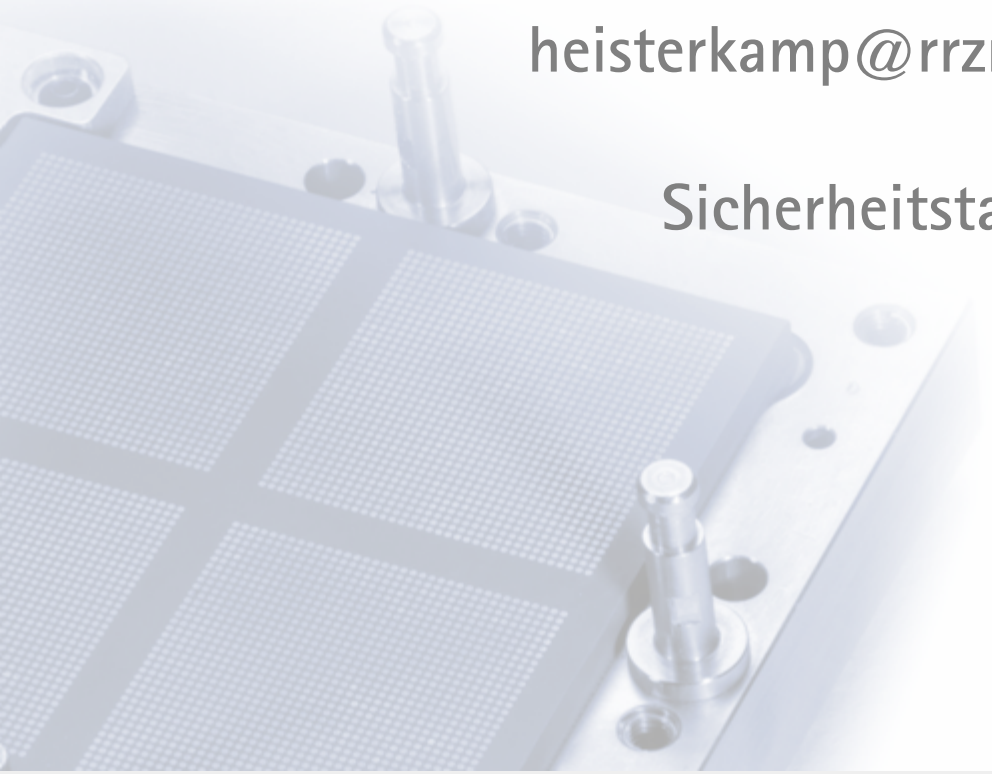
Leibniz Universität Hannover

Full Disk Encryption unter OS X (Mountain) Lion

Mark Heisterkamp
heisterkamp@rrzn.uni-hannover.de

Sicherheitstage WS 2012



Voraussetzungen – zwingend

- mind. OS X Lion (10.7)
- Recovery HD auf dem StartVolume:

