

# 专业实践总结和教学案例

信息技术学院 谢峰

暑假，学校为了提高教师的实践能力，加强教师的队伍建设，根据学校下达的文件精神，暑假期间老师都要深入到企业进行实践锻炼，在这段企业实践时间里，其间感悟颇多，受益匪浅，现将这一段工作时间来的所见所闻，所思所想作一次总结。

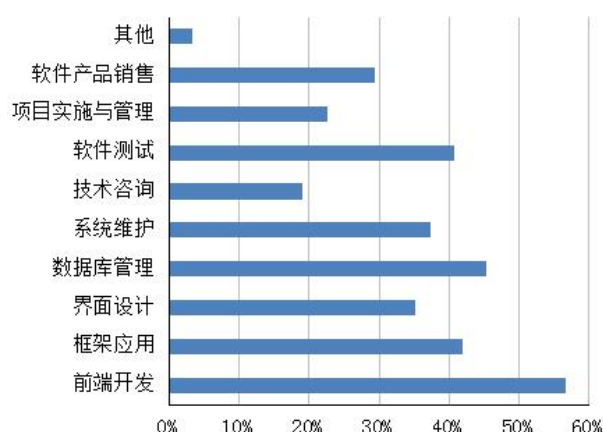
作为一名专业教师下企业锻炼是提升教师综合素质的重要举措，是以市场为导向，研究人才培养模式、专业课程建设、课程开发与建设等工作的重要内容。教师通过下企业锻炼，了解企业生产、经营全过程，提高动手能力，为专业设置、构建与高职培养目标、国家职业等级标准相适应的课程体系作好市场调研。通过专业实践，收获如下：

实践企业单位情况：

广州星戈琅信息科技有限公司情况：信息系统集成服务；信息技术咨询服务；商品信息咨询服务；计算机及通讯设备租赁；体育用品及器材批发；体育用品及器材零售；电子产品批发；电子产品零售；通信设备零售；计算机零配件批发；网络技术的研究、开发；计算机技术开发、技术服务；电子、通信与自动控制技术研究、开发；办公设备批发；商品批发贸易（许可审批类商品除外）；商品零售贸易（许可审批类商品除外）；办公设备租赁服务；办公设备耗材批发；办公设备耗材零售；数字动漫制作；游戏软件设计制作(依法须经批准的项目，经相关部门批准后方可开展经营活动)

## 1、 计算机应用对行业发展产生重要的影响

“互联网+”相关政策的支持，带动其他行业升级转型。计算机复合型人才需求旺盛，通过在企业工作中了解到企业对计算机人才的需求（如图所示），同学校的专业论证基本一致，在今后的人才培养方案设置中增加应用能力的培养和团队协作能力的锻炼。



## 2、 通过专业实践，对今后的教学工作促进作用。

通过专业实践，参与企业实际项目中去，实现了从理论到实践、再反馈到教学活动中，收到了明显的效果。对今后的教学工作有着非常有益的指导和促进作用。

## 3、 在企业实践中收获工作的成就感

到公司参加专业实践，除了完成公司的项目外，在日常工作中同公司同事友好相处，通过自己的计算机专业知识给公司提供相关技术支持。通过社会实践，也认识到不同企业管理人员，在暑假完成本专业社会公益培训 390 人次的任务。

## 对本专业（课程）建设方面的启发

### 1、 加快培养高素质的计算机应用技术师资

目前掌握目前专业智能硬件技能的教师队伍仍然不足，没有足够

的师资队伍显然不能满足专业教学。因此，在以后的专业建设方面，应该结合当前科学技术的发展，注重培养掌握现代信息技术、互联网技术的软硬件结合的复合型师资队伍。

将专业技术的发展趋势以及应用知识、专业技能传递给学生，不仅能使学生的专业知识技能在横向宽度和纵向深度上得到全面发展，而且能使学生同时学到专业知识以外的许多东西，如项目管理、市场运作等。

