凤 凰 卫 士

Phoenix Warrior

上海网腾信息科技有限公司

Tel: +86 21 61504333

WEB:www.wonderonline.cn

Email: support@wonderonline.cn

ADD: Room 712 ,Building3, Nano Technology Park,

No. 245, Road Jiachuan,XuHui,Shanghai, 200237,P.R.China

2010/7/1

目录

功能介绍

透明加密

基于 PKI 体系，透明的、强制的、自动的加密涉密文档。使这些文件，在特定的环境下可以使用。如公司内部（私自带离公司无法打开），部门内部（私自拿到其他部门或公司外部无法打开）。同时可以设定这些文档的权限，规定哪些人可以查阅、哪些人可以打印、哪些人可以修改、哪些人又只能使用到什么时间。

设备控制

对一些可能产生泄密的设备进行控制，如打印机和移动存储设备（U 盘、MP3、手机等）。对于打印机，可以设定某人某组是否可以打印涉密文档。对于移动存储设备，则可以根据实际要求，设置出强大的使用规则。

如下图所示

对于入和出（相对电脑而言）可以分别进行控制，组合后可以实现 9 种使用规则。实现如只读、禁用、拷入加密、拷出加密、只出不入等诸多功能。

自动备份

为防止文件意外损坏或者恶意删除，凤凰卫士提供了自动备份的功能。对于一些涉密的文件，当其打开时，即检查备份库中是否存在此文件，如不存在或者文件较旧，则自动备份之。并且可以根据此备份文件，形成一条版本库，查询到每次更改的内容。

日志监控

对于一些可能导致泄密的操作进行监控，如打印、拷 U 盘、解密文件等操作日志传送至服务器，以备后期追查。

工作原理

PKI 体系介绍

PKI（Public Key Infrastructure ）基于公开密钥理论和技术建立起来的安全体系。是提供信息安全服务的具有普适性的安全基础设施。该体系在统一的安全认证标准和规范基础上提供在线身份认证，是 CA 认证、数字证书、数字签名以及相关安全应用组件模块的集合。作为一种技术体系，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决身份认证、信息完整性和抗抵赖等安全问题，为应用提供可靠的安全保障。

