

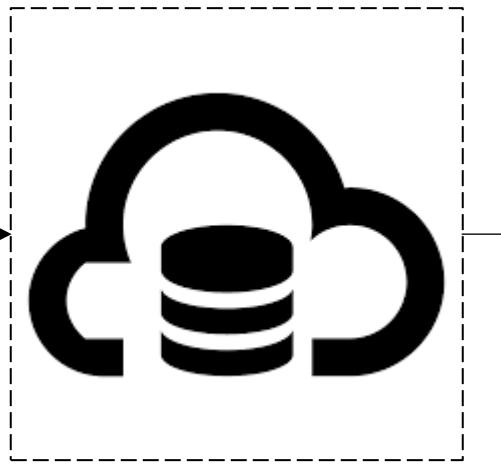
## Manager



## Member/Encrypt



## Cloud

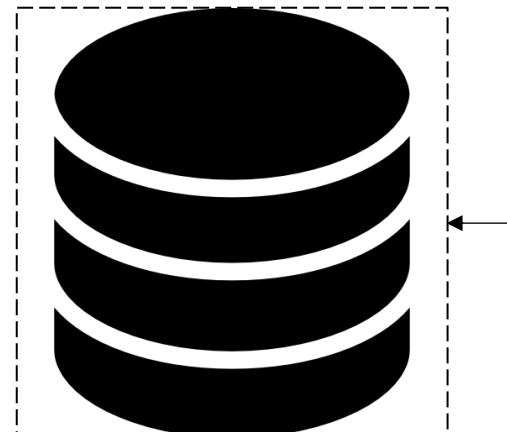


- Setup / KeyGen–Extract
- Issue KAC aggregate key (class subset)

- AES-GCM encrypt (fresh key + nonce)
- KAC wrap per file class  
Plaintext stays on Pi; header built locally  
RFID not required for encryption  
/etc/kac\_agg.json (0600)

- POST /upload/<name>Stores ciphertext + header only

## Storage



- Ciphertext + header