## **2、加强实训基地和课程建设**

培养高技能创新型人才，必须有完善的实践训练场所。结合校内创客空间等工作室，主动探索人才培养模式改革、课程体系创新等内容，逐步培养符合现代产业需求的高技能人才。

## **3、提高沟通和协调能力**

做项目过程中，从开始洽谈到最后实施每个步骤需要详细的落实，这个过程在课程的项目模拟里可以导入。在项目过程中学生的执行力是不能靠课堂教师传授的，必须鼓励学生多走出校园，否则难以与真实项目对接。

## **4、不断加强学习，自我完善。**

在教学过程中，我们必须不断加强新技术、新知识的学习，养成终身学习的习惯，不断提高自己的理论和实际操作能力。社会的迅速变迁使身边的事物每时每刻都在发生着日新月异的变化，有许许多多的问题要我们来回答，我们不可能样样精通，但至少应该去努力了解一些。教师不仅是教育者而且更应该是受教育者，要处处丰富自己的

知识，时时为自己“充充电”，要有一种永不衰竭的求知欲望，不断超越自己，努力提高自身的人格魅力。

加强课前准备。作为一名教师，要利用好课堂的教学时间，不认真准备，肯定是上不好课的。我觉得备课也不仅仅是把一次要讲的内容准备出来，而是要把一学期要讲的知识全部装在心中，你对每节课要讲些什么才心中有数。什么内容为以后的教学打下基础，哪些内容需要重点强调，能做到这些我们是需要下一番功夫的。

总之，这次下企业实践锻炼，虽然时间不长，但是提升了我的教育教学理念，丰富教育教学方法的一个大好机会，从中我不但开阔了眼界，同时也提高了自己的专业能力，锻炼了实践能力，对我的本职工作和专业建设有了更深、更新的认识，通过这次的下企业锻炼，我也会努力将“双证”改为“双能”，将自己培养成为一个既有理论教学能力，又有实践教学能力，成为真正符合职业教育需求的“双师”素质教师，为学校冲击国家优质高职院校 50 强贡献自己的力量。

## 项目文档教学案例

# 1. 内部网络电子文档安全解决方案

## 1.1. 透明加解密保护内网电子文档安全

通过对企业内网 PC 安装铁卷客户端，实现所有员工的 PC 机上的受控文件全部加密，未安装铁卷客户端的用户无法查看加密文件内容，保证未认证用户看不到，看到拿不走，从源头上保证了企业的电子文档安全。

铁卷采用的原理是内核文件实时透明加解密，在操作系统底层对文件进行加解密操作，不影响用户的原有使用习惯。安装铁卷的用户在使用文件时，用户终端自动将文件实时加解密；文件的接收者必须经过管理中心端的认证，才能够根据许可权限对文件进行操作。

所有的文档在用户创建、修改、保存时自动加密，完全无需用户手动操作。这种自动强制加密的方式优势在于：

- **强化安全性：**用户无法自己产生明文文档，更加有效地保障机密文件不会外泄；
- **提升效率：**用户可以更加高效快速地使用各类软件进行操作，而无需进行加解密工作，减少了隐性的时间成本浪费；
- **增强易用性：**用户无需经过复杂的操作培训就能掌握软件使用方法；
- **不用担心主动泄密：**不管是通过外设拷贝还是病毒传输抑或是设备遗失，都不会导致泄密事件的发生；
- **为创建、存储、使用和传输过程中的电子文档提供全方位防护：**铁卷电子文档安全系统提供电子文档全生命周期全方位防护。为了促进理解，我们将几种常见的加密技术进行了比较，如下图所示：

	文件创建	网络传输时	第一次使用	文件打开
传输链路加密		Yes		
文件加密→解密		Yes	Yes	
手动格式转换		Yes	Yes	Yes
透明加解密 (铁卷，全程保护)	Yes	Yes	Yes	Yes

