Lesk a bída šifrování disků

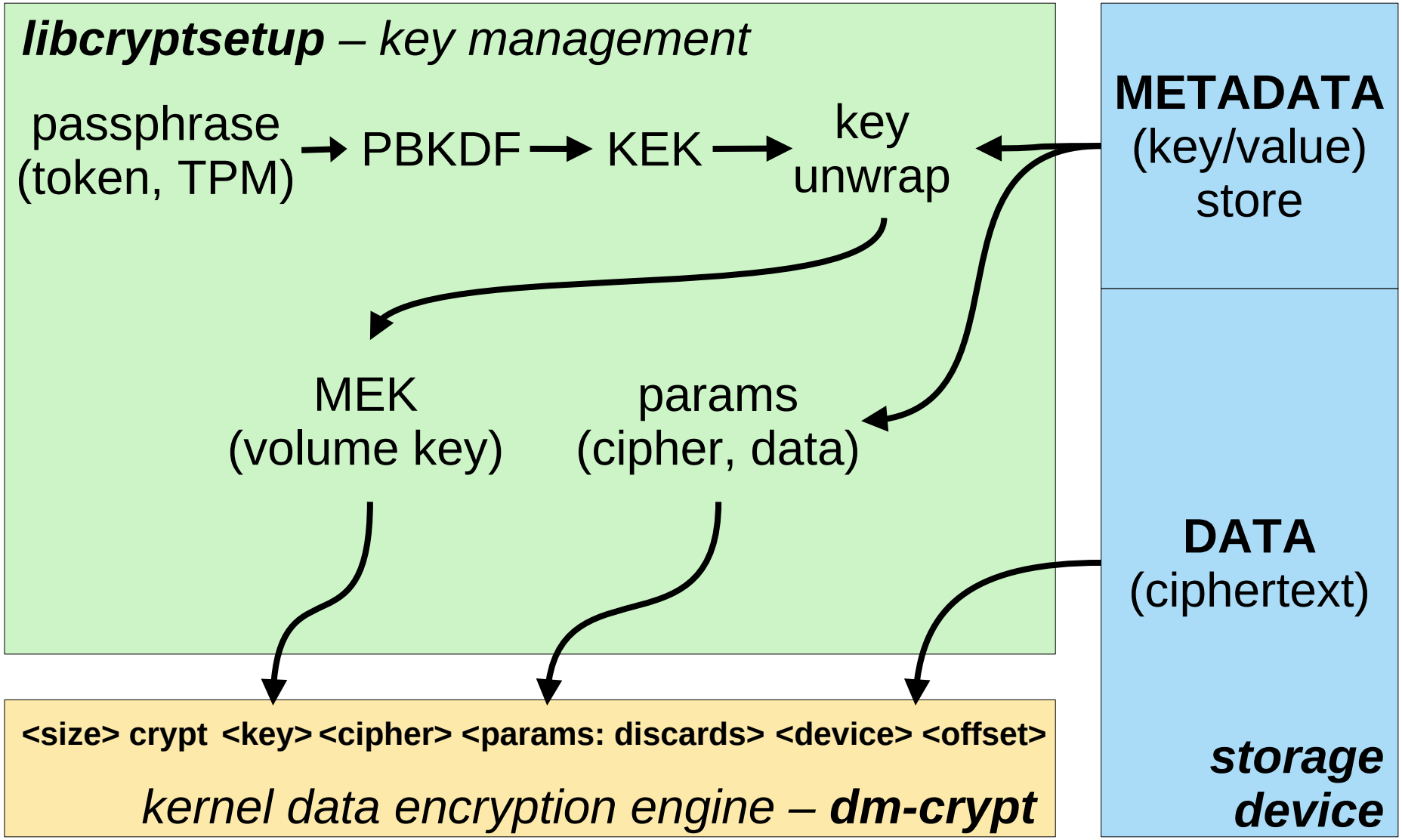
Milan Brož
milan.broz@mail.muni.cz

EurOpen 2022
Radešín

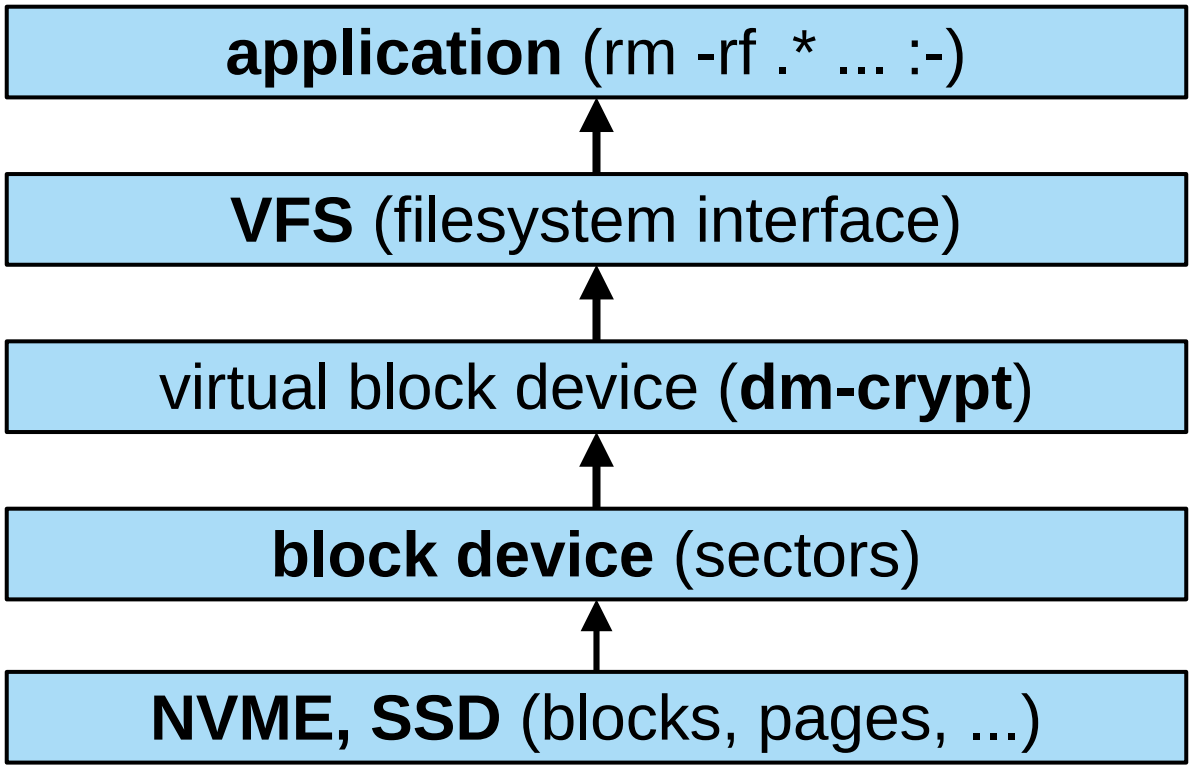
Šifrování disků

- Proč to (ještě) vlastně používáme?
  - ~~a co souborové systémy?~~
    ~~ZFS, btrfs, bcachefs, fscrypt~~
- Má smysl „podporovat“ proprietární formáty?
  - Jak sdílet šifrovaná data mezi OS
  - Data se obvykle ukládají na dlouhou dobu
    (a.k.a. „Proč ten backup už nejde otevřít?“)
- Jak to celé funguje v Linuxu
- Srovnání s LUKS

Linux: dm-crypt, libcryptsetup



Linux: storage layers*



/mnt/data

/dev/mapper/sdb_crypt

/dev/sdb

(driver)

*magic; simplified

Kryptografické knihovny

- dm-crypt – kernel crypto API
  - drivery, HW akcelerace
  - dm-crypt implementuje jen specifické IV
- libcryptsetup
  - OpenSSL
  - alt. gcrypt, Nettle, kernel user crypto API
- výjimky: Argon2, specifický key management

TrueCrypt, VeraCrypt

- Populární multiplatformní nástroj
- Prapodivná historie*
- Následovníci – dnes jen **VeraCrypt**
- **Metadata**
  - šifrovaná metadata, mnoho možných algoritmů
    - AES, Serpent, Twofish, Cammelia, Kuzniechik
    - XTS mód, zřetězené šifry
    - PBKDF2, PIM (Personal Iterations Multiplier)
  - skrytý disk (~dle zadaného hesla)

*konspirativní odbočka :-)

VeraCrypt na flashdisku – demo

- Fedora Workstation 36
- cryptsetup: příkazová řádka + kernel
  - podporuje i historické módy
- Integrace do desktop systému
  - podpora v udisks, GNOME desktopu
  - trik na automatickou aktivaci
    touch /etc/udisks2/tcrypt.conf
  - systemd – podpora v /etc/cryptab