PKI 体系此前更多的是应用于网络，凤凰卫士根据其原理思路，将其应用于文件透明加密领域。用来处理身份识别、权限分割。

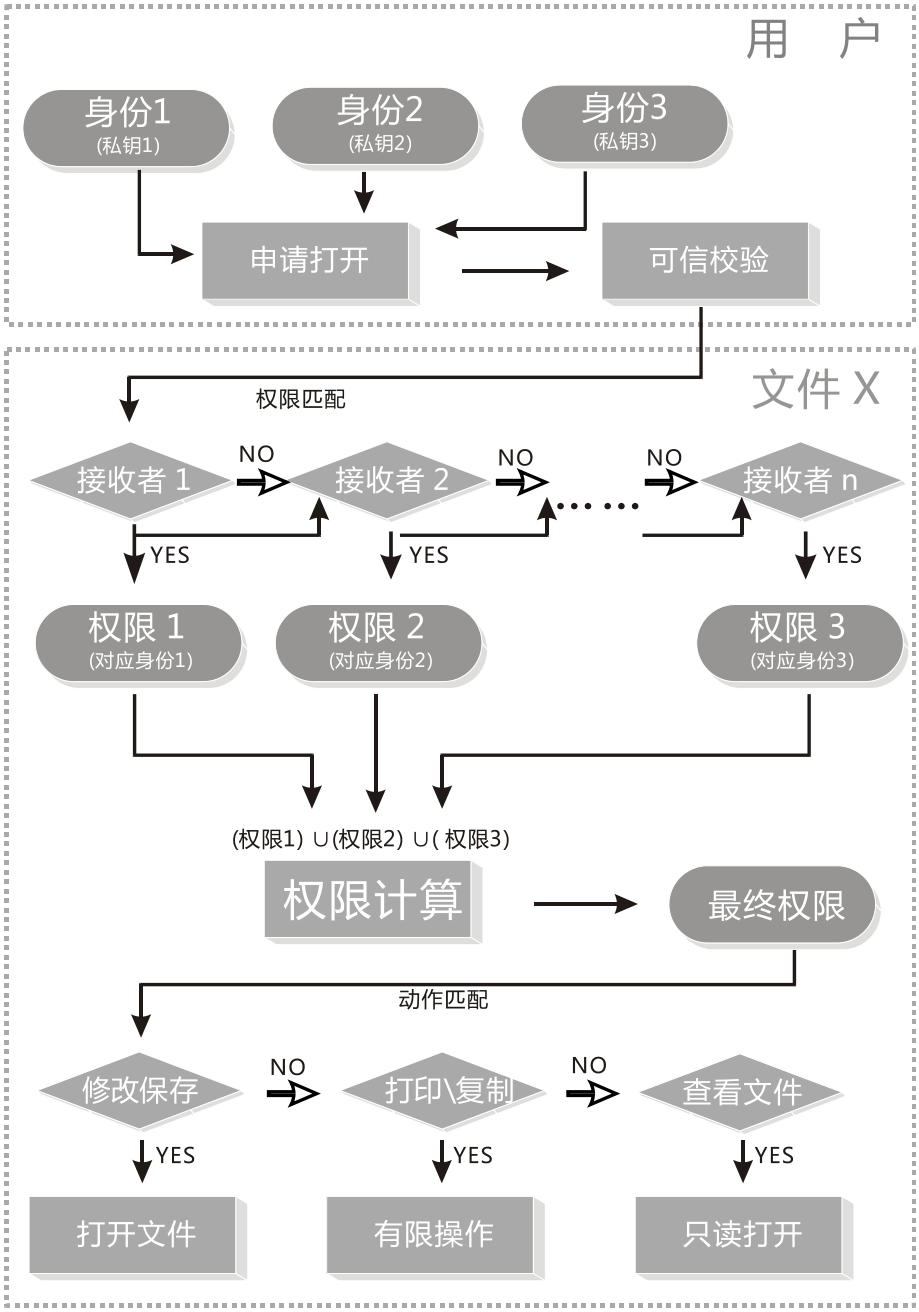
身份接收者

在 PKI 中，非对称算法是体系的基础。用公钥加密一段数据，然后只有用相应的私钥才能解开。这就构成一种最简单的 PKI 应用。为了便于理解，通常将私钥称为身份，公钥称为接收者。

