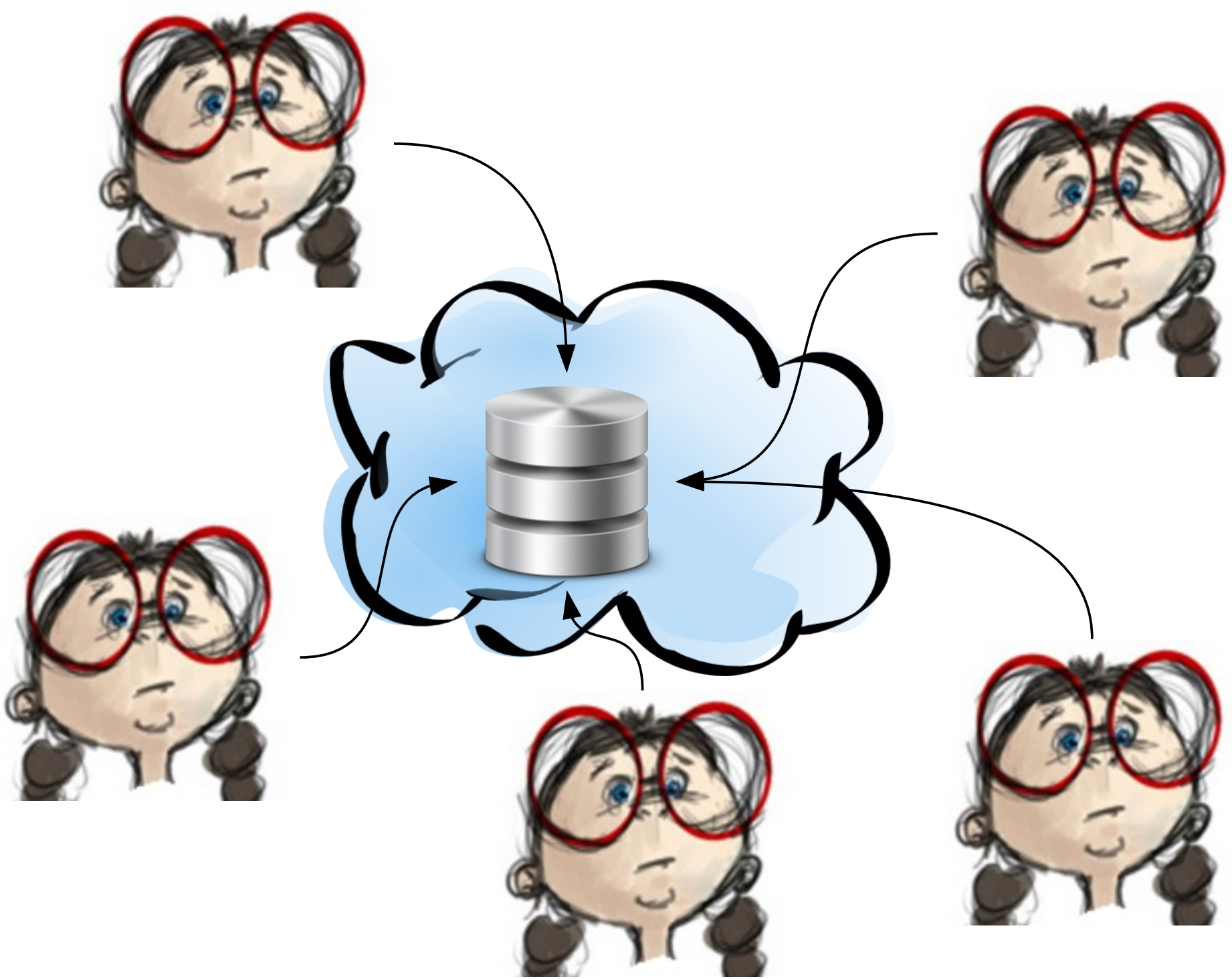
ARVER

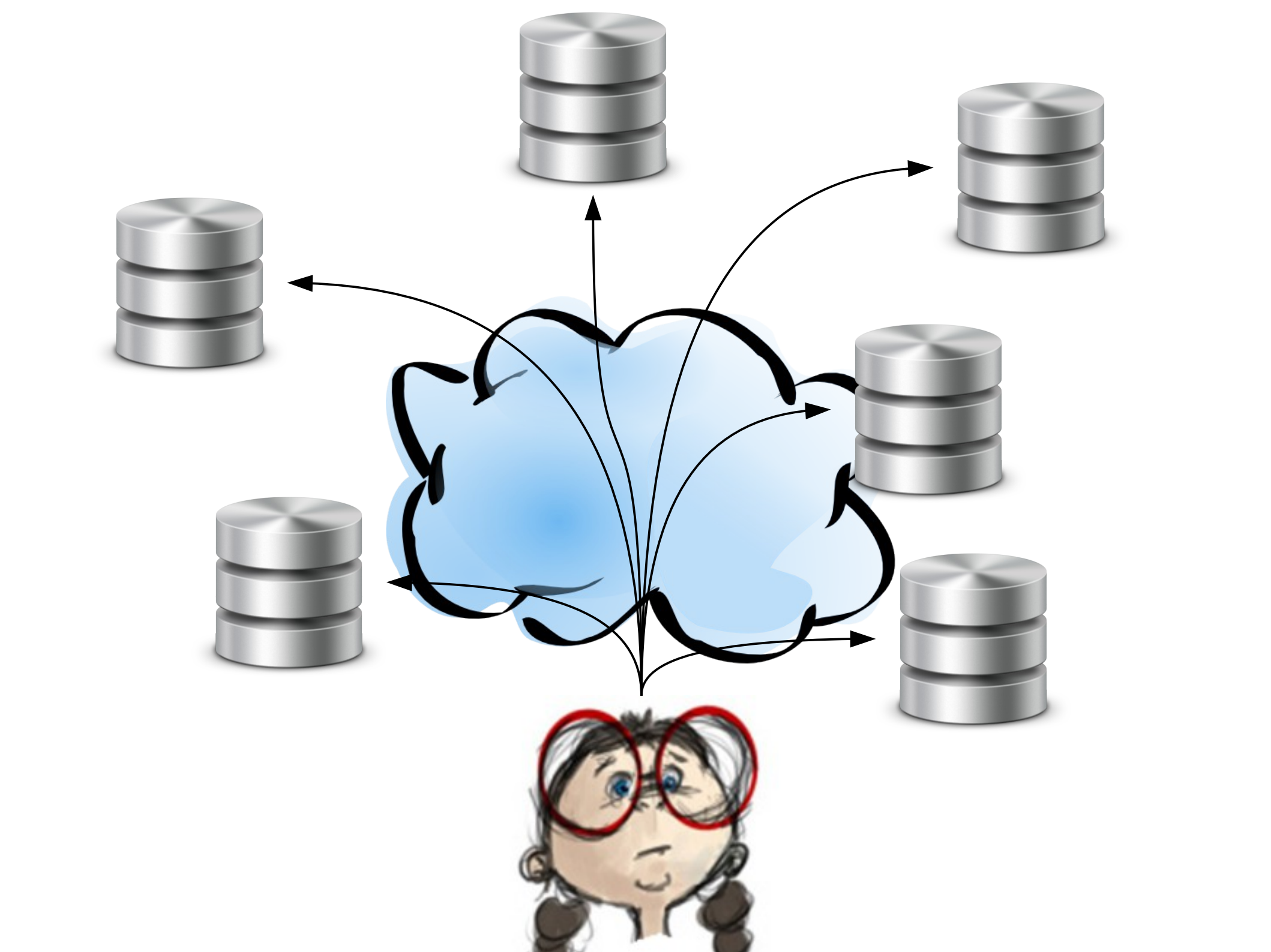
distributed

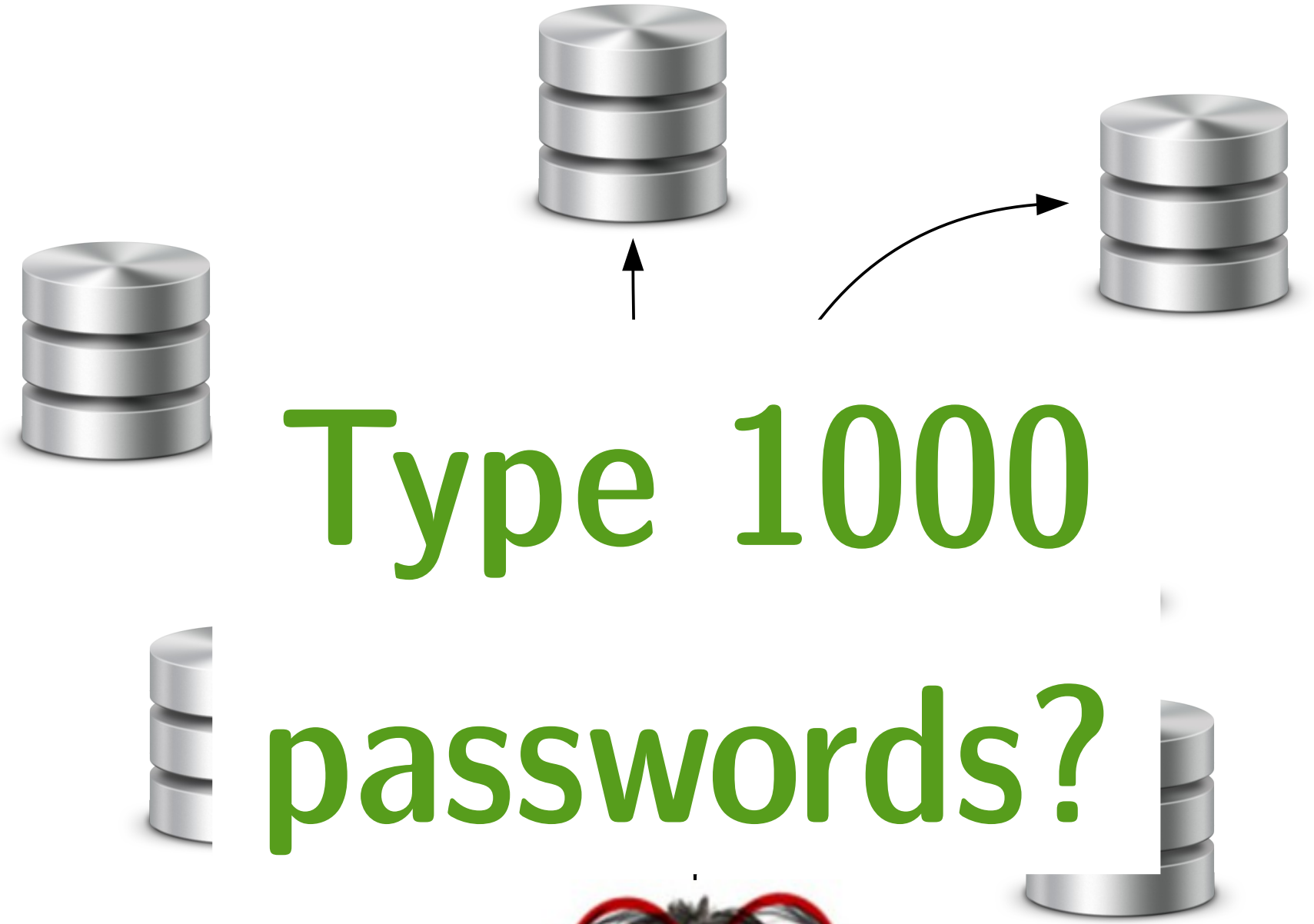
LUKS management

immerda.ch



Share the passwords?





