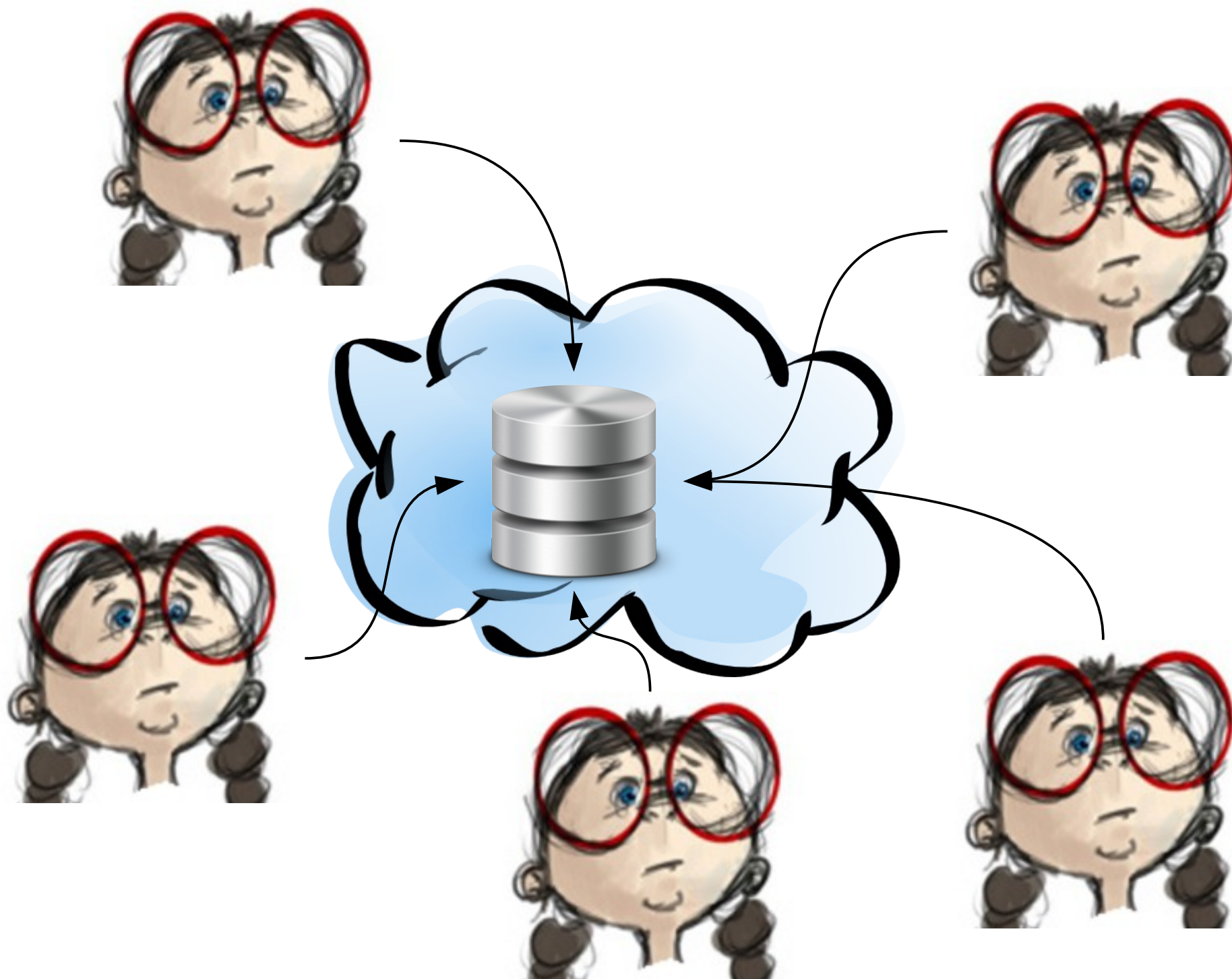


# ARVER

## distributed

## LUKS management

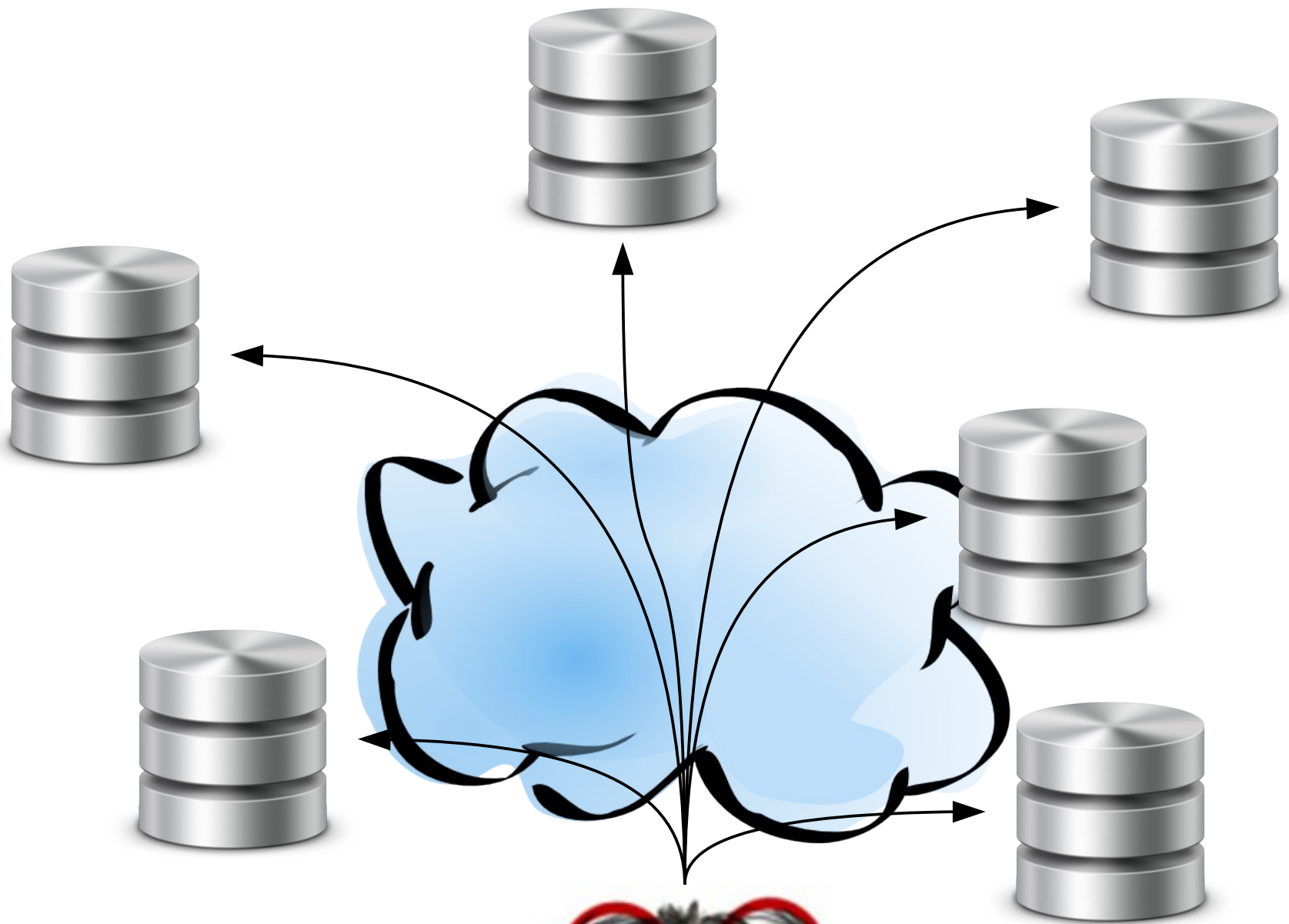


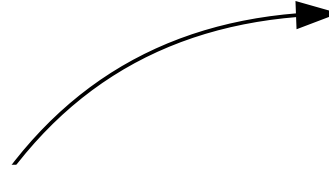


Share the

passwords?







Type 1000  
passwords?



**the Wishlist**

- ☒ Per-admin policy
- ☒ Key distribution
- ☐ Automation
- ☐ Deniability



# Linux Unified Key Setup:



Slot 1: Alice



Slot 2: (empty)



Slot 3: (empty)

...

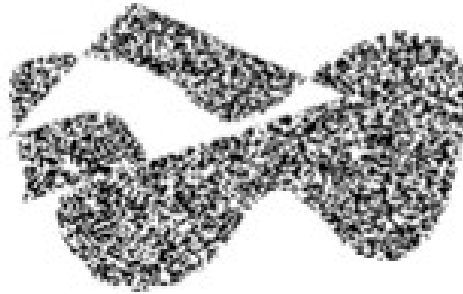


Slot 8: (empty)



