铁卷电子文档保护系统

技术白皮书

V1.0

仅供参考

2006.02.03

深圳市大成天下信息技术有限公司

ShenZhen Unnoo Information Tech., Inc.

二〇〇六年一月

版权说明

商标信息

文档号：UnnooP101302
2006 年 1 月

目录

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;
- 网络骇客通过网络攻击等非法手段取得访问权限，并把文件复制带走;
- 员工没有保密观念造成无意识地泄露，如使电子文档传给了没有阅读权限的阅读者，造成秘密信息公开;
- 计算机病毒自动发送电子文档。

从政府文件、企业工程图纸、标准操作程序到销售展示，各类文档对政府、企业的平稳有效运行是至关重要的。目前随着电子政务的深入开展，无纸办公、MIS、ERP 等系统也在政府及企业得到广泛的应用，利用网络发布、传递信息的个人和企业数量更是日益增长。

但目前的现状是当人们议论到信息安全，往往首先想到的是外部攻击，因此联想到的是防火墙、入侵检测、内部网和外部网物理隔离等技术，内部的信息泄露往往得不到应用的重视。

仅举几个数据作为佐证，我们就该能了解电子文档保护的必要性：但据 CSI/FBI 统计 2005 年各种安全漏洞造成的损失中，30%-40%是由电子文件的泄露造成的；而 Fortune 排名前 1000 家的公司中，每次电子文件泄露所造成的损失平均是 500,000 美元。

因此，对电子文档进行保护势在必行。

2.铁卷的应特点、优势及应用

2.1.产品特点

铁卷通过以下功能，为您提供值得依赖的文档保护方式:

- 全程保障: 从文档创建、传递直至销毁全过程完全控制。
- 介质无关: 无论通过存储（USB、光盘、软驱、ZIP 盘等）或网络（Email、FTP、红外、蓝牙等），均在保护范畴（介质无关的特性能够使用户不必为新的存储介质和传输协议/方式而被迫升级系统）。
- 集中控制: 通过集中控制台对每个客户端进行轮询和管理，有效保证电子文档既受保护，又能够灵活使用。
- 用户透明: 客户端无界面、无进程、无端口，使用者完全无需更改原有电子文档使用习惯。

2.2.技术优势

在电子文档保护领域曾经存在的最大挑战在于无法全程监控,让我们假想这样一个场景:

某 IT 企业融资前的一个月，公司财务总监编制了一份详细的融资及财务报告后发送给公司高管，同时抄送到自己的公网邮箱，准备进一步修改。

两天后，总经理的笔记本电脑失窃……

这个很普通的操作实际上可能存在的风险点包括:

1、财务总监的电脑;

2、邮件发送过程中的传输链路;

3、所有公司高管的邮箱;

4、收取过邮件的高管电脑;

5、财务总监的“公网邮箱”;

这一场景也对电子文档保护厂商提出了几个问题:

1、如何保障文档创建者（发送者）创建（发送）的是受保护的文件?

2、如何保障传输过程中即便有“窃贼”，也无法浏览文件内容?

3、如何保障文件的接收者能正常打开，但却无法通过任何介质将文件发给其它人?

目前国际上的电子文档保护系统，主要分为两大类型:

1、文件加锁->解锁型：通过文档的创建和发送人对文件加锁，再由文档的接收人解锁后阅读;

2、格式转换型：通过文档的创建和发送人将电子文档转换为另一种专有格式，再采用特定的查看工具打开阅读。

这两种保护方式存在的最大**缺陷**在于:需要创建人手工将原始文件转换为加密或专有文件。这会带来:

1、文件创建和发送者仍然能够不受控制地发放未给处理的文档;