peterpan — bash — 80×9

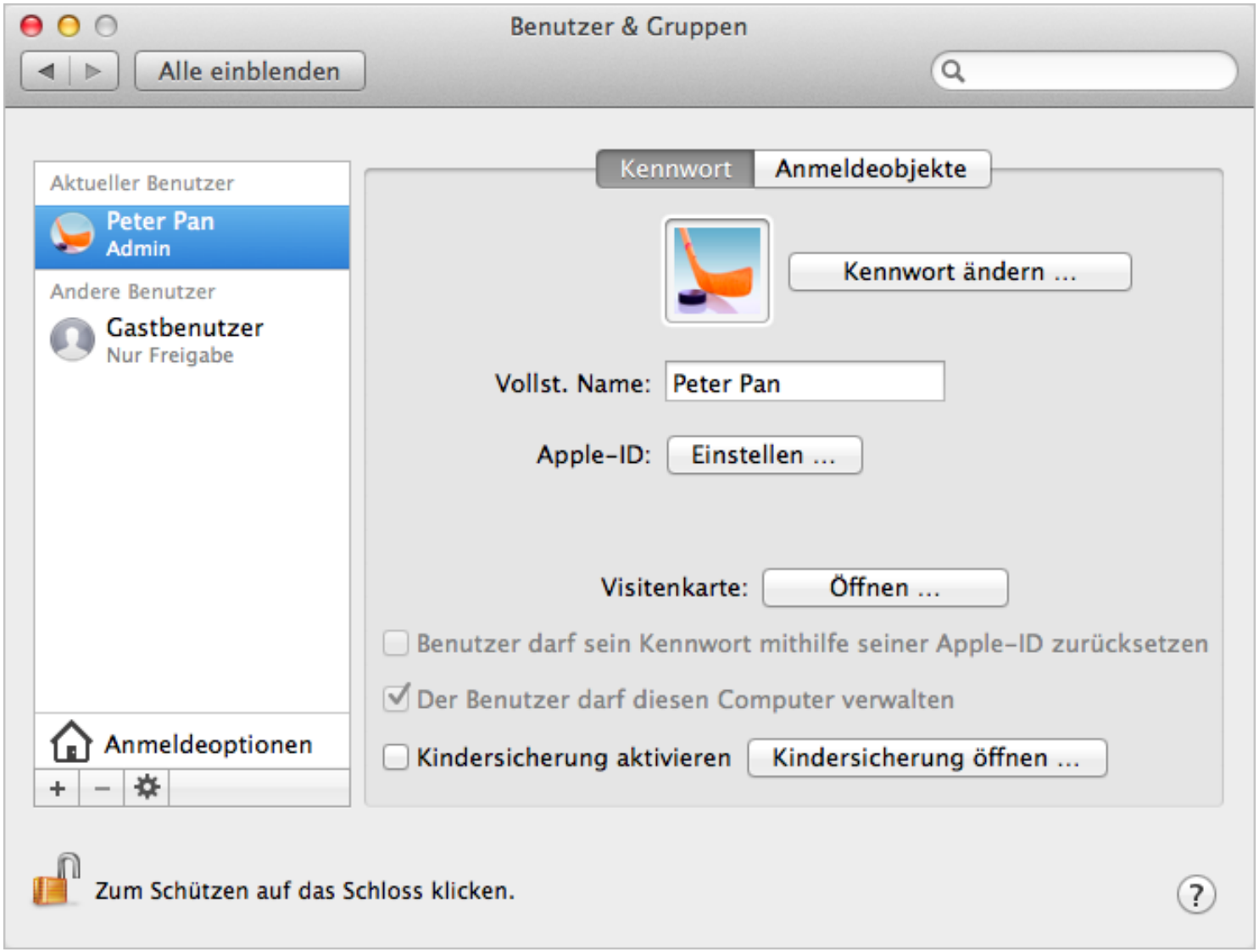
```
ip190:~ peterpan$ diskutil list
/dev/disk0
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *160.0 GB   disk0
   1:                        EFI                         209.7 MB   disk0s1
   2:                  Apple_HFS Ohne Titel              159.2 GB   disk0s2
   3:                Apple_Boot Recovery HD              650.0 MB   disk0s3
ip190:~ peterpan$
```

Voraussetzungen – sollte

- Verschlüsselung wird durch User-Passwort und Wiederherstellungsschlüssel gesichert.
- Mithilfe der Apple-ID kann ggf. das User-Passwort wiederhergestellt werden.
- Nach der Verschlüsselung kann das nicht mehr rückgängig gemacht werden.

→ Vorher abschalten!

