Secrets Rotation of Environment Variables and Mounted Secrets in Pods

This document covers some ways you can do secret rotation with environment variables and mounted secrets in Kubernetes pods

Mapping Secrets via secretKeyRef with Environment Variables

If we map a K8s native secret via a `secretKeyRef` into an environment variable and we rotate keys the environment variable is not updated even though the K8s native secret has been updated. We need to restart the Pod so changes get populated. Reloader solves this issue with a K8S controller.

```
...
    env:
        - name: EVENTHUB_CONNECTION_STRING
          valueFrom:
            secretKeyRef:
              name: poc-creds
              key: EventhubConnectionString
...
```

Mapping Secrets via volumeMounts (ESO Way)

If we map a K8s native secret via a volume mount and we rotate keys the file gets updated. The application needs to then be able pick up the changes without a restart (requiring most likely custom logic in the application to support this). Then no restart of the application is required.

```
...
    volumeMounts:
    - name: mounted-secret
      mountPath: /mnt/secrets-store
      readOnly: true
  volumes:
  - name: mounted-secret
    secret:
      secretName: poc-creds
...
```

Mapping Secrets via volumeMounts (AKVP SSCSID Way)

SSCSID focuses on mounting external secrets into the CSI. Thus if we rotate keys the file gets updated. The application needs to then be able pick up the changes without a restart (requiring most likely custom logic in the application to support this). Then no restart of the application is required.

```
...
    volumeMounts:
    - name: app-secrets-store-inline
      mountPath: "/mnt/app-secrets-store"
      readOnly: true
  volumes:
  - name: app-secrets-store-inline
    csi:
      driver: secrets-store.csi.k8s.io
      readOnly: true
      volumeAttributes:
        secretProviderClass: akvp-app
      nodePublishSecretRef:
        name: secrets-store-sp-creds
...
```

Last update: August 22, 2024