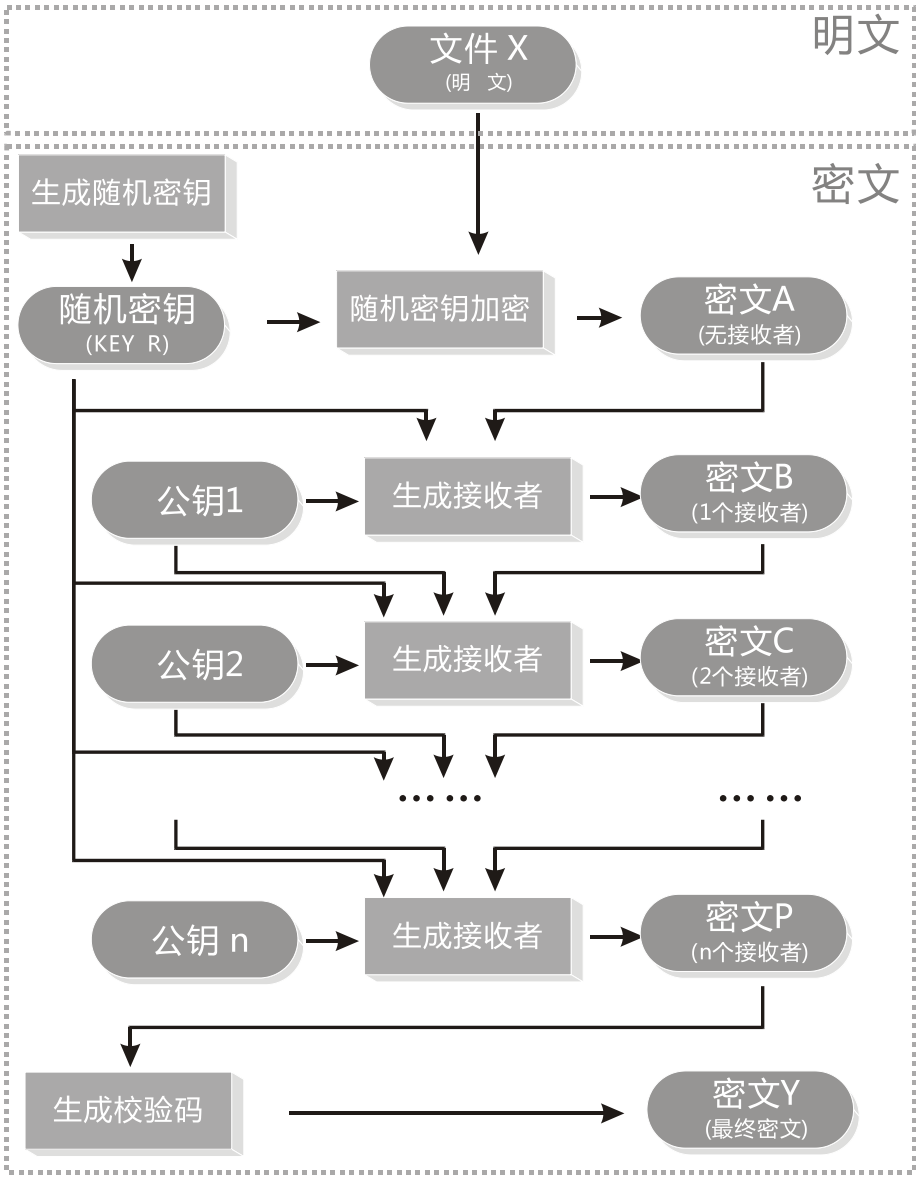
举个形象的例子，我们把一份文件当作为一个仓库，身份就象是你手中的钥匙。而接收者则相当于这个仓库上的门。很显然一个人可以拥有多把不同的钥匙，而一个仓库也可以同时有多个不同的门。

工作流程

打开文件



保存文件



PKI 体系同密级划分体系对比

密级划分的概念来自于保密法。根据规定，国家秘密分为“绝密”、“机密”、“秘密”。在民用领域，根据需要往往又增加一些级别。密级的划分很好的处理了上下级的权限级别。但他更多的是适用于垂直管理。而在复杂民用领域，有很多平行的单元。比如开发部、销售部、财务部等。他们之间并不存在谁的级别比谁更高，但彼此之间文件同样需要保密。

PKI 体系同多密钥体系对比

使用多密钥体系，不同的部门或个人，使用不同的密钥。可以使成员内部有一个分割，不能阅读与已不相关的文件。而对于领导，则可以拥有多个解密密钥，可以打开多个不同部门的文件。但是当不同的部门需要就某些文件交流时，需要将文件解密或者赋予相关人员以更多的密钥。无论是哪一种方案，均会存在泄密的分险。

产品特点

基于 PKI 体系的加密

同传统的透明加密产品相比，凤凰卫士采用 PKI 体系。其加密不再依赖密钥而是依赖数字证书。依赖 PKI 体系，凤凰卫士可以实现各种复杂的应用模型。具体可参见：常见几种部署方案。

两种用户识别模式

根据用户实际情况，凤凰卫士同时支持两种用户识别模式，分别为“硬件号”及“用户名”。对于小规模无域控制器的局域网，可以使用硬件号来管理。对于大规模有域控制器的网络，可以从域控制器上导入“组织单元”，然后以“用户名”进行管理。