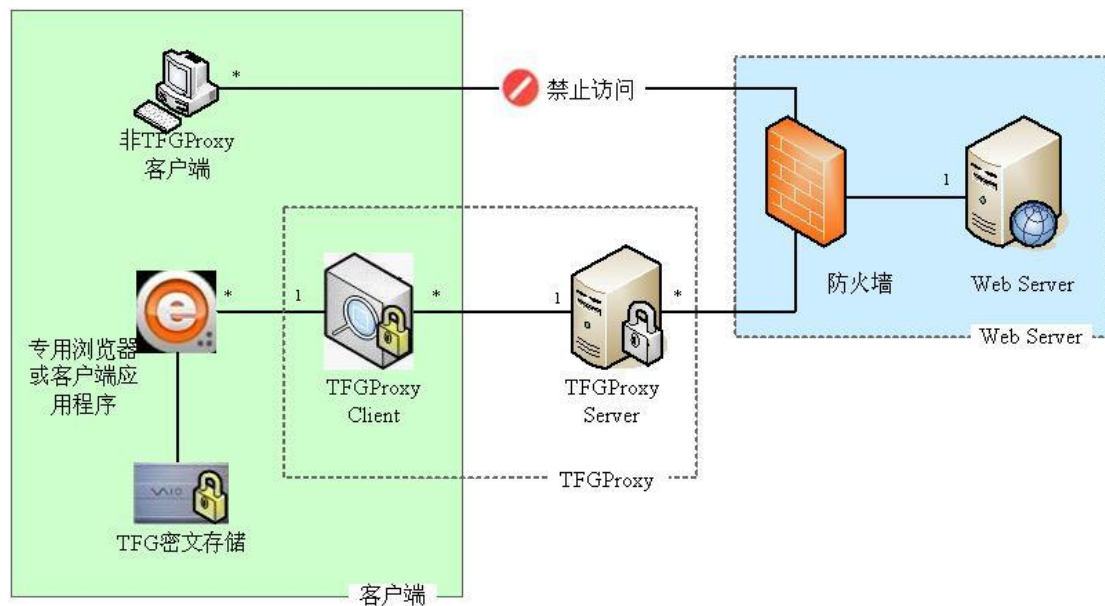
## 1.2. 铁卷保护企业业务系统数据安全

在本解决方案中我们采用了安全代理（TFGProxy）等技术来达到与企业现有业务系统的整合，不需要业务系统做任何更改即可对数据进行保护。

### 1.2.1. 基于安全代理（TFGProxy）的技术保护业务数据

大多数企业目前有 ERP、OA 系统、PLM 系统等，在部署了铁卷电子文档安全系统后，这里业务系统里的数据可能会以两种形式存在，即明文和密文。比如 PLM 系统是基于 B/S 结构的，服务器上数据为明文，那么任何人用 IE 去访问，都可能会存在泄密风险，即使做了 IE 进程保护。

为了解决以上问题，我们引入了安全代理（TFGProxy）解决方案。其工作原理图如下：



该方案能做到以下几点：

- 未安装铁卷客户端的机器或非专用浏览器上都无法正常访问 Web Server，会被 Web Server 的防火墙阻挡；
- 在装有铁卷客户端的机器上通过专用浏览器能正常访问 Web Server，而且这个专用浏览器只能访问 Web Server，下载回来的数据，强制保存为密文；
- TFGProxy Client 与 TFGProxy Server 之间的通讯可采用加密传输，防止传输过程中泄密。

## 1.3. 多种防护手段保证无法泄密

为了达到全面防止用户泄密的目的，铁卷从设计之初就坚持一个原理：重要文件全部加密存放，在操作系统驱动层对数据进行加解密操作，并且对截屏、打印、拷贝等行为进行防范与监控。