Type 1000 passwords?

the wish list

- [x] Per-admin policy
- [x] Key distribution
- [ ] Automation
- [ ] Deniability

Linux Unified Key Setup:

Slot 1: Alice

Slot 2: (empty)

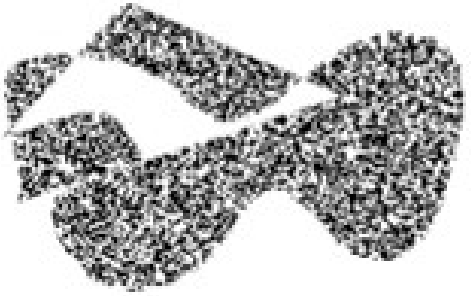
Slot 3: (empty)

...

Slot 8: (empty)

alice#: arver --add-user bob theDisk

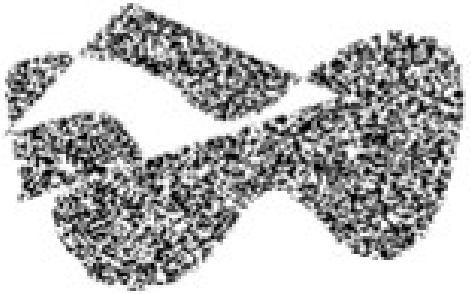
random LUKS key

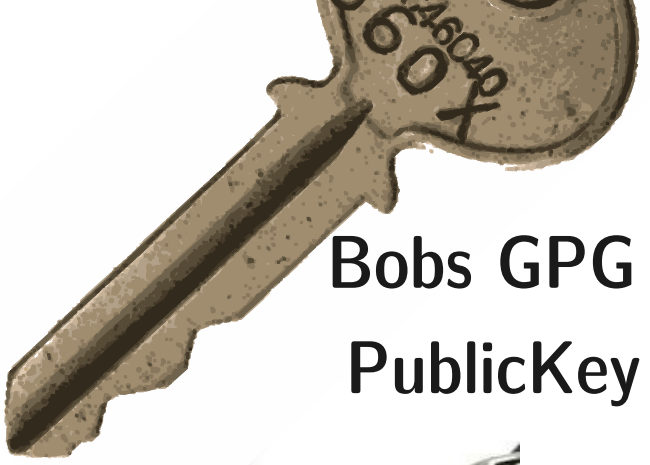


(via SSH)

