Atitit 信息设备加密机制 手机 电脑 tpm bitlock EFS加密

目录

[1.1. 智能文件系统（EFS） 1](#_Toc31053)

[1.2. BitLocker驱动器加密 2](#_Toc32285)

[1.2.1. BitLocker与加密文件系统（EFS） 2](#_Toc6183)

文件加密。。其他用户无法访问文件。。把硬盘挂载到其他系统任然无法打开文件。。防止强行修改用户密码，如果强行修改则，密钥失效，无法打开原加密文件。。

## **智能**文件系统（**EFS**）

EFS加密是windows系统自带的加密方式，一个系统用户对文件加密后，只有以该用户的身份登陆才能读取该文件。EFS加密的文件和文件夹名字颜色是绿色，或者在该文件或文件夹的高级属性是加密属性。这样做在很大程度尚提高了数据的安全性，但是如果秘钥文件丢失或者重装系统就会导致加过密的文件不能打开，今天的教程主要介绍的就是如果电脑使用ESF加密后却因为其他原因导致无法打开文件，我们应该怎么解密。

简单对上述这一加密过程进行归纳就形成了“用户密码－>主密钥－>私钥－>FEK－>EFS加密文件”的加密链。如果想要对EFS进行解密，我们需要得到的信息包括用户密码、主密钥、私钥。

4.被EFS加密过的数据是不是就绝对安全了呢？  
当然不是，安全永远都是相对的。以被EFS加密过的文件为例，如果没有合适的密钥，虽然无法打开加密文件，不过仍然可以删除（有些小人确实会这样想：你竟然敢加密了不让我看！那好，我就删除了它，咱们都别看）。

## BitLocker驱动器加密

BitLocker驱动器加密和加密文件系统之间存在一些差异。BitLocker旨在帮助保护安装Windows的驱动器上的所有个人和系统文件，如果您的计算机被盗，或者未经授权的用户尝试访问计算机。EFS用于帮助保护每个用户的任何驱动器上的单个文件。下表显示了BitLocker驱动器加密和EFS之间的主要区别。

### BitLocker与加密文件系统（EFS）