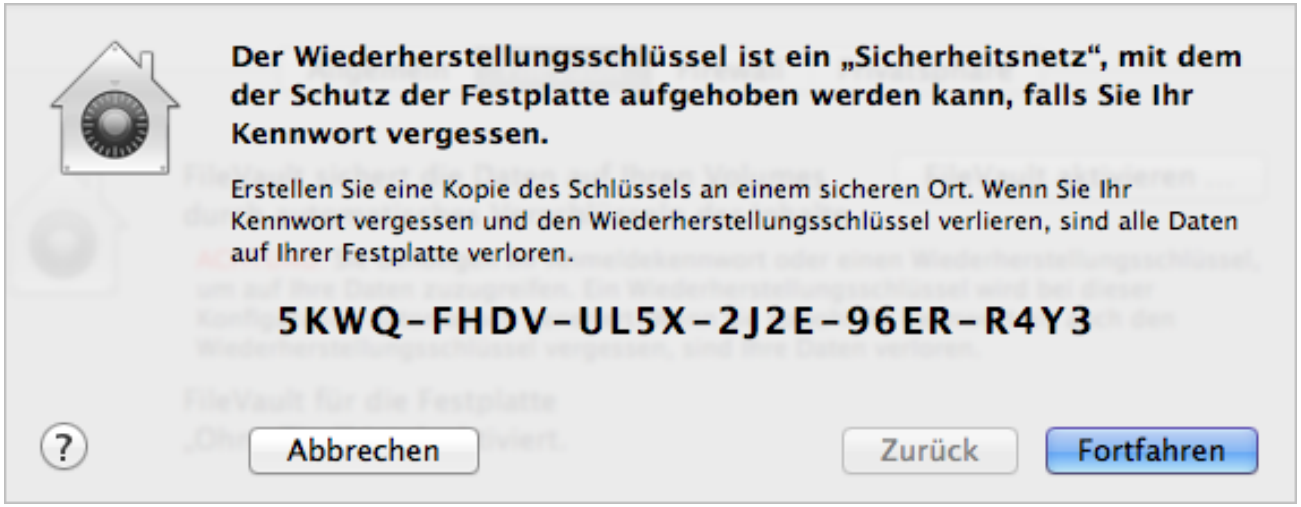
Voraussetzungen – sollte



File Vault aktivieren

Systemeinstellungen ➔ *Sicherheit* ➔ *FileVault*

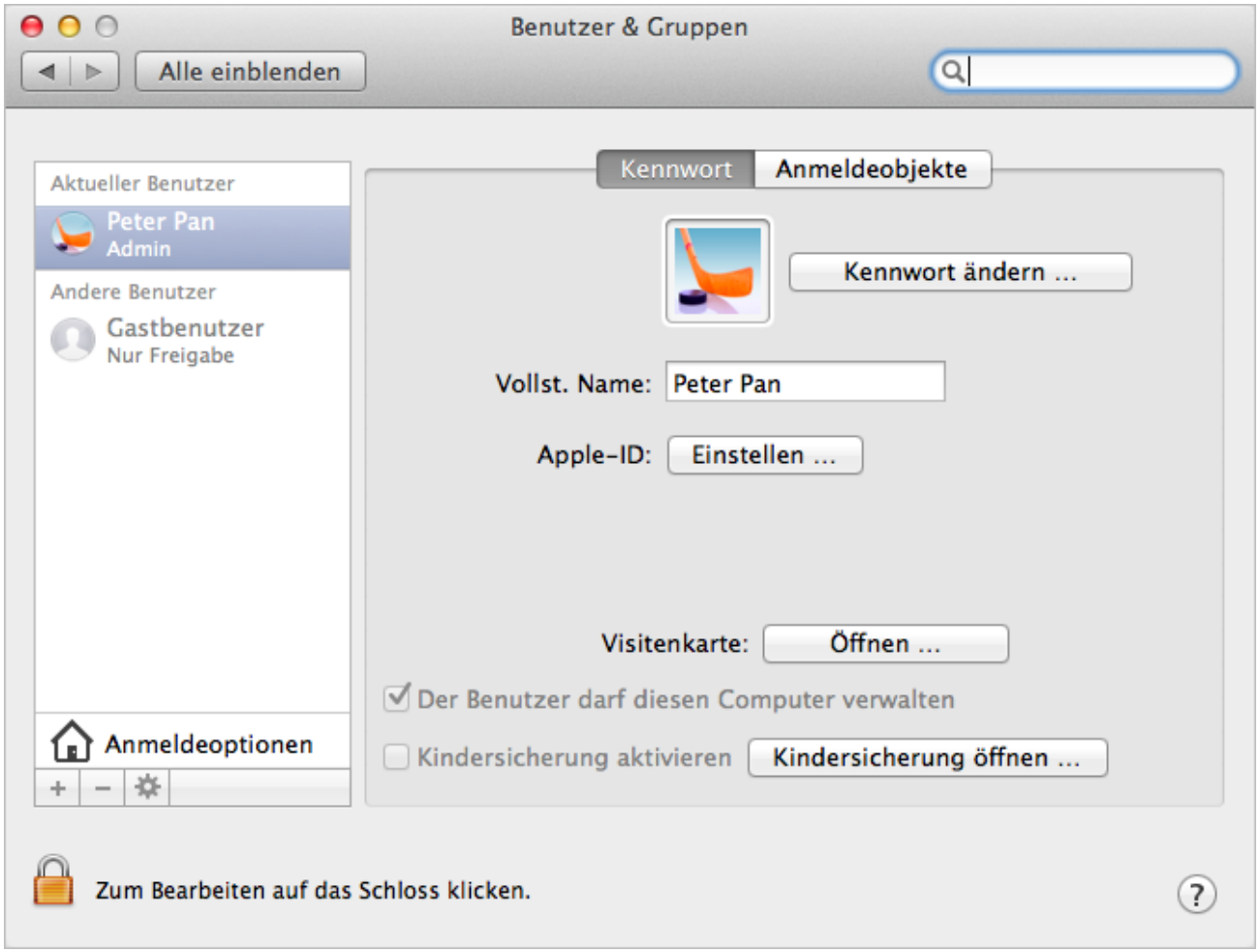
File Vault aktivieren – Wiederherstellungsschlüssel