### 1.3.1. 截屏保护

在需求调查过程中，用户多次提到截屏的问题，一份重要文件打开，轻轻按一下截屏键就有可能泄露出去，如何防范截屏也成了企业的一块心病。

如何有效防范截屏，如果应用了铁卷，你的担心就是多余的。铁卷有很强大的防截屏功能，不但能禁止截屏键截屏，还能禁止其他软件截屏。

### 1.3.2. 文档打印控制及水印

为了防止通过打印的方式泄露机密，铁卷设计了文档打印控制和水印功能，这些功能模块可以很好的做到如下几点：

- 系统支持对客户端的打印控制，分三种权限：允许打印、禁止打印和限制打印；
- 在打印的过程中加上浮水印，该水印详细的记录了用户在何时打印了什么内容的文档；
- 打印后的文档流传到企业以外仍然有威慑力；

## 1. 电子文档保护产品综述

随着 Internet 日益普及，越来越多的文件以电子文档的形式传输。众所周知，电子文档极易复制且复制后不留任何痕迹。通常电子文档的传输造成的信息泄露有以下几种形式：

- 内部员工因为离职等原因，把秘密文件拷贝到软盘带走，或通过网络向外传递：



时间	终端	类型	备注
2007-09-04 13:30:45	192.168.1.5(test4)	删除文件	删除文件 C:\WINDOWS\system32\cmd.exe
2007-09-04 13:30:17	192.168.1.5(test4)	水印	07470904051430009e001b57630070cc
2007-09-04 13:30:17	192.168.1.5(test4)	打印	Microsoft Word - 铁卷电子文档安全系统技术白皮书.DOC
2007-09-04 13:28:51	192.168.1.7(gysky)	重命名文件	重命名文件 C:\Documents and Settings\kysky\桌面\铁卷#
2007-09-04 13:28:41	192.168.1.7(gysky)	重命名文件	重命名文件 C:\Documents and Settings\kysky\桌面\铁卷#
2007-09-04 13:27:20	192.168.1.7(gysky)	移动文件	移动文件 C:\Documents and Settings\kysky\桌面\1410155
2007-09-04 13:27:08	192.168.1.5(test4)	移动文件	移动文件 C:\Documents and Settings\kysky\桌面\1410155
2007-09-04 13:27:05	192.168.1.5(test4)	删除文件	删除文件 C:\Documents and Settings\kysky\桌面\1410155
2007-09-04 13:27:05	192.168.1.5(test4)	删除文件	删除文件 C:\Documents and Settings\kysky\桌面\2006062
2007-09-04 13:27:00	192.168.1.5(test4)	复制文件	复制文件 C:\Documents and Settings\kysky\桌面\2006062
2007-09-04 13:26:59	192.168.1.5(test4)	复制文件	复制文件 C:\Documents and Settings\kysky\桌面\1410155
2007-09-04 13:26:55	192.168.1.5(test4)	复制文件	复制文件 C:\Documents and Settings\kysky\桌面\1410155
2007-09-04 13:26:52	192.168.1.5(test4)	复制文件	复制文件 C:\Documents and Settings\kysky\桌面\1410155