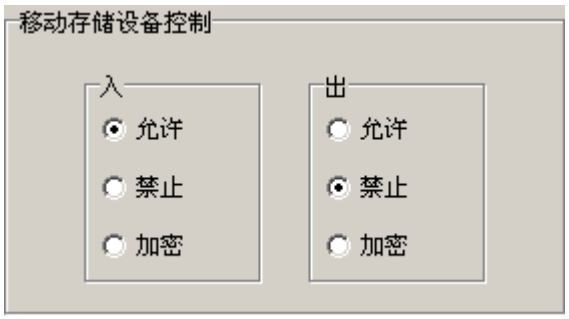
灵活的组策略结构

凤凰卫士采用的组织结构以 Root 为根，可以无限级分组。对于每一个组、用户均可进行单独的设置。同时根据需要，下层组可以选择是否继续上层的设置。当之间的设置有冲突时，自动以最严格的设置为准。

举例来说，有以下组织结构，如下图

子公司 1 的 U 盘规则设置如下图（双向禁止）

设计组 1 的 U 盘规则设置如下图（允许拷入，禁止拷出，即只读）



对于设计组 1 而言，当勾选 

时，则两个规则会进行计算，最终自动采用最严格的策略，即“双向禁止”

当不勾选 

时，只仅采用当前的规则。在本例中，为允许拷入、禁止拷出，即只读模型。

强大而灵活权限控制

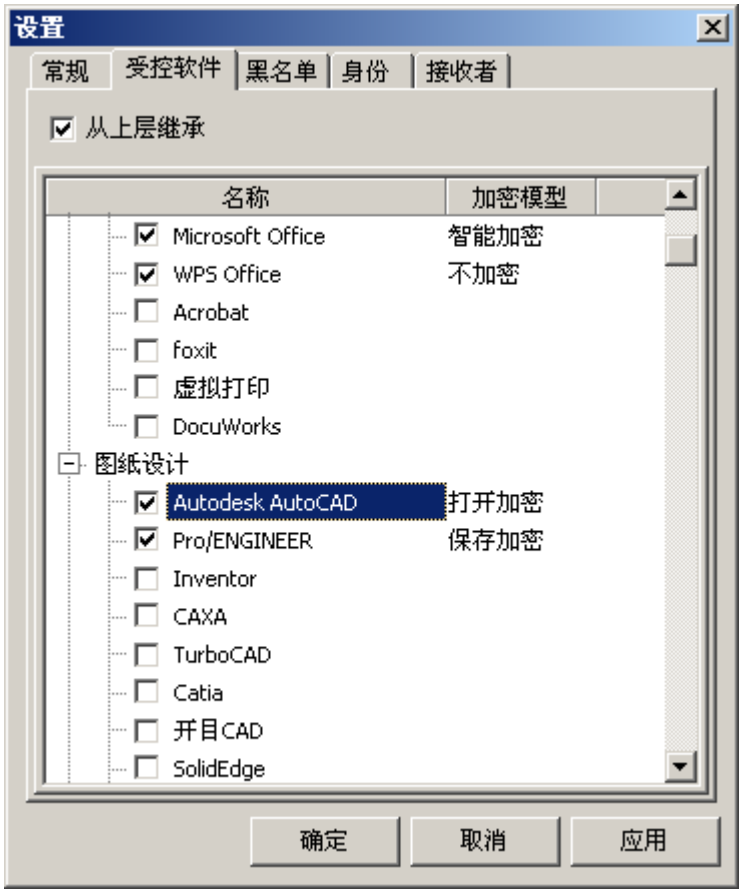
凤凰卫士不是一个单纯的防泄密软件，而是将分级管理的思想纳入其中。举例来说，有技术部、财务部、销售部三个部门。这三个部门的文件需要相互隔离。但有的时候又需要交流，比如财务部要发一份《餐旅报销注意事项》给所有的部门。销售部要发一份客户的要求给技术部，技术部要将设计方案回传给销售部。如果文件在之间流转需要解密的话，将会带来一定泄密风险。而利用凤凰卫士基于 PKI 体系的权限控制，则可以很好的解决这个问题。当财务部需要向整个公司发一份文件时，可以设定其他部门对这份文件的权限为只读。当技术部需要将设计方案传给销售部时，可以设置销售部或者销售部某个人对这份文件权限为只读、不可打印、同时限定使用时间。而所有这些，均不需要解密文件，而只需要调整指定文件的

