

---

# 密文卫士™电子文档防泄密系统

技术白皮书

V 1.1

上海谷亘软件有限公司

Shanghai Gugen Software Co., Ltd.

2008年7月

## 版权声明

©版权所有 2007-2008, 上海谷巨软件有限公司

本文是上海谷巨软件有限公司(简称谷巨软件)密文卫士™产品的一部分。本文件中出现的任何文字叙述、插图、方法、过程等内容,除另有特别注明,版权均属谷巨软件所有,受到有关产权及版权法保护。任何单位、个人未经谷巨软件的书面授权许可,不得以任何方式复制或引用本文件的任何片断。

版权所有,侵权必究。

## 目 录

密文卫士™电子文档防泄密系统.....	0
1 应用背景.....	3
1.1 电子文档防泄密的需求.....	3
1.2 电子文档泄密的途径.....	3
1.3 保护电子文档的方法.....	4
2 产品概述.....	4
3 产品结构.....	6
4 产品功能模块.....	7
4.1 虚拟磁盘子系统.....	7
4.2 进程监控子系统.....	8
4.3 P2P点对点文件交换子系统.....	8
4.4 加解密子系统.....	9
4.5 通讯子系统.....	9
4.6 Internet访问控制模块.....	10
4.7 文件服务器访问控制模块.....	10
4.8 打印监控模块.....	10
5 产品特色.....	10
5.1 内核驱动, 安全可靠.....	10
5.2 用户友好, 随时退出.....	11
5.3 强制保护, 零管理.....	11
5.4 文件交换方便, 无需授权.....	11
5.5 全程监控, 全方位监控.....	12
5.6 离线使用方便.....	12
5.7 版本控制和权限管理灵活.....	12
6 运行环境.....	13
7 联系方式.....	14

# 1 应用背景

## 1.1 电子文档防泄密的需求

随着计算机应用的普及和深入，越来越多的文件以电子文档的形式生成、保存。而计算机网络、各种便携式存储设备的发展，为电子文档的交换流通提供了便利的手段。

但是人们很快发现，正是由于这些技术进步带来的便利，使得对电子文档进行保护，防止机密的电子文档泄露出去比保护传统的纸质文档更加困难。

因此，在信息化的时代，企事业单位面临着既要充分利用现代科技提高自己的工作效率，又要保护自己的劳动成果的挑战。

## 1.2 电子文档泄密的途径

电子文档的泄密指电子文档从组织内部传输到组织外部，或者从有权访问的人传输到无权访问的人，并且可以查看到它们包含的内容。

电子文档的泄密途径有以下几种常见的形式：

内部员工因为各种原因，把涉密电子文档拷贝到移动盘带走，或通过计算机网络向外发送，造成主动泄密；

网络黑客通过安装木马程序等非法手段，把文件复制出去造成泄密；

内部员工由于缺少有效保密工具和手段而造成被动泄密；

计算机失窃、遗失造成泄密；

计算机病毒自动往外发送电子文档造成泄密等等。

根据 CSI/FBI 2006 年的计算机犯罪和安全调查，各种发生的计算机安全事件中，可能造成电子文档泄密途径的病毒占了 65%，电脑失窃占 47%，内部网络滥用占 42%，非法访问占 32%。

## 1.3 保护电子文档的方法

电子文档泄密事件的发生，对企业所带来的伤害和损失，是非常严重的，有可能直接导致企业的破产！

因此，必须采用有效手段保护机密的电子文档。

根据 CSI/FBI 2006 年的计算机犯罪和安全调查，在被调查的 616 家美国公司中，为保护信息，63% 的公司传输数据时进行加密，48% 的公司存储数据时进行加密。

密文卫士™是保护电子文档的有效工具，它提供了存储加密和传输加密功能，防止自动和被动泄密。

## 2 产品概述

密文卫士™是谷巨软件的电子文档防泄密产品。该产品可有效防止员工主动、被动泄密，防止电脑被盗、遗失泄密，防止恶意木马程序、病毒等复制发送涉密电子文档泄密。

产品借鉴了现有的一些电子文档防泄密产品，除了提供高效的防泄密功能外，还有针对性地在安全性、易用性和可维护性方面有所创新。

密文卫士™使用虚拟磁盘技术来存放涉密电子文档。系统在初始化时创建一个文件，并按照一定的格式格式化，然后从服务器获得该文件的加解密密钥，该文件创建完成后就可以被映射到一个虚拟磁盘。在每次映射加载该虚拟磁盘时，系统都需要从服务器获取该文件的加解密密钥。