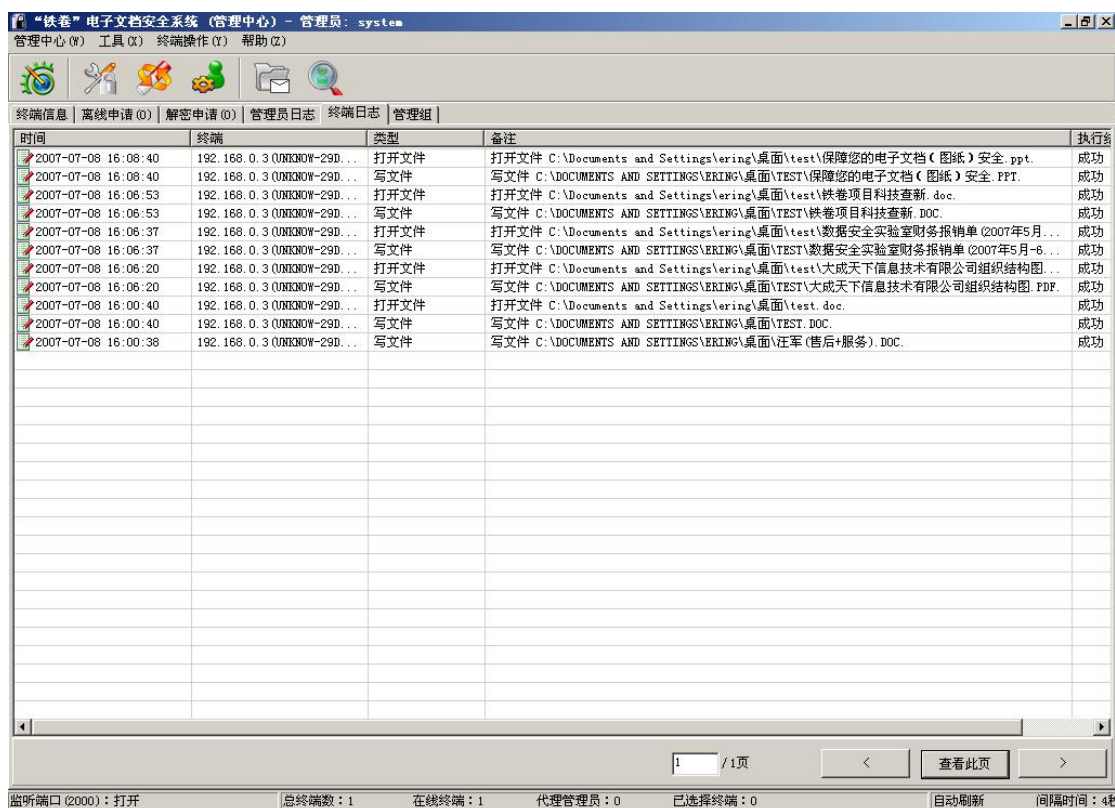
谁在什么时候在那台计算机上打印了什么文件

### 1.3.3.电子文档使用审计日志

铁卷完全符合萨班斯法案（SOX）的要求，其日志审计功能包括：

- 管理员日志
  - 各种管理操作如批准离线、解密等
  - 日志操作
- 客户端日志
  - 文件打开、编辑、拷贝等操作
  - 文件打印
- 日志搜索

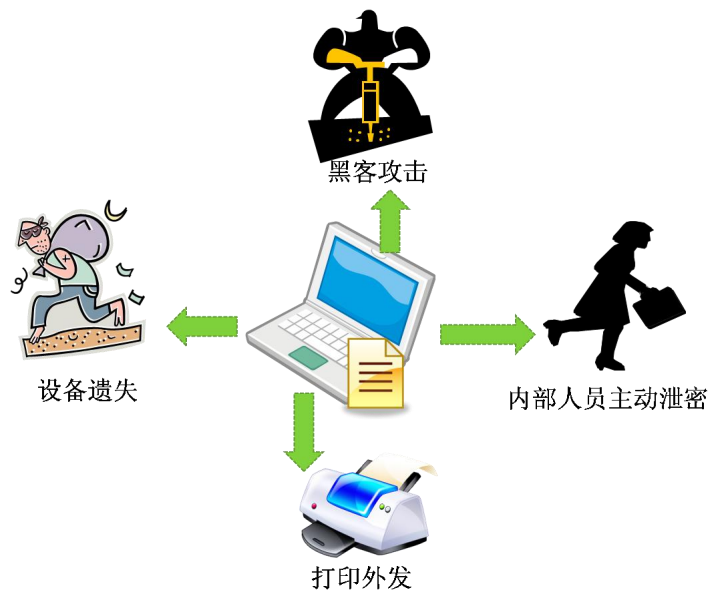




## 2. 移动办公解决方案

## 2.1. 现有的风险

目前移动 PC、笔记本、上网本、PDA 等移动办公设备在企业应用广泛。方便了工作，但也成倍增加了电子文档泄密的风险，总结起来有以下几种：



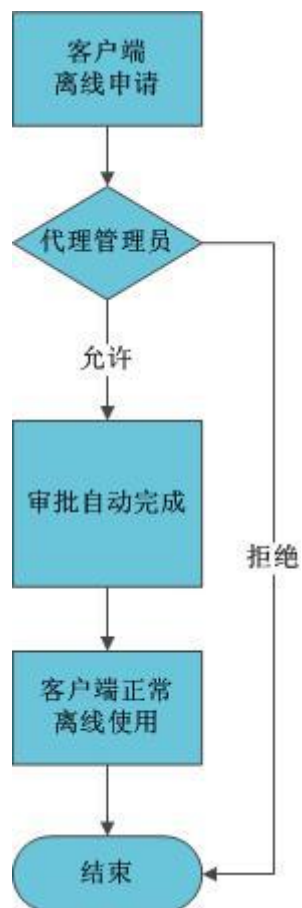
- 笔记本使用者主动泄密
- 笔记本遗失，导致存储在笔记本内的重要电子文档泄密
- 通过在外部打印机打印重要电子文档泄密
- 笔记本离开内部网络安全防护，导致笔记本遭攻击后电子文档泄密

## 2.2. 解决方案

因此，为解决移动办公产生电子文档泄密的风险，并且使笔记本用户能够在离开公司网络时正常使用笔记本上的加密文件，铁卷电子文档安全系统给出如下解决方案。

### 2.2.1. 提前离线申请

如果需要离开公司网络，事先提出离线申请，申请时需要填写离线的原因和预计离线期限，系统会自动通知相关的审批责任人，并且自动记录整个审批流程。离线申请流程如下图所示：



- 当笔记本用户回到公司网络后，铁卷客户端会将离线过程中使用加密文件的日志都上传到公司铁卷日志审计服务器上;
