

Sops avec Age

Définitions

Sops : Simple and flexible tool for managing secrets
(<https://github.com/getsops/sops>)

Age : A simple, modern and secure encryption tool (and Go library) with small explicit keys, no config options, and UNIX-style composability. (<https://github.com/FiloSottile/age>)

Installation

Sops

```
→ curl -LO https://github.com/getsops/sops/releases/download/v3.8.1/sops  
→ chmod 755 sops-v3.8.1.linux.amd64  
→ sudo cp ... /usr/local/bin/...; sudo chown ...
```

ou pour la démo

```
→ mv sops-v3.8.1.linux.amd64 sops
```

Age

```
→ sudo apt install age
```

Age : Création d'un jeu de clés

→ `age-keygen -o key.txt`

Public key: `age1f65fuqjfh2qhzrsn7gw75p5enwgdn9a282m80pvl0kdxrmpwcrsv8ll`

→ `cat key.txt`

created: 2024-03-27T09:56:43+01:00

public key: `age1f65fuqjfh2qhzrsn7gw75p5enwgdn9a282m80pvl0kdxrmpwcrsv8`

`AGE-SECRET-KEY-1QG6TV2GV3PMWS0LPV0F3D0NPG3YJCCFM9H5FMJGP684N5YDKV56QMFHA`

Exemple pour SOPS

```
→ cat <<EOF > exemple.yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
data:
  username: root
  password: sup3rs3cr3tp4ssword
EOF
```

Sops en action

Chiffrer

```
→ sops --encrypt \  
    --age "age1f65fuqjfh2qhzrsn7gw75p5enwgdn9a282m80pvl0kdxrmpwcrsv8" \  
    --encrypted-regex '^(data|stringData)$' \  
    --in-place \  
    ./exemple.yaml
```

Note : on utilise ici la clé publique

```
→ cat exemple.yaml
```

Sops en action

Déchiffrer

```
→ export SOPS_AGE_KEY_FILE=$(pwd)/key.txt  
→ sops --decrypt --in-place ./exemple.yaml
```

Note : on utilise ici la clé privée

```
→ cat exemple.yaml
```

Sops avec Flux

1. Créer un secret avec le contenu de `key.txt` (exemple : `sops-age`)
2. Créer de la magie

```
apiVersion: kustomize.toolkit.fluxcd.io/v1beta1
kind: Kustomization
...
spec:
  decryption:
    provider: sops
    secretRef:
      name: sops-age
```

3. Laisser la magie opérer

Conclusion

Dans les temps anciens, au lieu de chiffrer des fichiers entiers avec Gpg, on aurait pu le faire de façon ciblée avec Sops et Age (ou Sops et Gpg).

On pourrait même améliorer avec

<https://devops.datenkollektiv.de/using-sops-with-age-and-git-like-a-pro.html>

Flux gère Sops et Age (Sops et Gpg). Cependant, il est probable que nous utilisions plutôt le backend Vault.