密文卫士™在加载了虚拟磁盘后，用户就可以像使用其它磁盘一样使用该虚拟磁盘了。唯一的区别是，保存在该磁盘的文件都是加密的。

密文卫士™采用了世界最先进的 256 位的 AES 对称加密算法来加密存放的涉密电子文档。加密密钥由服务器随机产生，密钥保存在使用了 TPM 安全芯片的新一代安全服务器的安全芯片内，也可以存放在 USB 密钥内。系统采取“驱动层”透明加密技术提供完全自动化、动态化、透明化的涉密电子文档加密保

护。

在正常的工作环境下，客户端系统启动时自动从服务器获取密钥，该密钥用于涉密电子文档动态透明解密。而一旦脱离工作环境（离线或涉密电子文档非法复制出去），因为无法获取密钥，涉密电子文档将不能使用，进而达到防止内部涉密电子文档非法外流而泄密，非法外流的途径包括电脑遗失、被盗、主动非法复制等途径。

密文卫士™客户端系统在加载了虚拟磁盘后，用户只能往该虚拟磁盘复制、新建涉密电子文档，不能把虚拟磁盘中的涉密电子文档复制到其它磁盘。更严格的是，系统禁止向非虚拟磁盘的其他磁盘写文件。这样就从根本上阻止了员工主动泄密的渠道。

密文卫士™客户端系统限制可以访问虚拟磁盘的进程，只有经过认证的信任进程才可以访问虚拟磁盘。信任进程的特征在实施时定制写入客户端系统，系统根据信任进程的特征而不是进程名称来区别进程。这样系统就把可能造成泄密的程序进程阻挡在虚拟磁盘之外，非信任的进程包括各种网页浏览器、邮件客户端、木马程序、病毒程序等。

密文卫士™除了提供涉密电子文档的加密存放，还提供涉密电子文档的加密传输。系统提供的点对点的加密文件传输功能使用动态随机密钥来保证传输的安全。客户端系统运行时将动态刷新在线客户端用户列表，可以方便地给在线的用户发送电子文档，也可以主动共享电子文档，由其他用户来读取。但是，共享和发送的电子文档必须是在虚拟磁盘中的电子文档。接收或者复制到的电子文档也必须存放在虚拟磁盘中。

密文卫士™只需在访问加密盘中的涉密电子文档时再启动。系统没有启动时，用户只能看到一个大文件，该文件内容加密，就算复制或发送出去，也是无法解密的数据。由于只需在需要时启动，密文卫士™将不影响用户的大部分非涉密操作。

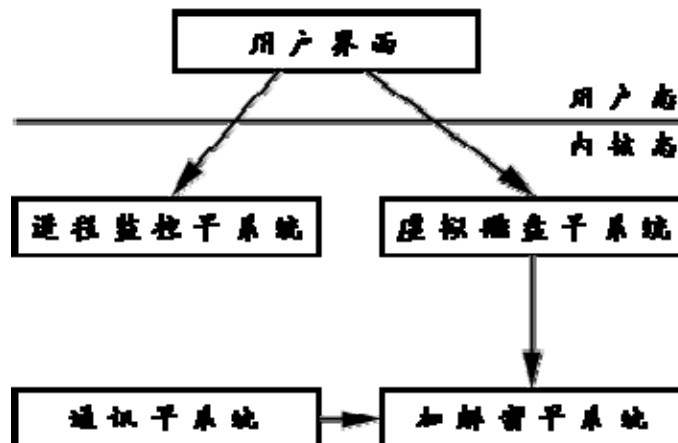
### 3 产品结构

密文卫士™产品基于客户端/服务器架构。服务器和客户端基本结构相同，只是服务器负责客户端加解密密钥的生成、保存和涉密电子文档的解密。

密文卫士™产品包括虚拟磁盘子系统、进程监控子系统、P2P 点对点文件交换子系统、加解密子系统和通讯子系统。

虚拟磁盘子系统负责将一个文件映射成一个虚拟磁盘；进程监控子系统负责监控合法和非法进程，监控涉密磁盘和普通磁盘之间的文件操作；P2P 点对点文件交换子系统负责客户端之间以及和服务器之间的涉密电子文档的安全交换；加解密子系统负责为虚拟磁盘子系统和 P2P 点对点文件交换子系统提供加解密服务；通讯子系统负责为客户端和服务器以及 P2P 点对点文件交换子系统提供通讯服务。

