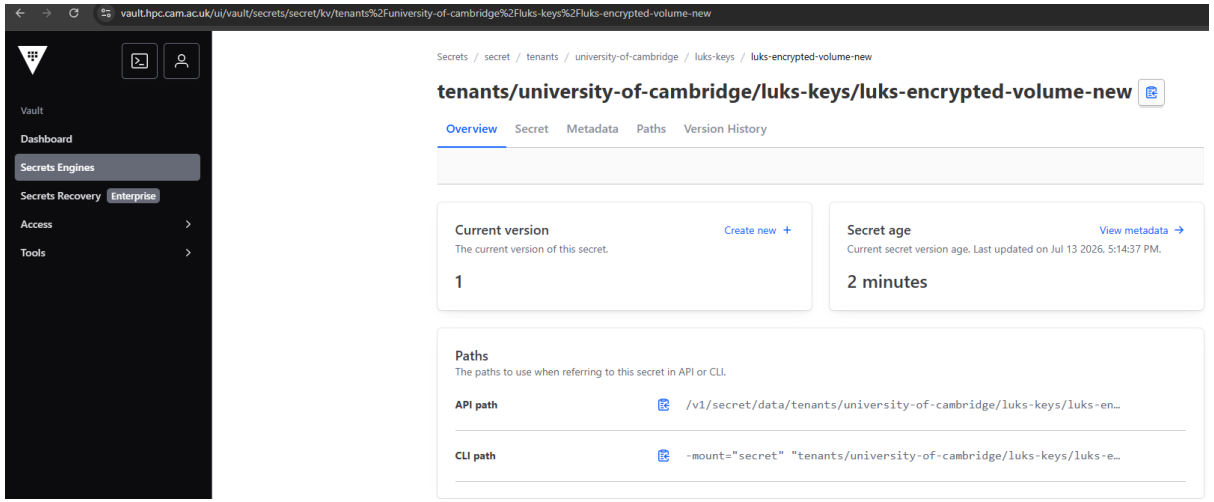
UNIVERSITY OF CAMBRIDGE

Demo



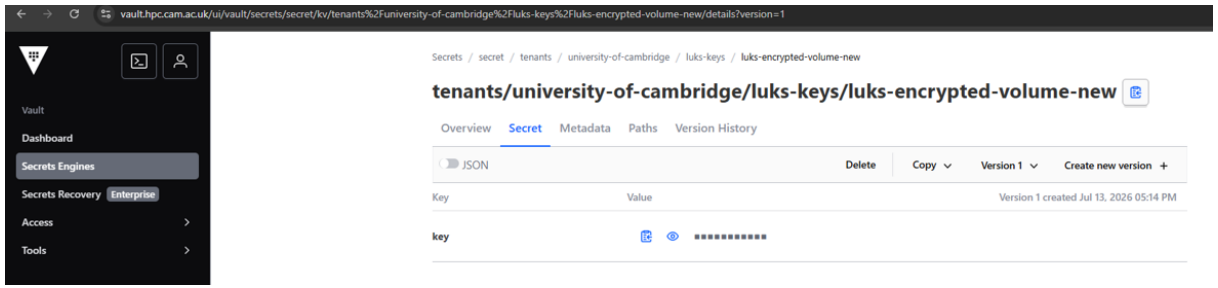


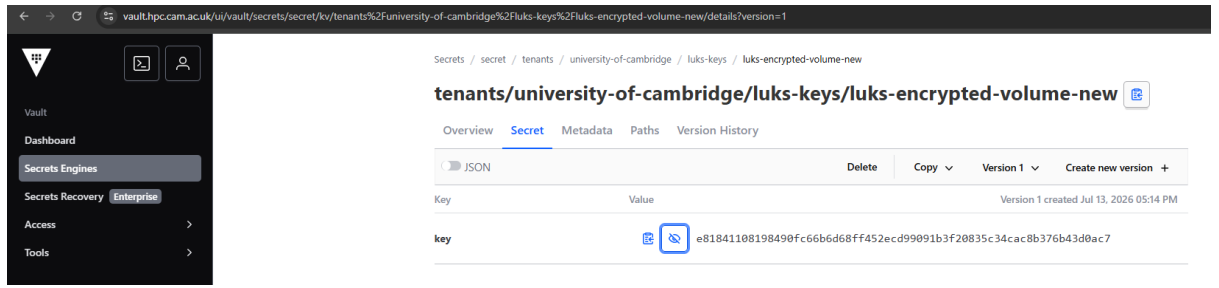




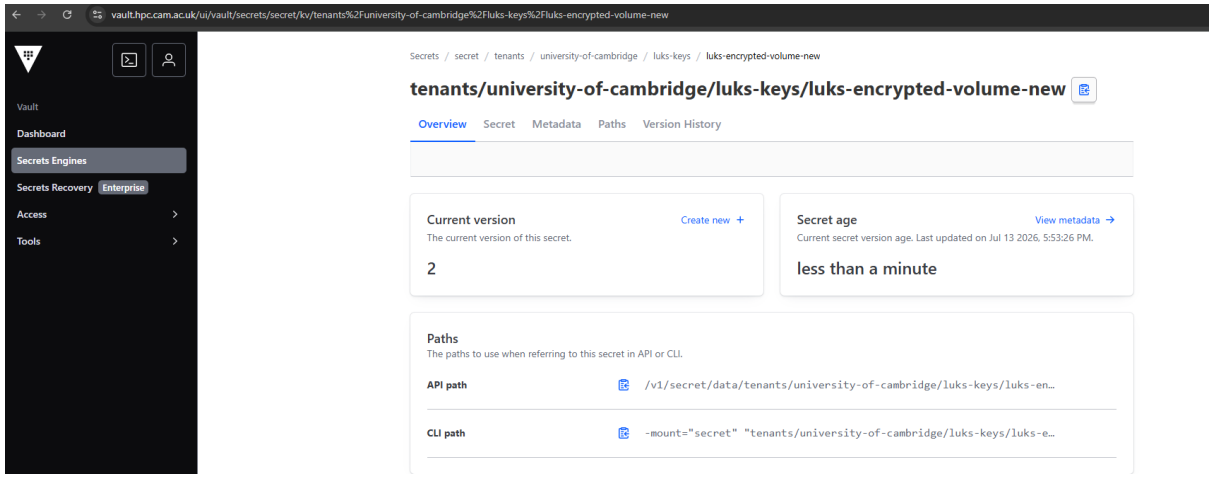
UNIVERSITY OF CAMBRIDGE

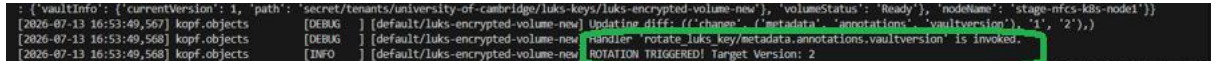
Demo –



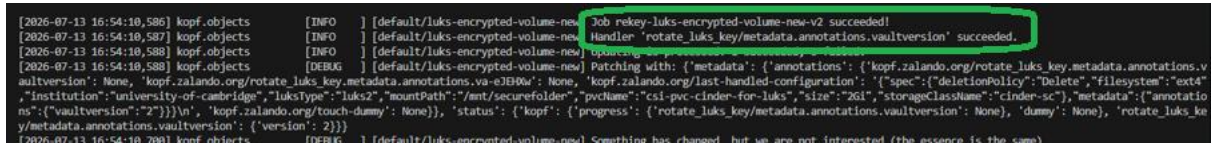


Key Rotation









UNIVERSITY OF CAMBRIDGE

Demo

Key Rotation

```
(base) [redacted]:~/pulumi-nfcs-k8s-staging$ kubectl get jobs,pods
NAME                                          STATUS    COMPLETIONS   DURATION   AGE
job.batch/rekey-luks-encrypted-volume-new-v2  Running   0/1           7s         7s

NAME                                          READY   STATUS    RESTARTS      AGE
pod/encrypt-luks-encrypted-volume-new         2/2     Running   0             39m
pod/keycloak-c666b7cb5-j7nxg                  1/1     Running   1 (9d ago)    68d
pod/luks-test-luks-operator-78b9fc8779-6nwkw  1/1     Running   0             55m
pod/rekey-luks-encrypted-volume-new-v2-wmm25  1/1     Running   0             7s
pod/vault-0                                   1/1     Running   1 (9d ago)    47d
pod/vault-1                                   1/1     Running   1 (9d ago)    47d
pod/vault-2                                   1/1     Running   1 (9d ago)    47d
pod/vault-agent-injector-7845f59846-pgjjp     1/1     Running   1 (9d ago)    84d
(base) [redacted]:~/pulumi-nfcs-k8s-staging$ kubectl get jobs,pods
NAME                                          READY   STATUS    RESTARTS      AGE