- 当用户在外出差使用笔记本需要临时延长离线时间时，铁卷系统管理员可以通过发送软证书的方式延长笔记本离线使用的时间;
- 适合普通员工出差使用，可按需要增加“自行解密”权限，控制打印权限。

### 2.2.2.USB KEY 授权

在笔记本上安装铁卷客户端，配备 Usb-Key 使用，其中 Usb-Key 有使用时间限制（可设置）。在接入公司网络时不需要使用 Usb-Key，当离开公司网络后插入 Usb-key 并输入认证密码即可正常使用笔记本上的加密文件。和“离线申请”方式相比，有如下优点：

- 不用代理管理员审批，省去离线申请步骤;
- 密码认证，多重保护;

- 安全性高，方便，因此适合使用笔记本进行移动办公的公司高管。

### 3. 合作伙伴解决方案

大多数企业已经拥有众多供应商、分销商等第三方合作伙伴，企业内部与这些合作伙伴之间的文档流转非常频繁。如何保证这些电子文档能提高双方办事的效率，而又不致被传递到第三方，是急待解决的问题。

因此，针对合作伙伴处的电子文档防泄密，我们推荐两套方案配合使用，具体如下描述：

- “外部合作伙伴”终端

适用于企业以外的第三方合作伙伴。创建客户端时选择该类型，则该客户端可在用户需要透明解密文档时手动执行，在此期间只能处理加密文档，无法打开明文文档，新建文档会被加密。处理完后可手动关闭客户端，将不会影响合作伙伴的其他工作，可正常处理明文文档，新建文档也不会被加密。

- 转换文档格式外发

适用于所有静态文档、图纸的外发。安装转换文档格式外发组件，将在终端产生虚拟打印机，加密文档可直接被打印为包含多种安全策略（密码、阅读次数、时间限制、硬件绑定等）的特殊格式，打印日志同时上传至服务器备查。只有在满足安全设定的条件下，才可阅读，且阅读期间无法复制或另存文档内容。