整个产品的结构如下图所示：



服务器由于需要安全地保存客户端的加解密密钥，因此服务器要使用带有 TPM 安全芯片的新一代安全服务器，也可以使用 USB 密钥(USB Key)。使用 TPM 安全电脑芯片或者 USB 密钥保存加解密密钥，只有程序才可以读取到该密钥，即使是电脑管理员也无法获得该加解密密钥。

客户端程序在初次使用时要设置好服务器程序所在服务器的 IP 地址或者机器名。客户端程序在相互发送文件时，只需要知道对方的 IP 地址或者机器名就可以了。

## 4 产品功能模块

### 4.1 虚拟磁盘子系统

密文卫士™使用虚拟磁盘技术来存放涉密电子文档，虚拟磁盘子系统使用该技术将一个文件映射成一个虚拟磁盘。

虚拟磁盘子系统为区分涉密电子文档和非涉密电子文档提供了便利。所有涉密电子文档保存在虚拟磁盘文件中，非涉密电子文档保存在其他磁盘中。

虚拟磁盘的大小在创建虚拟磁盘是指定，系统在初始化时创建一个文件，并按照一定的格式格式化，然后从服务器获得一个该虚拟磁盘文件的加解密密钥。可以创建多个虚拟磁盘文件，但是密文卫士™的 V1.0 版本一次只能加载一个虚拟磁盘文件。

虚拟磁盘中的文件被加密保存，系统在保存文件时自动加密，在读取文件时自动解密。加解密操作在系统内核层由驱动程序自动完成。系统在保存文件到其它磁盘和从其它磁盘读取文件时不进行加解密操作。

虚拟磁盘在需要时加载，在不需要时卸载。退出密文卫士™应用时自动卸载虚拟磁盘。加载虚拟磁盘后进入涉密态，卸载虚拟磁盘后进入非涉密态。

虚拟磁盘的使用和其它磁盘一样，可以在里面创建文件、删除文件、修改文件名，创建目录、删除目录、修改目录名。

卸载虚拟磁盘后，用户将看不到原来虚拟磁盘中的文件及其目录结构。用户只能看到一个创建虚拟磁盘时指定的那个普通文件。所有涉密电子文档隐藏在该文件中，无法从该文件中获得涉密电子文档的内容。

在每次加载虚拟磁盘时，指定一个需要映射的盘符，然后系统自动从服务器获得该虚拟磁盘文件的加解密密钥。

密文卫士™在加载了虚拟磁盘后，用户就可以像使用其它磁盘一样来使用该虚拟磁盘了。唯一的区别是，保存在该虚拟磁盘的文件都是加密的。

## 4.2 进程监控子系统

密文卫士™客户端系统在加载了虚拟磁盘后，用户只能往该虚拟磁盘复制、新建涉密电子文档，不能把虚拟磁盘中的涉密电子文档复制到其它磁盘。更严格的是，系统禁止向非虚拟磁盘的其他磁盘写文件。这样就从根本上阻止了员工主动泄密的渠道。完成这项功能的就是进程监控子系统。

进程监控子系统在系统加载了虚拟磁盘后开始监控用户操作。进程监控系统监控所有进程，任何进程对非虚拟磁盘的写操作被拒绝，但是任何进程对虚拟磁盘的写操作被允许，涉密电子文档“只进不出”。

进程监控子系统只允许经过认证的信任进程访问虚拟磁盘。信任进程的特征在实施时定制写入客户端系统，系统根据信任进程的特征而不是进程名称来区别进程。信任进程的特征指信任进程的可执行文件的摘要，通过标准的摘要算法计算出可执行文件的摘要，然后保存在系统中，系统运行时检查进程的可执行文件摘要是否在允许列表中。

这样系统就把可能造成泄密的程序进程阻挡在虚拟磁盘之外，可能造成泄密的程序包括各种网页浏览器、邮件客户端、木马程序、病毒程序等。

通过比较可执行文件的摘要，任何将非信任进程执行文件改名成信任进程执行文件的恶意攻击，包括修改信任进程执行文件的攻击都将无法奏效。

进程监控子系统还监控网络连接。在涉密态，只有文件交换子系统的网络通讯可以使用，其它网络端口都被禁止使用。从而防止通过网络共享、远程桌面等技术手段非法复制涉密电子文档。