VeraCrypt – cryptsetup open

```
# cryptsetup open --type tcrypt --veracrypt test.img test
Enter passphrase for test.img:
# mount /dev/mapper/test /mnt/tst
...

# cryptsetup status test
/dev/mapper/test is active.
  type:    TCRYPT
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: dm-crypt
  device:  /dev/loop12
  loop:    test.img
  sector size:  512
  offset:  256 sectors
  size:    130560 sectors
  skipped: 256 sectors
  mode:    read/write
```

VeraCrypt – cryptsetup dump

```
# cryptsetup tcryptDump test.img
Enter passphrase for test.img:
VERACRYPT header information for test.img
Version:        5
Driver req.:    1.b
Sector size:    512
MK offset:      131072
PBKDF2 hash:    sha512
Cipher chain:   aes
Cipher mode:    xts-plain64
MK bits:        512
```

BitLocker

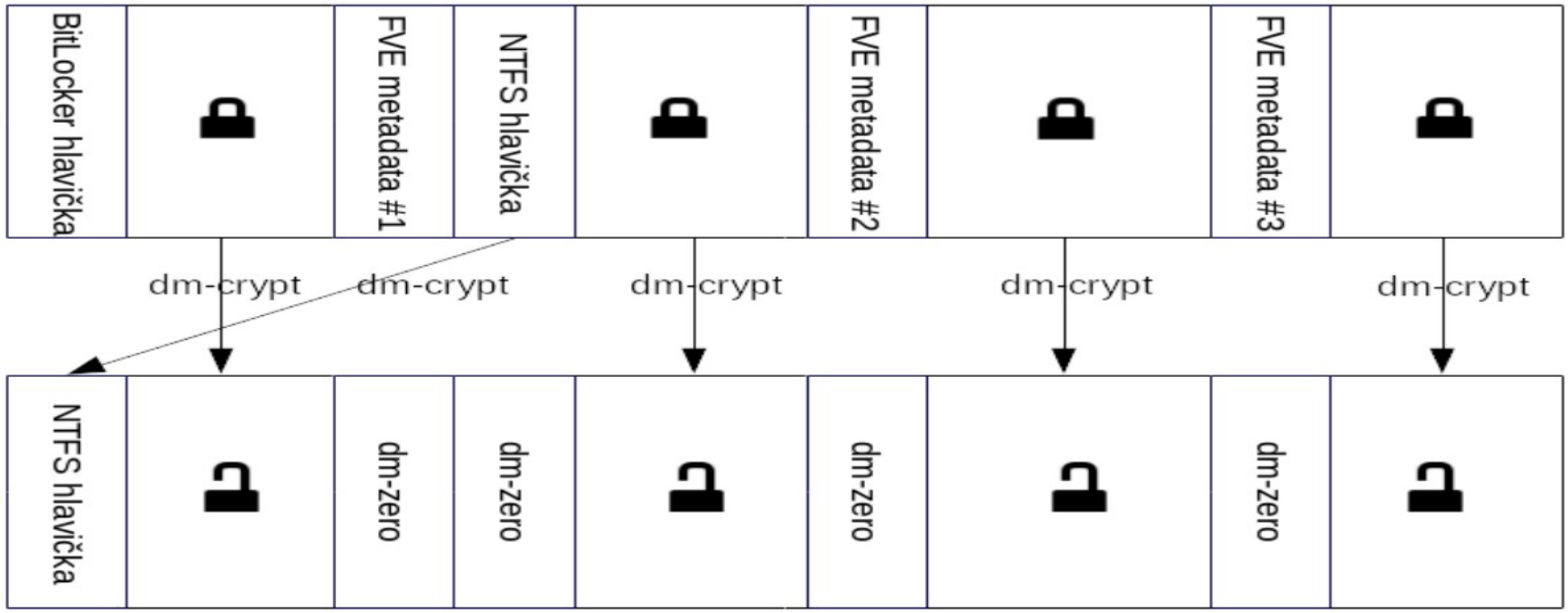
- Nativní šifrování disků ve Windows
- Varianta BitLocker to Go (flashdisky)
- Metadata „implantovaná“ do NTFS
  - ale souborový systém může být i FAT, exFAT
  - AES, XTS mód (dříve CBC + Elephant difuzer)
  - vlastní KDF založený na iteraci SHA256
  - key/value metadata
  - wrapping klíče AES-CCM (integrita!)