**A 方案最适宜长期合作伙伴且密级不是很高的文档传递；**

**B 方案适合临时客户或密级高的文档传递。**

### 4. 文档外发解决方案

企业内部部分加密的电子文档通过前期的铁卷电子文档防泄密系统已经达到了一定程度的保密效果，但出于各种因素的考虑，可能会对部分机密信息授权开放。

针对此类需求，我们提供如下解决方案。

## 4.1. 外发管理解决方案

- 解密审批

和笔记本离开网络环境使用一样，用户必须提出解密申请，发出申请后，申请内容会被自动转发到指定的解密责任人处，由指定的解密责任人进行审批。如下图所示：

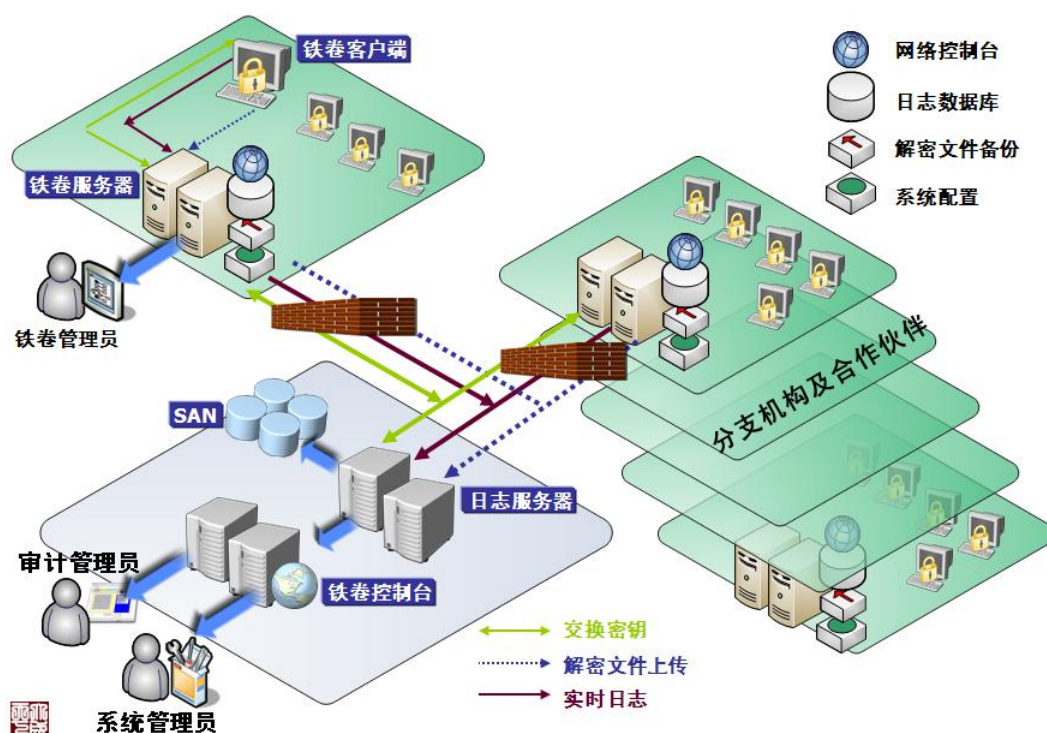


经过授权解密责任人的审批后，用户端的加密文档立即被解密。

当用户提出解密申请时，需要填写接收人信息，提供需要解密的文件等信息。如下图所示：

为防止在一个解密责任区域内，解密责任人不在的情况。我们建议设置多个授权解密责任人。

## 5. 部署实例



**铁卷服务器:** 监控所有客户端状态, 按需要执行远程升级、卸载操作; 查看并修改客户端配置; 提供身份认证服务, 备份客户端解密的文件等。

**铁卷客户端:** 透明加解密, 无需人工干预即可实现文件加解密, 如有必要可向部门代理管理员提出文件解密申请, 笔记本用户需要外出办公也可向代理管理员提出离线申请; 记录客户操作日志上传到日志服务器。

**日志服务器:** 接收铁卷客户端和服务器的操作日志。

**铁卷控制台:** 可向日志审计管理员提供详尽的日志, 并可生成详细的报表。

**分支机构:** 可通过 VPN 等通道直接接入公司内网与铁卷服务器连通, 也可单独配置服务器实现电子文档安全防护。

**合作伙伴:** 通过安装合作伙伴客户端达到交换数据的目的。