权限即可。

多种加密模型

凤凰卫士根据实际需要，可以对不同的软件分别实现 4 种不同的加密模型。

以下图为例



Office 采用智能加密的模型，即新生成的文件不自动加密，但可以打开加密的文件，修改保存后，其依旧为加密文件。如果打开修改不加密的文件，保存后，依旧为不加密文件。

WPS 采用不加密模型，即他可以打开加密的文件，但修改保存后文件将会变为不加密，其新建的文件同样为不加密。

AutoCAD 采用打开即加密的模型，只要用 AutoCAD 打开一个文件，如果其为不加密，则首先将其转为加密文件。

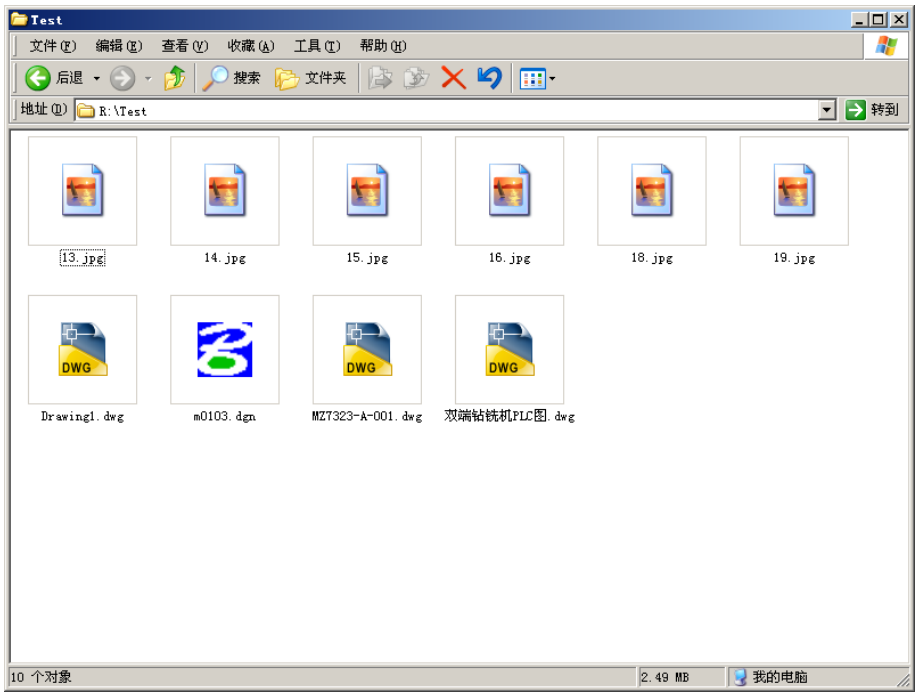
ProE 采用保存加密模型（默认），其新建的文件自动加密，当其打开修改一个不加密的文件，保存后，将会变为加密文件。当打开修改一个加密文件，保存后，依旧为加密文件。

加密文件的预览

对于透明加密产品，其明密文的分隔均是基于进程的。对于 Explore.exe 来说，显然是不需要受控的。那么这就导致一个会影响员工使用习惯的问题。就是对于加密的文件，无法直接预览。

下图为预览不加密文件的情形。可以看到缩略图

下图为预览加密文件的情况，无法看到缩略图



对于凤凰卫士，碰到这种情况只需要在服务器上将需要预览的文件格式设置进去，即可象未安装加密软件一样进行正常预览。

关键技术

凤凰卫士采用 PHOENIX 透明加密内核。其是一个基于应用层的解决方案。在保留了应用层加密原有的稳定、兼容性强等特点外，在多项关键技术上均取得重大突破。能够实现明文不落地的运算，已发展成为一个稳定性，兼容性、速度、抗破解能力均衡的透明加密内核。

内存映射文件（MappingFile）

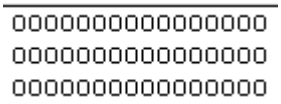
在 PHOENIX 透明加密内核问世之前，内存映射文件一直被业界认为那是不可能在应用层处理的。要处理这个问题，必须进入驱动层。PHOENIX 经过多年研发，使用 PreRead、DelayWrite