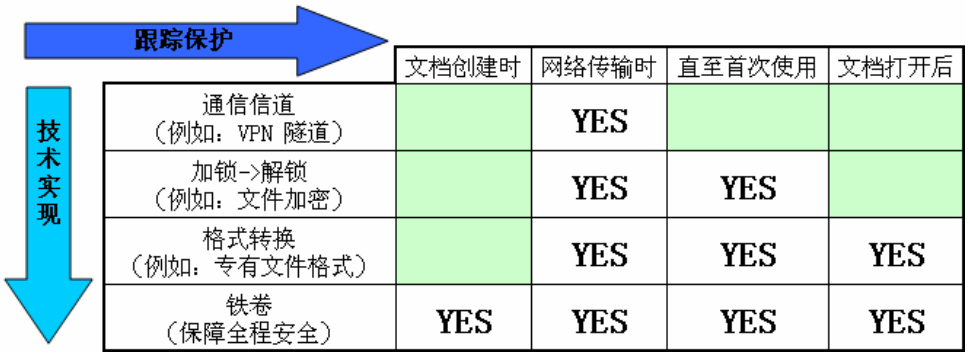
2、文件创建和发送者需要有较高的安全意识和安全操作习惯，需要对每个关键文件都进行加密操作，否则电子文档仍旧不受控制;

而部署铁卷后的场景将是:

某 IT 企业融资前的一个月，公司财务总监编制**（在编制过程中，这份电子文档已经默认保存为密文，但是公司的财务总监却完全感觉不到，因为他仍然使用 Microsoft Word 对文件进行编辑）**了一份详细的融资及财务报告后发送给公司高管**（因为也同样安装了铁卷，因此他们能够正常打开并阅读文件）**，同时抄送到自己的公网邮箱**（商业间谍盗走了文件，但却由于该文件是密文，无法打开）**，准备进一步修改**（回到家里，发现收回的文档无法在家里的电脑上打开）**。

两天后，总经理的笔记本电脑失窃**（由于控制台设置了心跳轮询，电脑遗失后无法及时与服务器通讯，读取功能失效，所有文件均暂时无法读取。如果电脑又失而复得，只需要到服务器上进行一次验证，便又能够正常使用）**……

因此对比多种电子文档保护技术，综合如下:



	文档创建时	网络传输时	直至首次使用	文档打开后
通信信道（例如：VPN 隧道）		YES		
加锁->解锁（例如：文件加密）		YES	YES	
格式转换（例如：专有文件格式）		YES	YES	YES
铁卷（保障全程安全）	YES	YES	YES	YES

2.3. 应用范围

政府和军队需要严格保护许多不对外公开或者限制部门及个人阅读、复制的安全性文档，如政府公文、机要文件、会议记录、涉密文件等。

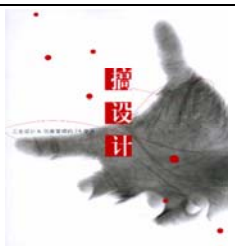
银行、证券等机构中有大量与现金相关联的敏感信息，需要严格控制，以防止商业秘密泄露，如投资融资信息、大客户信息、交易资料及帐目分析等。

制造业有许多重要文件如产品设计图纸、产品设计文档、专利及商业秘密等资料具有极高的价值。

GIS 及地图领域由的航空图片，详细地图资料都是有价数据。

律师楼的合同、诉讼文档往往涉及到客户信息甚至各种各样的机密。

保健及保险行业则是患者病例、保险客户的信息等。

<table>
<tr>
<td>制造企业、设计院
- 产品设计图纸
- 产品设计资料和文档
- 专利设计及商业机密
  </td>
<td>GIS及地图领域
- 航空图片
- 详细地图
  </td>
</tr>
<tr>
<td>政府、军队
- 工作计划、档案
- 军事计划
- 工作预算
  </td>
<td>金融机构
- 帐目分析
- 交易资料
- 数据库
  </td>
</tr>
<tr>
<td>律师行
- 合同
- 诉讼文档
  </td>
<td>保健及保险行业
- 患者病例
- 保险需求
- HIPPA 规章
  </td>
</tr>
</table>

因此，电子文档保护系统的应用范围极其广泛，受到了各领域的普遍关注。

3. 铁卷如何保护电子文档

铁卷遵循简洁但严格的“默认禁止”保护规则：未经批准，都不允许外发。

铁卷电子文档保护系统的部署、使用过程如下:

3.1. 安装

铁卷电子文档保护系统需要安装客户端（Agent）和服务器（Server）。Agent 安装在所有希望受保护的工作站上，Server 安装在文档管理员专用的文档管理服务器上。