BitLocker – metadata

Metadata na disku:

Hl.	Data	FVE 1	Data	FVE 2	Data	FVE 3	Data

Metadata vymaskovaná přes dm-crypt:



BitLocker to Go – demo

- stejný systém jak u předchozího dema
- automatické odemčení
- NTFS read/write
- odemčení heslem, obnovovacím klíčem
- mapovací tabulka, dump metadat

BitLocker – cryptsetup open

```
# cryptsetup open --type bitlk /dev/sdb test
Enter passphrase for /dev/sdb:
# mount /dev/mapper/test /mnt/tst
...

# cryptsetup status test
/dev/mapper/test is active and is in use.
  type:    BITLK
  cipher:  aes-xts-plain64
  keysize: 256 bits
  key location: dm-crypt
  device:  /dev/sdb
  sector size:  512
  offset:  16 sectors
  size:    15974400 sectors
  skipped: 16 sectors
  mode:    read/write
```

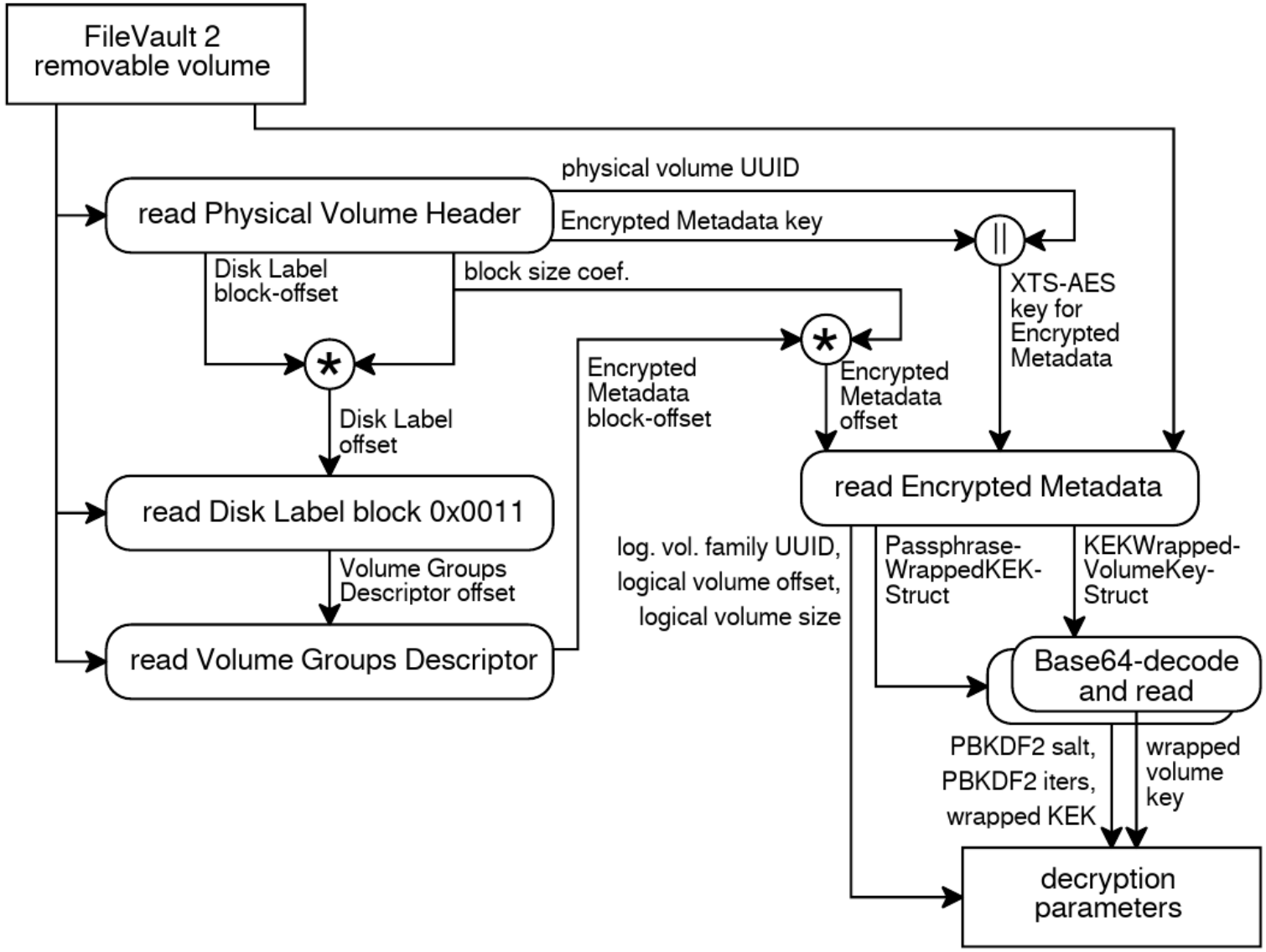
BitLocker – cryptsetup dump

```
# cryptsetup bitlkDump /dev/sdb
Info for BITLK device /dev/sdb.
Version:        2
GUID:           fccc81d1-91b3-4947-85c2-0cb98cd17950
Sector size:    512 [bytes]
Created:        Sat Apr 23 16:24:22 2022
Description:    DESKTOP-71L8959 TEST 23.04.2022
Cipher name:    aes
Cipher mode:    xts-plain64
Cipher key:     256 bits

Keyslots:
 0: VMK
        GUID:           a78c6964-0619-4ac7-a63d-b2a56f5c9e49
        Protection:     VMK protected with passphrase
        Salt:           1cdd33ae1dabe5ccfda16e6c0bad4403
        Key data size:  44 [bytes]
 1: VMK
        GUID:           23a8c064-5de6-46f1-98be-91ebb5c09fd4
        Protection:     VMK protected with recovery passphrase
        Salt:           95d386c7016f62884a13d211321eea7e
        Key data size:  44 [bytes]
 2: FVEK
        Key data size:  44 [bytes]

Metadata segments:
 0: FVE metadata area
        Offset:         34603008 [bytes]
        Size:           65536 [bytes]
 1: FVE metadata area
        Offset:         1108344832 [bytes]
        Size:           65536 [bytes]
 2: FVE metadata area
        Offset:         2182086656 [bytes]
        Size:           65536 [bytes]
 3: Volume header
        Offset:         34668544 [bytes]
        Size:           8192 [bytes]
        Cipher:         aes-xts-plain64
```