## 4.3 P2P点对点文件交换子系统

密文卫士™的点对点文件交换子系统提供涉密电子文档的点对点文件交换功能。在协同办公环境下，文件交换非常频繁，需要多人协作对一份电子文档进行编辑。点对点文件交换功能提供了便利的手段支持协作办公。

点对点文件交换子系统使用动态刷新技术更新在线用户列表。用户通过在用户列表选择要发送文件的用户，就可以为该用户发送涉密电子文档。

用户也可以主动共享电子文档，由其他用户来读取。

但是点对点文件交换子系统只为所有涉密态的用户提供文件交换功能。共享和发送的电子文档必须是在虚拟磁盘中的电子文档。接收或者复制到的电子文档也必须存放在虚拟磁盘中。

系统在传输涉密电子文档时使用动态随机密钥来保证传输的安全。

## 4.4 加解密子系统

密文卫士™加解密子系统负责为虚拟磁盘子系统和 P2P 点对点文件交换子系统提供加解密服务。

密文卫士™采用了世界最先进的 256 位的 AES 对称加密算法来加密存放的涉密电子文档。加密密钥由服务器随机产生，密钥保存在使用了 TPM 安全芯片的新一代安全服务器的安全芯片内，也可以存放在 USB 密钥内。加密密钥长度达 512 位，由大小写字母、数字、特殊字符组成。系统采取“驱动层”透明加解密技术提供完全自动化、动态化、透明化的涉密电子文档加密保护。

客户端和服务端通讯时，系统使用对称和非对称混合加密技术。非对称加密采用 RSA 算法，对称加密采用 Blowfish 算法。系统使用 RSA 公钥加密交换对称加密的会话密钥。

系统使用 RSA 公钥来相互认证。在系统初始化时，会为每个客户端生成一对 RSA 公钥和私钥。用户的公钥发送给服务器和同事，用来加密发送给自己的会话密钥。

## 4.5 通讯子系统

密文卫士™通讯子系统负责为客户端和服务端以及 P2P 点对点文件交换子系统提供通讯服务。

由于系统禁止所有的网络活动，系统自己提供了用于文件交换的通讯子系统。系统使用 8888 端口作为默认的服务端口。

## 4.6 Internet访问控制模块

密文卫士™ Internet 访问控制模块是可选的服务器模块，安装该模块后，可以结合代理服务器实现在涉密态下可控的上网。即通过配置代理服务器，使涉密客户端只能通过该代理来访问指定的站点和服务。

## 4.7 文件服务器访问控制模块

密文卫士™文件服务器访问控制模块是可选的服务器模块，文件服务器安装该模块后，通过在客户端上配置该文件服务器，即可在涉密态下读写该文件服务器的网络共享文件。而没有配置文件服务器的客户端在涉密态下是不能向网络共享写操作的。

## 4.8 打印监控模块

密文卫士™打印监控模块是可选的服务器模块，服务器安装该模块后，通过在客户端上配置该服务器，即可在涉密态下通过该服务器打印涉密文件，并记录打印日志和保存一份被打印文件。

# 5 产品特色

## 5.1 内核驱动，安全可靠

密文卫士™的虚拟磁盘技术和进程监控使用内核驱动的方式实现。使用内核驱动技术将软件和操作系统紧密结合，攻击者难于解除监控。系统在底层动态透明工作，而非使用应用层挂钩技术，能抵抗破解读出明文，也更不会被当成病毒被禁止运行。即使内核驱动被卸载，系统也将关闭虚拟磁盘，使得攻击者无法获得涉密电子文档。

## 5.2 用户友好，随时退出

密文卫士™使用内核驱动的方式实现虚拟磁盘和进程监控，对于用户而言完全感觉不到系统的加密和解密操作。由于采用了高效的加密密算法，打开和保存文件操作几乎和原来一样，感觉不到延迟。

密文卫士™仅需要在需要操作涉密电子文档时才启动，在操作完成后可随时卸载虚拟磁盘退出。由于不是完全控制用户的电脑，不会限制和影响用户的非涉密操作，对于用户而言，使用电脑进行涉密操作的时间只占全部工作时间的少部分，完全控制系统会使用户一些非涉密操作无法完成，降低了非涉密工作的效率和丧失了使用电脑娱乐休息的功能。