铁卷的 Agent 建议部署在企业内部网所有客户端上，用于对客户端创建、打开、保存文档的全过程进行保护。（Agent 的安装仅需要双击安装包即可顺利完成，安装完毕后需要重新启动电脑，才能够起到保护作用。）

铁卷的 Server 端能够显示企业内部有多少台电脑在线，并能够通过心跳监测对电脑的机密文档进行控制、启用或禁用某台客户端的解密功能、设置特定客户端可以**在规定时间内离线**察看文档。

3.2. Agent 使用

对普通用户而言，铁卷完全处于透明状态。安装完 Agent 后，用户仍然使用原有的客户端创建、打开和保存文档。

但此时创建（写入）的文档全部经过加密处理，只有同样安装有铁卷 Agent 的计算机能够正常打开加密文档，Agent 会定时与 Server 进行心跳连接，一旦连接失败并且超出了 Server 的规定时间，则 Agent 失效，本机所有加密文件将无法被打开。直至 Agent 与 Server 再次通讯成功并解除锁定。

这种设计模式保证了:

1、所有用户在企业内部使用文档完全透明，对各种格式文件均能顺利打开;

2、用户可以通过任何存储介质（U 盘、软盘、光盘等）或网络（Email、FTP 等）将文档传递到外网，但这时所有文档全部处于加密状态;

3、无论是内部恶意员工或是外部黑客试图窃取文件，都只能获取加密文档;

4、笔记本电脑如果失窃，由于心跳连接失效，窃贼将无法察看加密文档。

3.3. Server 使用

文档管理员拥有对全部文档的控制权限，类似于 Unix 系统中的根用户（root），他能够使用铁卷的服务器进行:

1、瞬间高效批量文档加解密;

2、观测 Agent 状态，能够灵活控制某一台 Agent 失效（设置失效标记后，该 Agent 便无法打开所有加密文档）;

4. 系统部署

4.1. 系统运行的软硬件需求

服务器端硬件需求:

- CPU：不低于 Pentium III 2.2G
- 内存：不低于 512M，建议 1G 以上
- 硬盘：不低于 50M 剩余空间，建议 500M 以上剩余空间
- 网卡：至少一块 100Mbps 以太网卡

客户端硬件需求：

- CPU：不低于 Pentium II 1G
- 内存：不低于 256M
- 硬盘：不低于 20M 剩余空间，建议 200M 以上剩余空间
- 网卡：至少一块 100Mbps 以太网卡

软件需求：

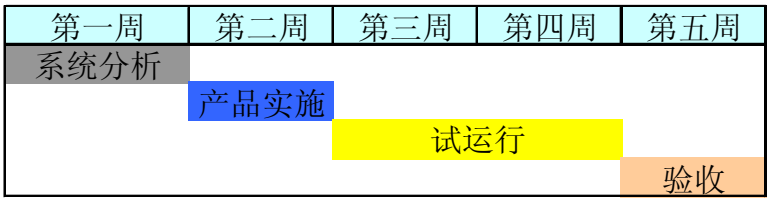
Windows 2000 SP4 以上，包括 Windows XP、Windows 2003

网络需求：

建议与 AD 集成，能够更大程度提升安全性。

4.2. 实施进度表

通常情况下，对中型规模的企业，铁卷部署周期为五周时间。时间计划预估如下：



4.3. 目前版本

铁卷目前推出的版本为制造业专版，该版本对 AutoCAD 等制图软件及十余种 CAD 格式进行保护。

5.技术支持

如果用户在安装和使用铁卷电子文档保护系统时遇到问题，请及时与我公司技术支持部门联系，我们将尽力和您一起解决问题，最大限度地保护用户的权益。

要获得有关铁卷电子文档保护系统的技术支持，请按下列方式与深圳市大成天下信息技术有限公司技术支持部门联系：

邮件：service@unnoo.com

电话：(0755)86092828

传真：(0755)86092828

假如您利用 E-mail 或传真和我们联系，请在问题报告中包含用户 ID、版本信息、主机使用平台名称和尽可能详细的问题描述，以便于我们能尽快解决您的问题。