FileVault2

- varianta šifrování disku v macOS (OS X)
  - část „core storage“
  - přechází se na APFS (není podpora v Linuxu)
- souborový systém FAT, HFS+
  - HFS lze (bez žurnálu) zapisovat v Linuxu
- AES-128, XTS mód
- PBKDF2 s SHA256
- Experimentální implemenatace pro cryptsetup
  - ve stabilní verzi za ~ 3 měsíce

FileVault2 Metadata



FileVault2 flashdisk – demo

- disky vytvořeny ve virtuálním macOS
- není moc testovacích dat
- (Chce to vůbec někdo? :-)
- core storage je velmi komplikovaný
  - ale stačí jen pár klíčových parametrů
- demo open, dump

FileVault2 – cryptsetup open

```
# cryptsetup open --type fvault2 /dev/sdb2 test
Enter passphrase for /dev/sdb2:
# mount /dev/mapper/test /mnt/tst
...

# cryptsetup status test
/dev/mapper/test is active and is in use.
  type:    FVAULT2
  cipher:  aes-xts-plain64
  keysize: 256 bits
  key location: dm-crypt
  device:  /dev/sdb2
  sector size:  512
  offset:  131072 sectors
  size:    6586368 sectors
  mode:    read/write
```

FileVault2 – cryptsetup dump

```
# cryptsetup fvault2Dump /dev/sdb2
Info for FVAULT2 device /dev/sdb2.
Physical volume UUID    047a90a3d7b94b62974917d0fde502d7
Logical volume offset:  67108864 [bytes]
Logical volume size:    3372220416 [bytes]
Cipher:                 aes
Cipher mode:            xts-plain64
PBKDF2 iterations:      160780
PBKDF2 salt:            50ab6b6aeb18661f7b660ed762fa5fb0
Family UUID:            ca2f817c39ca467f86095ccd5cb377c9
```

Srovnání s LUKS

- Metadata
  - viditelné vs šifrované
  - formát – binární, XML, JSON
  - oblast na začátku/konci disku
  - keysloty
- Algoritmy
  - AES, XTS mód, Adiantum?
  - PBKDF2, Argon2
  - TPM, tokeny, integrace (systemd-cryptenroll)

děkuji za pozornost

Milan Brož
milan.broz@mail.muni.cz

EurOpen 2022
Radešín