Used for the encryption off secrets within a file that we're committing to source control - specifically those in helm charts.

SOPS: Secrets OPerationS

**sops** is an editor of encrypted files that supports YAML, JSON, ENV, INI and BINARY formats and encrypts with AWS KMS, GCP KMS, Azure Key Vault, age, and PGP.

Shape

Description automatically generated with medium confidence

**Some advantages** comparing to other solutions:

* Designed and published by [Mozilla Corporation](https://en.wikipedia.org/wiki/Mozilla_Corporation) under Mozilla Public License 2.0
* Encrypts only values. This is important for tracking changes in a version control system.
* Supported by helm (via plugin)
* Supports many file formats and secrets store providers

Please check [GitHub repository](https://github.com/mozilla/sops) for further details.

Installation

Vault Configuration

Instructions are at <https://github.com/mozilla/sops#25encrypting-using-hashicorp-vault>, can be done via the vault UI as well. Perform the workstation setup first.

It is highly important to remember that deleting the sops secret in hashicorp vault will remove all access to encrypted secrets and cannot be recovered.

Windows Workstation Setup

1. Request access access to [Hashicorp Vault](https://confluence.westpac.co.nz/display/BUSINESS/Hashicorp+Vault) name space
2. Install vault cli (see [Set up Vault CLI](https://stash.westpac.co.nz/projects/CLOUD/repos/knowledgebase/browse/vault/on-boarding.md))
3. Download the latest stable sops binary release from <https://github.com/mozilla/sops/releases> (currently [sops-v3.7.1.exe](https://github.com/mozilla/sops/releases/download/v3.7.1/sops-v3.7.1.exe)) (I had to use chrome as it was blocked as a security risk in edge).
   * Copy the sops binary to your %PATH% directory and rename to sops.exe. (We prefer C:\bin for kubectl, helm, sops, terraform)
4. Download and install [gpg4win](https://gpg4win.org/download.html) (possibly not required anymore)
5. Install helm plugin

|  |
| --- |
| helm plugin install https://github.com/jkroepke/helm-secrets |

* + Under Windows version 3.13.0-dev worked where version 3.9.2-dev failed
  + *This installed the dev version rather than latest release version - needs investigating*

1. Set vault information and editor from command line

|  |
| --- |
| # Temporary  SET VAULT\_ADDR=https://vault.westpac.co.nz  SET VAULT\_NAMESPACE=azure\_devops  SET EDITOR="C:\\Program Files\\Microsoft VS Code\\bin\\code.cmd" --wait    # Permanent  SETX VAULT\_ADDR https://vault.westpac.co.nz  SETX VAULT\_NAMESPACE azure\_devops  SETX EDITOR="\"C:\\Program Files\\Microsoft VS Code\\bin\\code.cmd\" --wait" |

1. Test login (replacing the username with your salary id)

|  |
| --- |
| vault login -method=ldap username=M773407 |

Usage

The process for setting this up is:

1. Login to vault using the instructions above
2. Create a .sops.yaml configuration file in the root directory of your project to define which keys are used for which filename. We suggest using \*.enc.yaml file extension for encrypted secrets.

**.sops.yaml**

|  |
| --- |
| creation\_rules:    - path\_regex: '(secrets.\*\.yaml|.\*\.enc\.yaml)$'      hc\_vault\_transit\_uri: "[https://vault.westpac.co.nz/v1/sops/keys/helmsecrets"](https://vault.westpac.co.nz/v1/sops/keys/helmsecrets) |

1. Encrypt a secrets file (note: file name must be named "secrets.\*.yaml")

|  |
| --- |
| sops --verbose -e secrets.dec.yaml > secrets.enc.yaml |

1. Decrypt in your favourite editor

|  |
| --- |
| sops <file name> |

1. Decrypt by helm plugin

|  |
| --- |
| # show plain text in stdout  helm secrets view secrets.enc.yaml  # installation example  helm secrets -n NS upgrade --install HELMRELEASE HELMREPO -f values.yaml -f secrets.enc.yaml  # or  helm -n NS upgrade --install HELMRELEASE HELMREPO -f values.yaml -f secrets://secrets.enc.yaml |