密文卫士™启动后不会隐藏进程、不存在进程无法杀死的流氓软件特征。在用户需要时可以立即退出。

## 5.3 强制保护，零管理

密文卫士™简化了电子文档的权限类型，即只分为涉密和非涉密（也称为普通）。而且涉密电子文档不分所有者，只要是涉密电子文档，就归企业所有，任何人不能复制出公司。采用这种权限模型，完全简化了企业的管理，可以做到零管理。特别是对于人员众多、涉密电子文档众多的企业，一个个电子文档给一个个人授权，无论是文档创建者还是专职管理员，都难以应对，而且随着时间的推移，人员变化和文档变化也无法及时更新。

采用这种简单有效的权限模型，除了省却了授权过程，也可以完全取消策略的定义。密文卫士™系统策略简单，完全内置在系统之中而无需管理员变更。而依赖于管理员人工设置的监控策略，往往会出现由于管理员失职、疏忽、违反规定操作而造成泄密。

## 5.4 文件交换方便，无需授权

密文卫士™采用了简化的电子文档的权限类型，除了将电子文档分为涉密和非涉密外，将用户也分涉密和非涉密。

基于这种模型的授权非常简单，即涉密用户可以使用涉密电子文档，非涉密用户不能使用涉密电子文档。

根据以上这个简单的授权策略，涉密电子文档的交换也非常简单，即涉密电子文档只能发送给涉密用户。

## 5.5 全程监控，全方位监控

密文卫士™从涉密电子文档新建开始，全程监控涉密电子文档。只要电子文档保存在虚拟磁盘中，就受到保护。

密文卫士™提供全方位的监控，除了禁止将涉密电子文档复制到普通磁盘，还禁止非信任进程对涉密电子文档的访问，在退出客户端系统时还清空剪贴板和关闭打开的窗口，以防它们保留涉密电子文档的内容。

密文卫士™还限制对网络的使用，在进入涉密态后，只有自己的文件传输系统可以使用。

## 5.6 离线使用方便

密文卫士™可方便地离线使用。由于需要和客户交流、演示，一些涉密电子文档需要带出公司。在不能解密的情况下，可以通过在公司架设拨号服务器远程拨入公司获得解密密钥。

如果客户那里没有电话线路可以使用，也可以申请使用服务器的USB密钥，该USB密钥是服务器USB密钥的一个复制品，客户机通过将服务器设置成本机，并插入USB密钥就可以打开涉密电子文档。

## 5.7 版本控制和权限管理灵活

密文卫士™可结合各种版本控制和权限管理系统使用，实现更细粒度的访问控制，如结合 Visual SourceSafe 可用来管理软件公司的程序源代码。

## 6 运行环境

密文卫士™客户端运行环境:

- ✓ 操作系统: Windows 2000、Windows XP 及各种升级版本
- ✓ CPU : Intel Pentium 4 系列以上 32 位处理器
- ✓ 内存: 512MB
- ✓ 硬盘机: 至少 1G 剩余空间
- ✓ 网卡: 一块

密文卫士™服务器运行环境:

- ✓ 操作系统: Windows 2000、Windows XP、Windows 2003 服务器及各种升级版本
- ✓ CPU : Intel Pentium 4 系列以上 32 位处理器
- ✓ 内存: 512MB
- ✓ 硬盘机: 至少 1G 剩余空间
- ✓ 网卡: 一块
- ✓ TPM 安全芯片 (可选): 兆日
- ✓ USB 密钥 (可选): 飞天诚信

密文卫士™支持各种应用程序和文件格式, 包括但不限于以下所列:

- ✓ 办公软件: 微软 Office 系列, IBM Lotus 系列, 金山 Office 系列等
- ✓ 设计软件: PhotoShop, AutoCAD, Pro-E, 3DMAX 等
- ✓ 软件开发: Java, C, C++ 等

## 7 联系方式

如您对以上技术白皮书介绍的密文卫士™产品有兴趣，请立即和上海谷巨软件有限公司联系。联系方式如下：

地址：上海市浦东新区春晓路 109 弄 100 号 1 号楼 607 室

电话：(8621) - 55298988

网址：<http://www.gugensoft.com>

访问网址可获得最新的产品信息和联系方式。