![[Pasted image 20220420221804.png]]

解释说明如下

* 可操作功能： 当前界面已经存在操作入口
* 不支持操作功能： 界面存在操作入口，但是会引发其他bug
* 界面缺失功能：界面缺少操作入口
* 问题：该功能点的一些疑问
* 建议：该功能点的一些建议

### 情况1： 分区创建加密磁盘

***crypt1***

* 可操作功能有：
  1. 擦除（创建文件系统），挂载，卸载（存在文件系统情况下） //此时该加密设备等同于普通分区的操作
  2. 与lvm结合后操作为：创建vg,加入vg(vg空间调整) //加入vg之后的操作见情况2
  3. 擦除（加密）：再次加密（是否需要限制对某一个映射盘重复加密？） //技术上可行，可以不做限制，但是前端如何显示之间的映射关系？
* 不支持操作功能为：
  1. 空间调整 (加密后的设备不支持空间调整功能，分区空间调整需要分区表，加密后磁盘应该相当于一个普通分区)
* 界面缺失功能：
  1. 关闭加密磁盘 (没有入口可以主动关闭加密磁盘)
  2. 修改密码or删除密码/密钥 （支持最低8个不同的密码，同时支持修改删除等功能）当没有可用的密钥槽，且仅仅知道口令时，会出现无法永久挂载问题。详细见下方问题永久挂载功能建议。
* 问题：

1. 擦除功能：分区或lvm擦除后，格式化为新的文件系统，同时自动挂载至临时目录下，加密后的映射磁盘擦除后但是是否要自动进行临时挂载？
2. 永久挂载功能：需要keyfile文件，在首次加密磁盘后，自动生成keyfile文件？

* 假设某移动硬盘命令行加密后，用户通过命令行或者文管将加密磁盘解密，打开磁盘管理器，此时可以看到映射的加密磁盘，但是由于不是通过磁盘管理器解密，所以没有keyfile文件或口令。
* 同时，如果未经用户知情情况下，首次加密时自动生成keyfile文件，个人认为不是安全的行为。（代码开源，通过阅读代码逻辑可以非常容易查找到保存keyfile的路径，从而盗取key）
* 建议：
* 用户可以通过两种方式解密，口令（密码）和keyfile。  
  用户卸载后再次挂载时，选择提供口令或keyfile。  
  提供口令时，创建新的keyfile，其中拷贝一份由用户保存至指定位置备份，另一份放入公共路径下限制读写权限，但是会面临用户总是提供口令，不提供keyfile的情况。 解释 最少支持8个不同的密钥槽，但是如果只删除keyfile，不删除密钥槽，可能会出现再也没有密钥槽位置添加keyfile的情况  
  提供keyfile文件时，使用该文件自动挂载，不需要密码输入弹框。所以建议同时提供keyfile文件解密的操作入口。

1. 卸载功能：  
   卸载情况下，是否需要删除保存的keyfile?  
   不删除：公共路径会保存残留的keyfile文件,再次挂载且提供keyfile文件时，会覆盖公共路径下的keyfile文件,文件命名规则:映射名\_uuid  
   删除 : 用户再次挂载时，选择提供口令或keyfile,提供口令时，再次创建新的keyfile，提供keyfile文件时，使用该文件自动挂载

### 情况2：分区创建加密磁盘后，加密磁盘创建vg或加入vg

***crypt2创建为vg后，crypt2可操作功能有：***

* 可操作功能有：

1. 与lvm结合后操作为：pv删除 (此时仅作为vg中的一个pv设备，不可做其他操作)  
   其中有一点需要特殊说明,假设某一个磁盘加密后，创建vg,vg创建lv，lv创建加密，加密加入vg,这个情况是允许的。自己再跟自己套娃。

root@liuwh-PC:/home/liuwh/Desktop# lsblk -fa  
NAME FSTYPE LABEL UUID FSAVAIL FSUSE% MOUNTPOINT  
loop0  
loop1 crypto\_LUKS a48765b6-53c3-43c5-ba07-8cd3860a2038  
└─test2 LVM2\_member yyOeHB-H8dB-zPLL-5d0i-Wwhm-OkOn-1OFaTQ  
└─vg01-lvol0 crypto\_LUKS b5e5d985-2a62-4eff-aba9-dcfba606148f  
└─test3 LVM2\_member OkfQ8K-vi4s-Z5oB-kINp-fWIo-31qB-drOqWm  
root@liuwh-PC:/home/liuwh/Desktop# pvs  
PV VG Fmt Attr PSize PFree  
/dev/mapper/test2 vg01 lvm2 a-- 1004.00m 0  
/dev/mapper/test3 vg01 lvm2 a-- 984.00m 984.00m  
root@liuwh-PC:/home/liuwh/Desktop# vgs  
VG #PV #LV #SN Attr VSize VFree  
vg01 2 1 0 wz--n- 1.94g 984.00m  
root@liuwh-PC:/home/liuwh/Desktop# lvs  
LV VG Attr LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert  
lvol0 vg01 -wi-ao---- 1004.00m  
root@liuwh-PC:/home/liuwh/Desktop#

这种情况就非常诡异了，因为按照正常逻辑删除lv,然后删除vg，再删除pv。  
现在因为lv上创建加密，加密后的lv又创建为pv加入了自己的vg中。。。。所以此时正确的删除方式应该是vgreduce 加密磁盘test3，关闭test3,关闭test2,删除lv,删除vg。

* 不支持操作功能为：
  1. 空间调整
  2. 擦除，挂载，卸载
  3. 创建vg,加入vg(vg空间调整)
  4. 加密操作：再次加密 (作为vg中的pv设备，再次加密将导致vg丢失物理卷)
* 界面缺失功能：
  1. 同crypt1
* 问题：

假设设备sda1为加密磁盘，sda2为普通分区，使用sda1,sda2创建vg,其中加密磁盘的未打开，此时该vg会处于丢失物理卷的状态，vg将无法使用  
对于加入vg的磁盘是否提供关闭加密磁盘的功能？如果关闭加密磁盘，同样相当于物理卷丢失。

* 建议：  
  对于加密磁盘加入vg的情况应该显示说明或提醒用户，不可随意关闭磁盘

### 情况3：分区创建vg，vg创建加密磁盘

***crypt3***

* 可操作功能有：
  1. 同crypt1
* 不支持操作功能为：
  1. 同crypt1
* 界面缺失功能：
  1. 同crypt1

### 情况4: 加密的普通分区或lv：

* 可操作功能有：
  1. 擦除（加密）：遗失密码或首次加密情况 需要提供口令或密钥文件（用户首次加密也可使用密钥文件） 将擦除之前的加密格式，数据无法找回。
  2. 挂载（未解密情况下）：提供密钥或口令解密，需要提供映射名称
* 不支持操作功能为：
  1. 空间调整 (加密后的设备不支持空间调整功能，分区空间调整需要分区表，加密后磁盘应该相当于一个普通分区)
  2. 加入vg
  3. 创建vg
  4. 卸载
* 界面缺失功能：
  1. 同crypt1