技术，成功破解这一难题。使 PHOENIX 有更广泛的适用性和更高的稳定性。

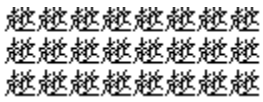
高标准算法的应用

应用层的透明加密与驱动层的透明加密不同，其中有一点表现在 IO 操作上，驱动层的读写是对齐的、整块的读写。而应用层的读写则是随机的，边界、大小均不确定。这种特性，就给加密算法的应用带来了麻烦。正是因为这种难度，部分透明加密产品采用最简单的按位运算的算法，使得安全性存在严重的隐患。而 PHOENIX 透明加密内核独创了预读（PreRead）、延迟写(DelayWrite)技术。将零碎的文件读写操作变为整块的读写。然后再应用各种高标准的算法进行加密。

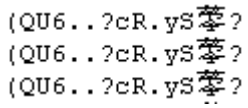
下图为加密前的明文



下图为经过接位运算后得到的密文



下图为 PHOENIX 透明加密内核加密得到的密文



常见的几种部署方案

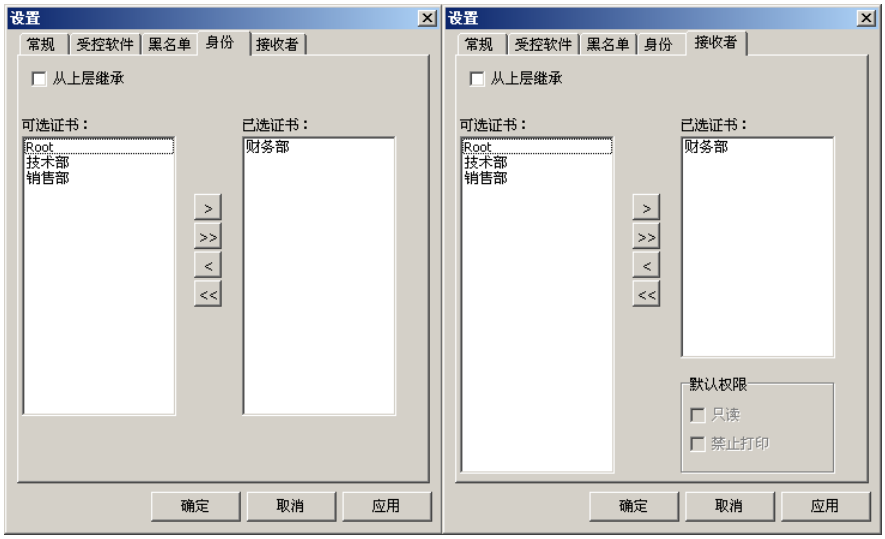
方案一

需要描述

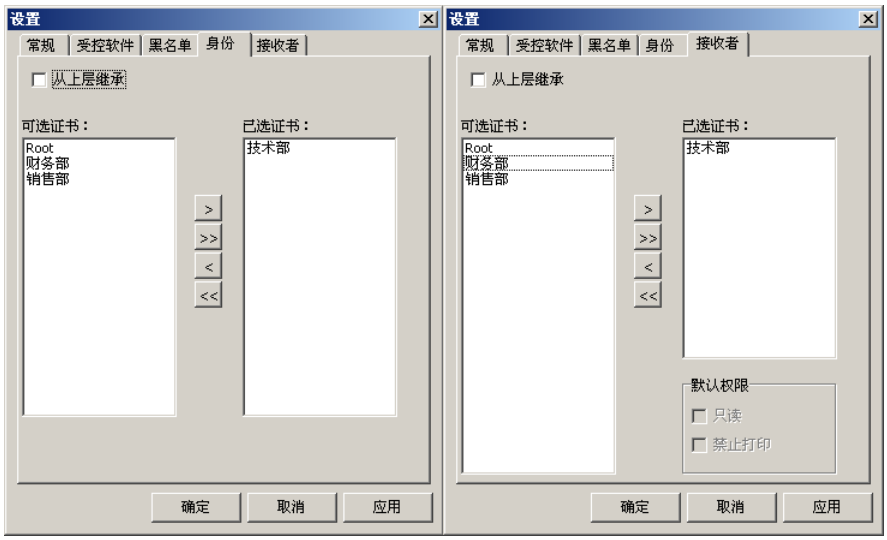
分别在财务部、技术部安装客户端，彼此的文件互不相通。对于上级主管，比如老板，则可以同时打开双方的文件。