pod/encrypt-luks-encrypted-volume-new         2/2     Running   0             41m
pod/keycloak-c666b7cb5-j7nxg                  1/1     Running   1 (9d ago)    68d
pod/luks-test-luks-operator-78b9fc8779-6nwkw  1/1     Running   0             57m
pod/vault-0                                   1/1     Running   1 (9d ago)    47d
pod/vault-1                                   1/1     Running   1 (9d ago)    47d
pod/vault-2                                   1/1     Running   1 (9d ago)    47d
pod/vault-agent-injector-7845f59846-pgjjp     1/1     Running   1 (9d ago)    84d
(base) [redacted]:~/pulumi-nfcs-k8s-staging$
```

```
(base) [redacted]:~/pulumi-nfcs-k8s-staging$ kubectl exec -it encrypt-luks-encrypted-volume-new -c jupyter-notebook -- /bin/sh
$ ls
work
$ df -h
Filesystem                                Size  Used Avail Use% Mounted on
overlay                                   58G  9.9G   49G  18% /
tmpfs                                     64M     0   64M   0% /dev
tmpfs                                     32G  4.0K   32G   1% /vault/secrets
/dev/sda1                                 58G  9.9G   49G  18% /etc/hosts
shm                                       64M     0   64M   0% /dev/shm
/dev/mapper/luks-luks-encrypted-volume-new 2.0G  532K  1.9G   1% /home/jovyan/work
tmpfs                                     32G   12K   32G   1% /run/secrets/kubernetes.io/serviceaccount
tmpfs                                     16G     0   16G   0% /proc/acpi
tmpfs                                     16G     0   16G   0% /proc/scsi
