Client-Side Data Encryption with Public Cloud Object Storage Systems for Both Individuals and Groups

rclone – S3
XSalsa20 – Poly1305
AES – PKCS#7 – EME – BASE32

Dominik Pantůček <dominik.pantucek@trustica.cz>

Trustica

13th October 2024

Agenda

- Background Information
- Object Storage
- Synchronization Tool: rclone
- Encryption Layer: crypt remote
- Configuration Protection
- Sharing Secrets
- Configuration Encryption
- Latest Improvements
- Questions & Answers

Background Information

- Cryptography (since 1999)
- Security Consultancy Company (since 2002)
- Brmlab Hackerspace (since 2010, founding member)
- Programming Language Theory (formally since 2015)
- Racket Development (since 2019)
- Securing Cloud Storage for Research Teams (since 2024)

Object Storage

- Key-Value Pairs
- Similar to Files
  - but not the same
- Directories
  - usually do not exist as standalone thing
  - can be simulated within object names
- S3 - Simple Storage Service
- Access
  - Connection End-Point
  - Access Credentials
  - ACCESS_KEY_ID
  - SECRET_ACCESS_KEY

Synchronization Tool: rclone

- Like rsync and/or mount
- Commonly used features:
  - sync
  - bisync
  - mount
- Terminology:
  - remote – specification of remote storage as seen by rclone user
  - endpoint – object storage specific network endpoint (typically URL)
  - access credentials – usernames, passwords, access keys ...

Example: S3 Remote Configuration

```
[s3-clean]
type = s3
provider = Ceph
access_key_id = QUAITIX7ACH0XEIZAI2E
secret_access_key = Oy7eethoupa5op0aifejuashedei6yeequuquie6
endpoint = s3.example.com
acl = private
```

Mount Remote

```
$ rclone mount --daemon s3-clean: s3-clean-dir/

$ df -h s3-clean-dir/
Filesystem      Size  Used Avail Use% Mounted on
s3-clean:   1,0P     0  1,0P   0% /home/.../s3-clean-dir

$ umount s3-clean-dir/
$
```

Encryption Layer: crypt remote

- Works with actual storage remote
- Uses symmetric encryption with shared key derived from:
  - Passphrase
  - Salt
- Both key and salt are slightly obscured in the configuration
  - AES-CTR with fixed key + BASE64 encoding
  - Does not protect from decoding
  - Protects from looking over user's shoulder
- Cryptographic Model
  - KDF: SCrypt(N=16384, r=8, p=1)
  - Data: XSalsa20-Poly1305 (secretbox)
  - Meta-data (only names)
    - Padding: PKCS#7
    - Cipher: AES/EME (Encrypt-Mix-Encrypt)
    - Encoding: BASE32, BASE64, BASE32768

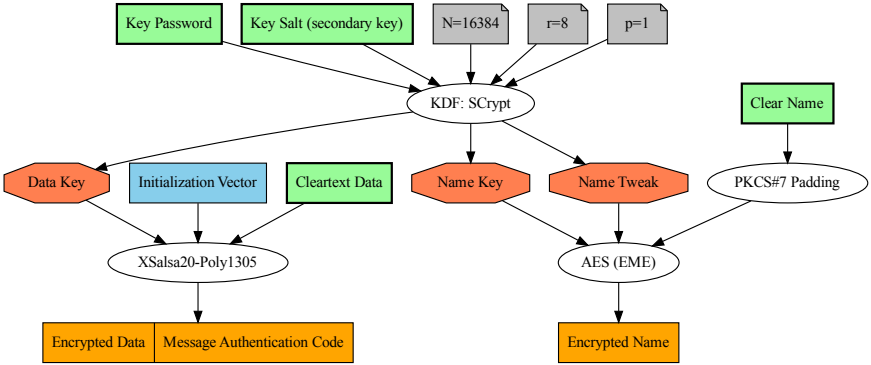
Example: Crypt Remote Configuration

```
[s3-clean]
type = s3
provider = Ceph
access_key_id = QUAITIX7ACH0XEIZAI2E
secret_access_key = Oy7eethoupa5op0aifejuashedei6yeequuquie6
endpoint = s3.example.com
acl = private

[s3-encrypted]
type = crypt
remote = s3:data
password = TUUXhgLbND28r63XfnG1W7wxqyUrHVmu
password2 = ac5bb_7XutO_VBU87DYGnua-k_s
```

Mount Encrypted Remote

```
$ rclone mount --daemon s3-encrypted: s3-encrypted-dir

$ ls s3-encrypted-dir/
-rw-rw-r-- 1 joe joe 13 Oct  8 09:06 hello.txt

$ rclone mount --daemon s3-clean: s3-clean-dir

$ ls s3-clean-dir/data/
-rw-rw-r-- 1 joe joe 61 Oct  8 09:06 kbebacp7h18dqaul8jap7octdk

$ umount s3-encrypted-dir
$ umount s3-clean-dir
$
```

Crypt Remote: Cryptographic Schema



Sharing Secrets

- Multiple People
- Single Key
- Multiple Locations of Secret Key Material
- Multiple Risks