实现

财务部的身份及接收者设置



技术部的身份及接收者设置



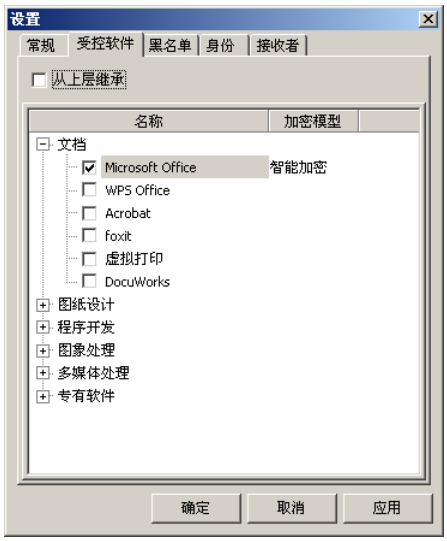
方案二

需求描述

销售部经常需要将文件与外部交流，如果所有的文件均加密，则解密的工作量将会很大。而重要的文件只占很少的一部分。需要实现：对于新做的文件不加密，如果修改不加密的文件，则仍然不加密。如果修改加密的文件，则保存时继续保持加密状态。

实现

销售部的受控软件设置



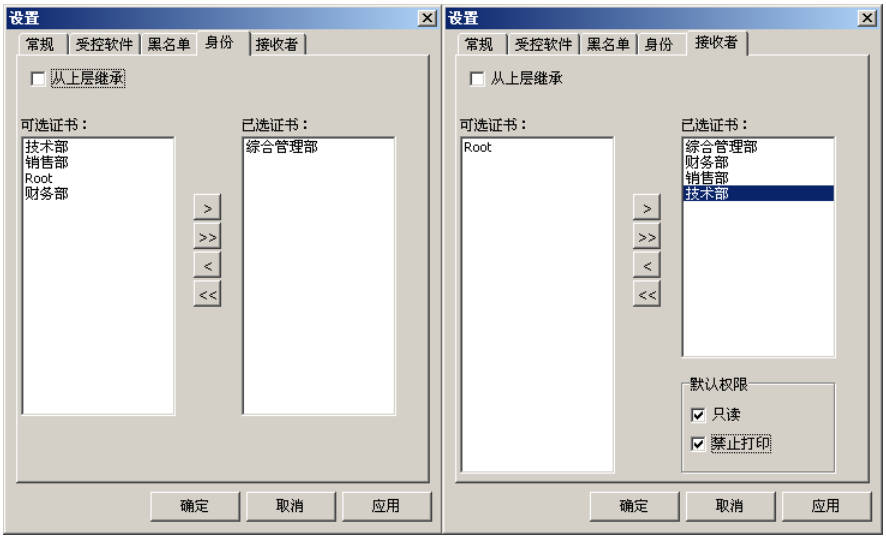
方案三

需求描述

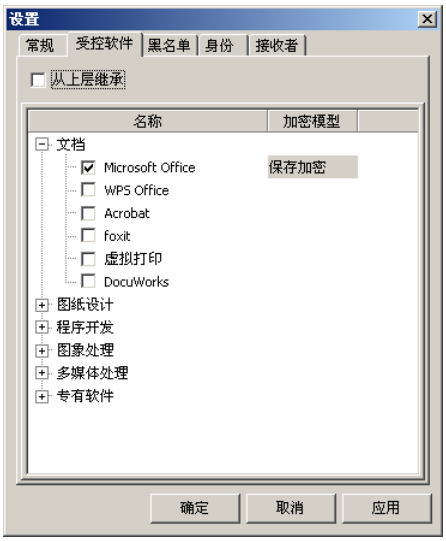
管理部需要加密 Office 文件，技术部则仅加密图纸设计文件。但管理部需要将 Office 交给其他部门包括技术部看。

