Aittt info const sftwr and hdwr信息化建设软硬件

目录

[1.1. 硬件类的 1](#_Toc28683)

[1.2. 通用服务类的ms google ifttt wordpress github vpn采购 1](#_Toc23720)

[1.3. 专用app建设自己 日志类财务类oa系统等 1](#_Toc3433)

[2. Other 1](#_Toc5834)

[2.1. Efs加密 1](#_Toc26986)

## 硬件类的

手机 tablet 笔记本（带tpm安全芯片的海外laptop）

安全sim卡。。

u盘 ，key密钥蓝牙

## 通用服务类的ms google ifttt wordpress github vpn采购

文档 文章，图片，音视频， 代码

## 专用app建设自己 日志类财务类oa系统等

启动u盘。。

密码管理系统，xls即可

密钥管理系统 xls与加密文件夹

Efs文件加密 Encrypting File System，**加密文件**系统

# Other

## Efs加密

**密钥的备份和恢复**

说到加密，[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)是一个非常重要的概念。EFS是一种公钥加密，那么这里就要说说什么是公钥加密了。在使用EFS加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的FEK (File Encryption Key，[文件加密](https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%8A%A0%E5%AF%86" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)钥匙)，然后利用FEK和数据扩展标准X算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。随后系统利用你的[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)加密FEK，并把加密后的FEK存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密FEK，然后利用FEK解密出文件。在首次使用EFS时，如果用户还没有[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)/私钥对（统称为密钥），则会首先生成密钥，然后加密数据。

文件的加密和解密都需要[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)的参与，而密钥分为公钥和[私钥](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)两种。很明显，无论是加密还是解密文件，都需要用到个人[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)。加密文件的时候使用[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)，解密文件的时候则使用相对应的[私钥](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)。那么无论是丢失了公钥还是[私钥](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)，都会给我们的使用带来麻烦，尤其是私钥，丢失之后就再也无法解密文件了。

为了保证数据安全，最好能在加密文件之后立即将自己的[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)备份出来，并保存到安全的地方，以防系统崩溃或其他原因导致数据无法解密。方法是，运行“certmgr.msc”打开证书管理器，在“当前用户/个人/证书”路径下，应该可以看见一个以你的用户名为名称的证书（如果你还没有加密任何数据，这里是不会有证书的）。用鼠标右键点击这个证书，在“所有任务”中点击“导出”。之后会弹出一个证书导出向导，在向导中有一步会询问你是否导出[私钥](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)，在这里要选择“导出私钥”，其它选项按照默认设置，连续点击继续，最后输入该用户的密码和想要保存的路径并确认，导出工作就完成了。导出的证书将是一个[pfx](https://baike.baidu.com/item/pfx" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)为后缀的文件。这个[pfx](https://baike.baidu.com/item/pfx" \t "https://baike.baidu.com/item/EFS%E5%8A%A0%E5%AF%86/_blank)文件最好能保存到其他位置，并且要保证该文件的安全。