Configuration Protection – Encryption

- Optional configuration file encryption
- Symmetric key derived from passphrase
- KDF: SHA2-256
- No Salt but Pepper is used
  - Prefix: `"["`
  - Suffix: `"][rclone-config]"`
- Cipher: XSalsa20-Poly1305 (secretbox)

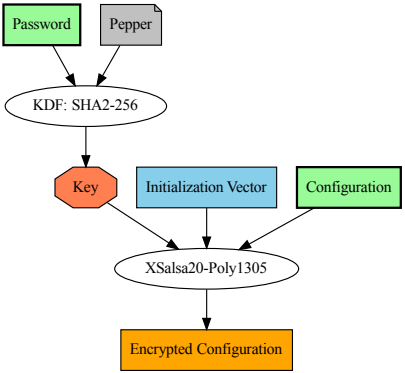
Example: Encrypted Configuration

```
# Encrypted rclone configuration File

RCLONE_ENCRYPT_V0:
4txRCT0zoOCNN+HfG5b4B09QJ0kOo2hltlFJazPcaa+ddVVqh9uhKxU/sAn5IHiYBOy6TP5XVXp9L/aBJRwNPEC5ilGud
UAGeCKQJQkNkMOz5jjk+OMrBdDgznwyy3d/xPYG4gheCUN1jrm3dqM3uw9YCMLS9j1Jul82uDYZuD+s7wfKvBHtGQ+/IM
O0nNADCiTsIErsdOKdwmXRiSJwtqn33zOd6ZCLwgBlWlSd+53XAaqs3vhTgopPbhl7yFlR/gX9IHpkPGdi+DJEbsjUIN1
Q65rpO+Yde5FwvCTSM/XwfD2f6OHhK1QUHLJ+Fjw1T2scUKTiwSJyEOKBPBXKqbHYAf9s5ANACPssvD/YzrWNshIUoVFo
qUeXhwePNa+Fc2Z3pFL5PRX8+nF+uf/8DUSWQg5PRdUX3QcCM364GA+puqGM87bW4eOHY52lV8uJ5DbU1/DDcKkGdpdvM
TaT22WSMg/LEJ0qCMdcRYz504huDzzlonLnb2R4UbXcZbO+VAHf/EiBQ+imEqbVFbhez7Uco7VZ1LHsuWr7x1AbuN2Q+v
Ut/1LGY78QDf8vHWDK7xmBMQzBv0modJxszVLIFuBxO0UEqgcJ2J914FY1qC+LYSjcNPrglhQDoB4WyrXI4muSMhhQpq5
Gb893Q+tmZN+Fpd7y84M5jgM+U+hpnDkswsdOW7kr64KfsyV5q3Ip17EjE9VLeu6qqquQfoCzFSOSru0h4Hty+tzmHCbw
n1ygBtpXRXtVVCqflD5PuDiA7xQCon9taQbIpV8gJwOL6v3yjXEjf7qSO/phVLnKV2bCkh5OLFuYi3Yqh6JrJPTjRDakP
ckzaZp0Ywt22CPjKGvnUqtpmLL/W4HFLfTkZUeFyP9d1D9mqjnr4u0qM1Y+PQvQ93JEzGMT2KdeuW81J96gLBnySQAwYT
YPb2XVe9yxjiXx58B9oWiIPM7QtpU9z6TOpv8aJDMDw3rclSpKvFlYfboLF1focB6MQ7MsBclRuI/nMCpS616QGTRVyKR
p3/7iTDYa21/HWeWAj0Tu+nJEoxY8y+q1B/Ypy2TMeapkISYOmJ+LNtc=
```

Mount Encrypted Remote from Encrypted Configuration

```
$ rclone mount --daemon s3-encrypted: s3-encrypted-dir

Enter configuration password:
password:

$
```

Configuration Encryption: Cryptographic Schema



Latest Improvements: rclone 1.68

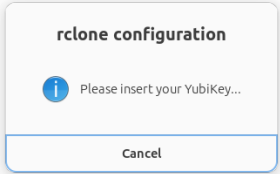
- New version: rclone 1.68, released 8th September 2024
- Important ChangeLog Items (all by Nick Craig-Wood)
- New commands
  - config encryption: set, remove and check to manage config file encryption
- New Features
  - config
    - Internal config re-organised to be more consistent and make it available from the rc
    - Use –password-command to set config file password if supplied

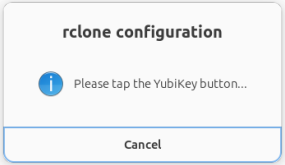
Latest Improvements Results

- External Application for Password Input
  - Pinentry
  - Zenity
- Password Managers
  - MacOS
  - Windows
  - GNOME Keyring
- YubiKey support
  - Does not protect against scanning RAM for the key

Mount Remote from YubiKey-Protected Configuration

```
$ rclone --password-command ykrcpw.sh \
   mount --daemon s3-encrypted: s3-encrypted-dir

$
```





Future Work

- CEK: Content Encryption Keys
  - Each file encrypted with unique symmetric key
  - Ability to reencrypt only CEKs
  - May be used for sharing securely single objects
- KMS: Key Management System (2025)
  - With reencrypting all CEKs ...
  - Unlocking Master Key using multiple User Keys
  - Finally: User Key Revocation

Questions & Answers

Your Questions ...

... and my Answers

Thank you and enjoy the rest of LinuxDays!