实现

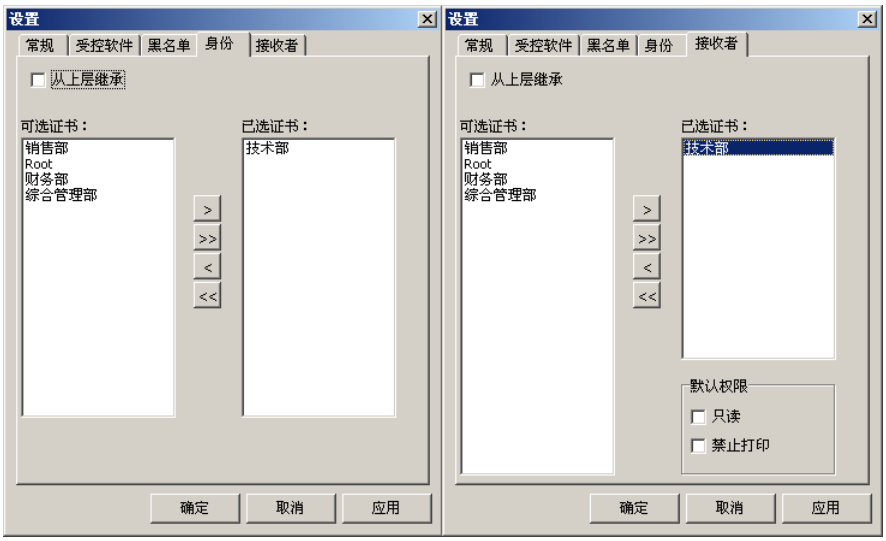
管理部身份接收者设置。在接收者中，将其他部门如技术部的权限设为只读及禁止打印。



管理部的受控软件设置



技术部的身份接收者设置



技术部的受控软件设置

方案四

需求描述

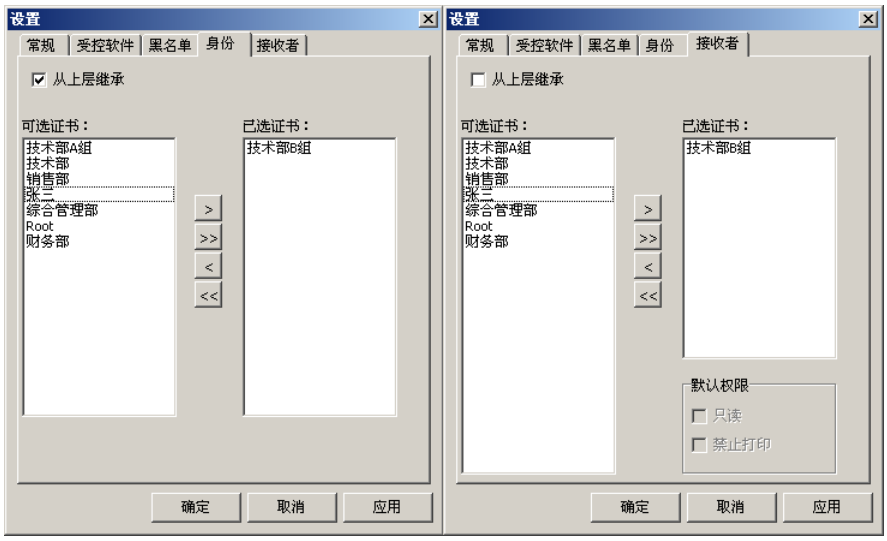
技术部 A 组设计的产品需要经常和技术部 B 组的人员交流，但是希望仅让技术部 B 组的某个人能够看到，并且限制他不能修改打印文件。

实现

为技术部 B 组特定的人生成一份数字证书。

A 组的身份接收者设置。在接收者中，要将张三的权限设为只读及禁止打印

B 组的身份接收者设置



张三的身份接收者设置