**alice#: arver --add-user bob theDisk**

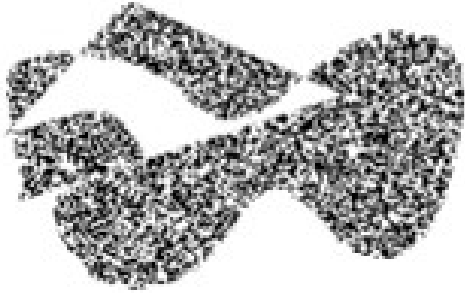
random LUKS key



Slot 2

(via SSH)

random LUKS key



Bobs GPG  
PublicKey



Bobs ARVER key  
for theDisk

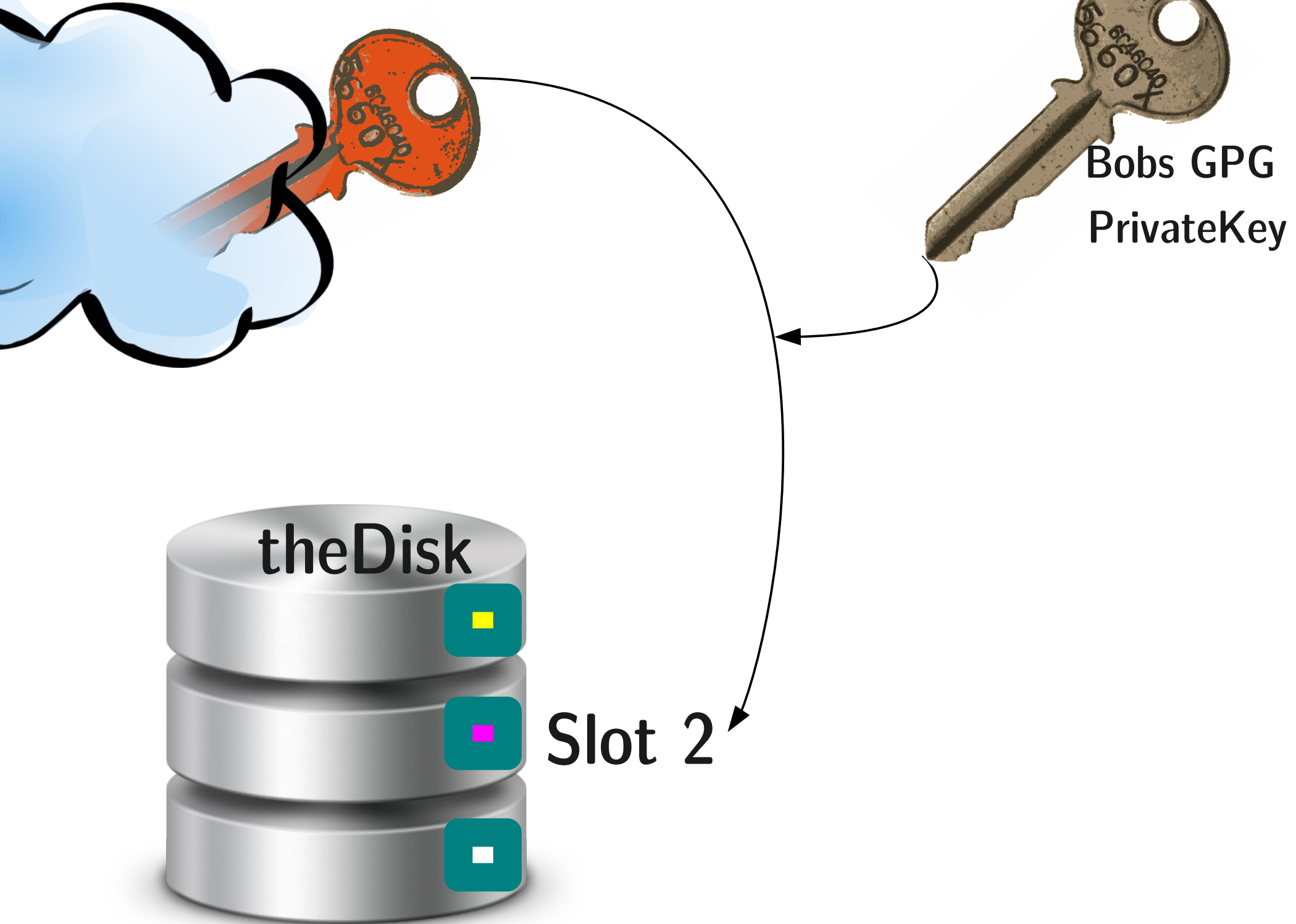




Bobs ARVER key  
(for theDisk)



**bob#: arver --open theDisk**



☐ Per-admin policy

☐ Key distribution

☒ Automation

☒ Deniability



# Examples

`arver --open /berlin/coloX`

`arver --del-user eve ALL`

`arver --garbage-collect`

# Future Work

## Shared Secret

## “Better” deniability

## Initrd integration

<https://git.codecoop.org/projects/arver>

<https://tech.immerda.ch/2011/08/arver-distributed-luks-key-management/>

[arver@lists.immerda.ch](mailto:arver@lists.immerda.ch)

6036 9F10 3542 9963 EAE9 B698 D4C1 6590 A6C0 C4BD