File Vault aktivieren – Wiederherstellungsschlüssel

File Vault aktivieren – … 2.5 Stunden warten für 11.6 GB …

Die Option, mithilfe der Apple-ID das User-Passwort zurückzusetzen, ist nicht mehr vorhanden. Das heißt aber nicht, dass sie auch deaktiviert ist!



Leibniz Universität Hannover

Performancetest mit Xbench :

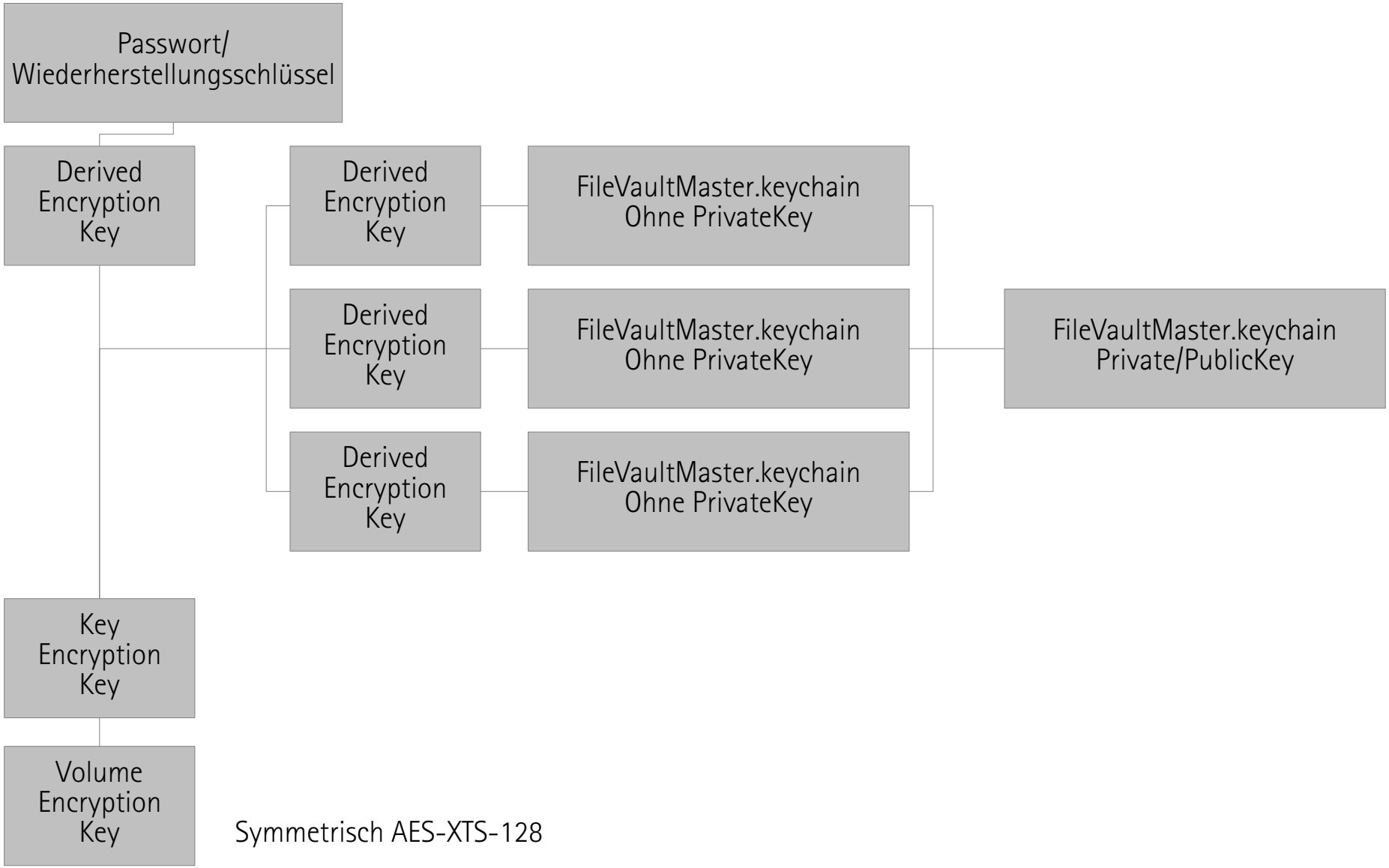
Name	Score	Detail
Results	53.69	
System Info		
Xbench Version		1.3
System Version		10.8.2 (12C60)
Physical RAM		4096 MB
Model		MacBook5,1
Drive Type		FUJITSU MHZ2160BH FFS G1
Disk Test	53.69	
Sequential	71.07	
Uncached Write	112.74	69.22 MB/sec [4K blocks]
Uncached Write	92.14	52.13 MB/sec [256K blocks]
Uncached Read	35.25	10.32 MB/sec [4K blocks]
Uncached Read	122.08	61.35 MB/sec [256K blocks]
Random	43.14	
Uncached Write	16.87	1.79 MB/sec [4K blocks]
Uncached Write	93.97	30.08 MB/sec [256K blocks]
Uncached Read	70.19	0.50 MB/sec [4K blocks]
Uncached Read	116.64	21.64 MB/sec [256K blocks]