tmpfs                                     16G     0   16G   0% /sys/firmware
tmpfs                                     16G     0   16G   0% /sys/devices/virtual/powercap
$
```

UNIVERSITY OF CAMBRIDGE

Demo – Clean up

```
(base) [redacted]:~/pulumi-nfcs-k8s-staging$ kubectl delete EncryptedVolume luks-encrypted-volume-new
encryptedvolume.crypto.example.com "luks-encrypted-volume-new" deleted
```

```
[2026-07-13 17:19:51,296] kopf.objects         [DEBUG   ] [default/luks-encrypted-volume-new] Handler 'cleanup_resources' is invoked.
[2026-07-13 17:19:51,296] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Cleanup triggered for luks-encrypted-volume-new
```

```
[2026-07-13 17:19:51,312] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Janitor successfully closed the LUKS device.
[2026-07-13 17:19:51,313] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] check jwt: eyJhbGciOiJSUzI1NiIsImtpZCI6ImpPbG93TT
```

```
[2026-07-13 17:19:51,587] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] PVC csi-pvc-cinder-for-luks deleted.
[2026-07-13 17:19:51,588] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Final cleanup for luks-encrypted-volume-new complete. Finalizer will be removed.
[2026-07-13 17:19:51,589] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Handler 'cleanup_resources' succeeded.
[2026-07-13 17:19:51,589] kopf.objects         [INFO    ] [default/luks-encrypted-volume-new] Deletion is processed: 1 succeeded; 0 failed.
```

UNIVERSITY OF CAMBRIDGE

Thank You