# SOPS CLI Cheatsheet

## Subcommands

| key | file | secret | script | service |
|---|---|---|---|---|
| updatekeys | edit | set | exec-env | publish |
| groups add | filestatus | unset | exec-file | keyservice |
| groups delete | rotate | encrypt | | |
| | | decrypt | | |

## Common options

I'm unsure whether these are global options

### Misc

| option | | arg? | default | delimiter | env | |
|---|---|---|---|---|---|---|
| -h | --help | | | | | show help |
| -v | --version | | | | | print the version |
| | --check-for-updates | | | | | do check whether the current version is latest during `--version` |
| | --disable-version-check | | | | `SOPS_DISABLE_VERSION_CHECK` | do not check whether the current version is latest during `--version` |
| | --verbose | | | | | |

### Config

**--keyservice $svc**
    can specify repeated `protocol://address` e.g. `tcp://myserver.com:5000`

**--filename-override $file**
    use the provided argument for loading configuration, and for determining input type and output type

| option | arg? | default | delimiter | env | |
|---|---|---|---|---|---|
| --config | value | | | `SOPS_CONFIG` | Prevents recursive search for .sops.yaml |
| --filename-override | file | | | | Use this filename instead |

### Action

**--set $json**
    edit mode only. json only.
    - example: `'["somekey"][0] {"somevalue":true}'`

**--extract $key**
    example `'["somekey"][0]'`

| | option | arg? | |
|---|---|---|---|
| | --set | json | set specific key or branch in the input document |
| -d | --decrypt | | decrypt file; output to stdout |
| -e | --encrypt | | encrypt file; output to stdout |
| -r | --rotate | | generate a new data encryption key; reencrypt all values with new key |
| -i | --in-place | | write output back to the same file instead of stdout |
| | --extract | key | extract a specific key or branch from the input document. Decrypt mode only. Example: |

| | option | arg? | |
|---|---|---|---|
| | --input-type | format | json, yaml, dotenv and binary; defaults to using extension |
| | --output-type | format | json, yaml, dotenv and binary; defaults to using extension |
| | --output | file | Save output after encryption/decryption to the file specified |

## Backends

All of these except AWS Profile accept a comma-separated list.

**--add-\***
    add to the list of master keys on the given file
**--remove-\***
    remove from the list of master keys on the given file

| | option | arg? | env | desc |
|---|---|---|---|---|
| | --aws-profile | profile | | AWS profile for requests to AWS |
| -k | --kms | KMS ARNs | `SOPS_KMS_ARN` | |
| | --add-kms | KMS ARNs | | |
| | --rm-kms | KMS ARNs | | |
| | --gcp-kms | KMS Resource IDs | `SOPS_GCP_KMS_IDS` | |
| | --add-gcp-kms | KMS Resource IDs | | |
| | --rm-gcp-kms | KMS Resource IDs | | |
| | --azure-kv | Azure KV URLs | `SOPS_AZURE_KEYVAULT_URLS` | |
| | --add-azure-kv | Azure KV URLs | | |
| | --rm-azure-kv | Azure KV URLs | | |
| | --hc-vault-transit | Vault Key URIs | `SOPS_VAULT_URIS` | |
| | --add-hc-vault-transit | Vault Key URIs | | |
| | --rm-hc-vault-transit | Vault Key URIs | | |
| -a | --age | Age Recipients | `SOPS_AGE_RECIPIENTS` | |
| | --add-age | Age Recipients | | |
| | --rm-age | Age Recipients | | |
| -p | --pgp | PGP FPs | `SOPS_PGP_FP` | |
| | --add-pgp | PGP FPs | | |
| | --rm-pgp | PGP FPs | | |

## Crypto Handling

| | option | arg? | default | delimiter | env | desc |
|---|---|---|---|---|---|---|
| | --shamir-secret-sharing-threshold | n master keys | 0 | | | For the `data key` key retrieval. |
| | --ignore-mac | | | | | ignore MAC during decryption |
| | --mac-only-encrypted | | | | | compute MAC only over values which end up encrypted |
| | --encryption-context | value | | comma | | KMS encryption context `key:value` pairs |
| | --decryption-order | key types | | comma | `SOPS_DECRYPTION_ORDER` | list of decryption key types |
| -s | --show-master-keys | | | | | display master encryption keys in the file during |
| | --enable-local-keyservice | | | | `SOPS_ENABLE_LOCAL_KEYSERVICE` | |
| | --keyservice | value | | | `SOPS_KEYSERVICE` | Key services, in addition to local |

## Formatting

| option | arg? | default | desc |
|---|---|---|---|
| `--indent` | n spaces | default `0` | |
| `--encrypted-suffix` | suffix | override the encrypted key suffix. | When empty, all keys will be encrypted, unless otherwise marked with unencrypted-suffix. |
| `--unencrypted-suffix` | suffix | override the unencrypted key suffix. | |
| `--unencrypted-regex` | regex | Unencrypted key regex. | When specified, only keys matching the regex will be left unencrypted. |
| `--encrypted-regex` | regex | Encrypted key regex. | When specified, only keys matching the regex will be encrypted. |
| `--unencrypted-comment-regex` | suffix | Unencrypted comment suffix. | When specified, only keys that have comment matching the regex will be left unencrypted. |
| `--encrypted-comment-regex` | suffix | Encrypted comment suffix. | When specified, only keys that have comment matching the regex will be encrypted. |

| | options | | | |
|---|---|---|---|---|
| exec-env | pristine | user | background, same-process | keyservice |
| exec-file | {input,output}-type, filename | user | no-fifo | keyservice |

## Service

| | options | | | |
|---|---|---|---|---|
| publish | recursive, omit-extensions | | verbose | keyservice |
| keyservice | addr, net | prompt | verbose | |

Created: 2025-11-17 Mon 05:31

# Subcommand Options

Summaries of options for subcommands are incomplete

## Key

| | options | | | |
|---|---|---|---|---|
| updatekeys | input-type, yes | | | keyservice |
| groups add | file, in-place | kms (value only) | shamir | keyservice |
| groups delete | file, in-place | | shamir | keyservice |

## File

| | options | | | |
|---|---|---|---|---|
| edit | {input,output}-type | kms (value only), context, aws profile | un/encrypted suffix/ regex | shamir, decryption order |
| rotate | {input,output}-type, output | kms (add/rm only), context | | |
| filestatus | {input,output}-type | | | |

## Secret

| | options | | | | |
|---|---|---|---|---|---|
| set | yes, {input,output}-type | idempotent, value-{file,stdin} | | shamir, ignore-mac, decryption-order | keyservice |
| unset | yes, {input,output}-type | idempotent | | shamir, ignore-mac, decryption-order | keyservice |
| encrypt | {input,output}-type, output, in-place | {un,}encrypted-{regex,suffix} | kms | shamir, encryption-context | keyservice |
| decrypt | {input,output}-type, output, in-place | filename-override | | | keyservice |

`--idempotent`
    `set` does nothing if index already exists,
- `unset` does nothing when the index doesn't exist

## Script

| | options | | | |
|---|---|---|---|---|