Slot 2

random LUKS key





Bobs GPG
PublicKey

Bobs ARVER key
for theDisk

Bobs ARVER key

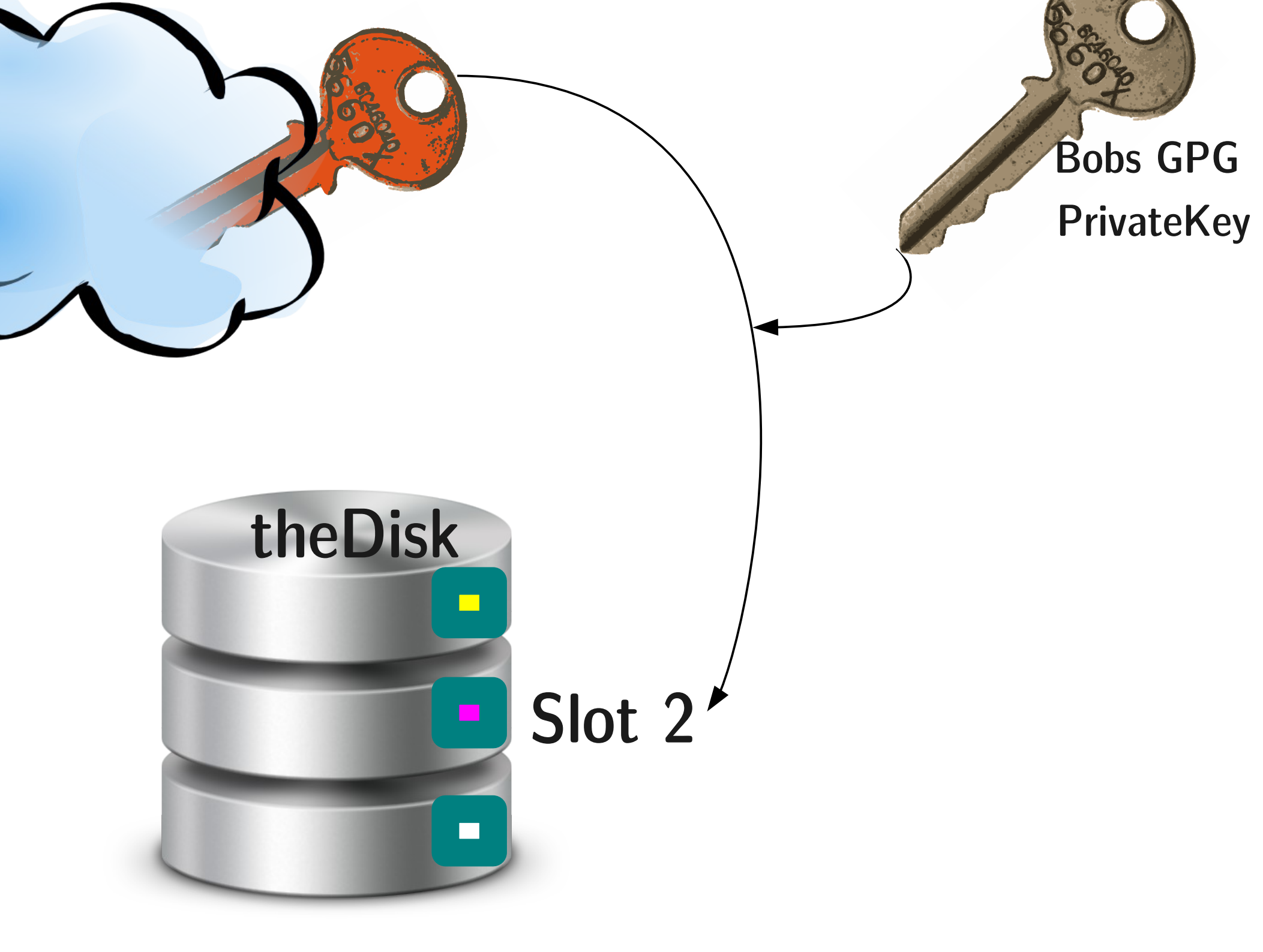
(for theDisk)

Mail

Git

...

bob#: arver --open theDisk


Bobs GPG
PrivateKey
theDisk
Slot 2

- [ ] Per-admin policy
- [ ] Key distribution
- [x] Automation
- [x] Deniability

Examples

arver --open /berlin/coloX

arver --del-user eve ALL

arver --garbage-collect

Future Work

Shared Secret

Other crypto stacks

(“Better” deniability)

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

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

arver@lists.immerda.ch

6036 9F10 3542 9963 EAE9 B698 D4C1 6590 A6C0 C4BD