Name	Score	Detail
Results	49.02	
System Info		
Xbench Version		1.3
System Version		10.8.2 (12C60)
Physical RAM		4096 MB
Model		MacBook5,1
Drive Type		Ohne Titel
Disk Test	49.02	
Sequential	57.69	
Uncached Write	105.01	64.47 MB/sec [4K blocks]
Uncached Write	71.70	40.57 MB/sec [256K blocks]
Uncached Read	26.52	7.76 MB/sec [4K blocks]
Uncached Read	122.41	61.52 MB/sec [256K blocks]
Random	42.62	
Uncached Write	16.79	1.78 MB/sec [4K blocks]
Uncached Write	99.56	31.87 MB/sec [256K blocks]
Uncached Read	68.19	0.48 MB/sec [4K blocks]
Uncached Read	104.20	19.34 MB/sec [256K blocks]

Verschiedenes

- Neuer Recovery-Key: Decrypt und wieder encrypt
- Alte (Partitions-)Verschlüsselung File Fault unter Snow Leopard kann weiter genutzt werden. File Fault 2 ist dann deaktiviert. Migration durch abschalten der alten und aktivieren der neuen Verschlüsselung.
- Entschlüsselung per Kommandozeile ist möglich.
- Deployment per FileVaultMaster.keychain möglich

Verschiedenes



Links

- Anleitung von Apple:
  http://support.apple.com/kb/HT4790
  Best Practices von Apple:
  http://training.apple.com/pdf/WP_FileVault2.pdf
- Apple-ID-Problematik:
  http://mjtsai.com/blog/2012/08/07/filevault-2s-apple-id-backdoor/
- zur Technik:
  https://dl.dropbox.com/u/46593175/JNUC_2012_fv2_talk.pdf
  http://eprint.iacr.org/2012/374.pdf