北京首信科技有限公司　　地址：中国 北京东直门外将台路 5 号　　(100016)
电话: (8610) 64338899-8343 (8610)87088673 (8610)87088674 传真: (8610) 84561344
网址: http://www.capitek.com.cn　　http://www.capitel.com.cn

首信计算机数据安全防护系统

灵巧的企业/个人数据保护方案

技术白皮书

北京首信科技有限公司

2006 年 3 月

一. 产品功能

首信公司在原有硬件安全产品的基础上，为了更好的为广大用户提供更安全的保障，开发出了首信计算机数据安全防护系统。该软件运行于 Windows 平台之上，提供基于操作系统核心层的安全保护机制，对计算机数据资源进行加密保护。软件基于 IFS 进行开发，在操作系统的文件系统中加上自己的过滤驱动模块，对用户应用程序的读写操作进行拦截，并将数据提交加密模块处理，产品配以国内自主研发的核心密码芯片，提供信息存储与信息传输的数据加解密，在提高算法强度安全性的情况下，还使加解密操作可以快速高效的进行，从而使上层应用程序可以高效的读取或保存数据。用户身份认证钥匙是具有 usb 接口、只有 U 盘大小的微型智能卡，在有身份认证钥匙的情况下，对加密项的操作与普通文件夹或文件一样，加解密过程对用户和应用程序完全透明。在没有身份认证钥钥匙的情况下，加密项被彻底隐藏。

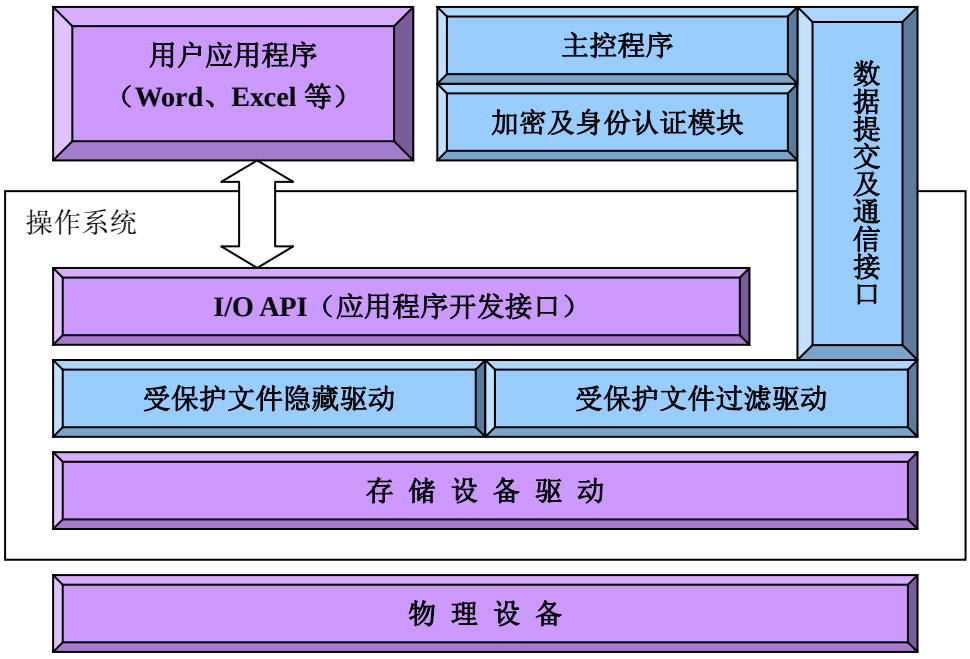
本产品中，加密目录分为小组公用区和私用区，公用区对同一小组的所有成员都是可见的，组员可以在这里共享重要的数据，但对于小组以外的成员则无法访问和解密这些文档。私用区则只有钥匙的持有者可见，任何其他用户无法访问和解密。这使同一台计算机可以由多个人使用，每一个人有自己的加密目录。

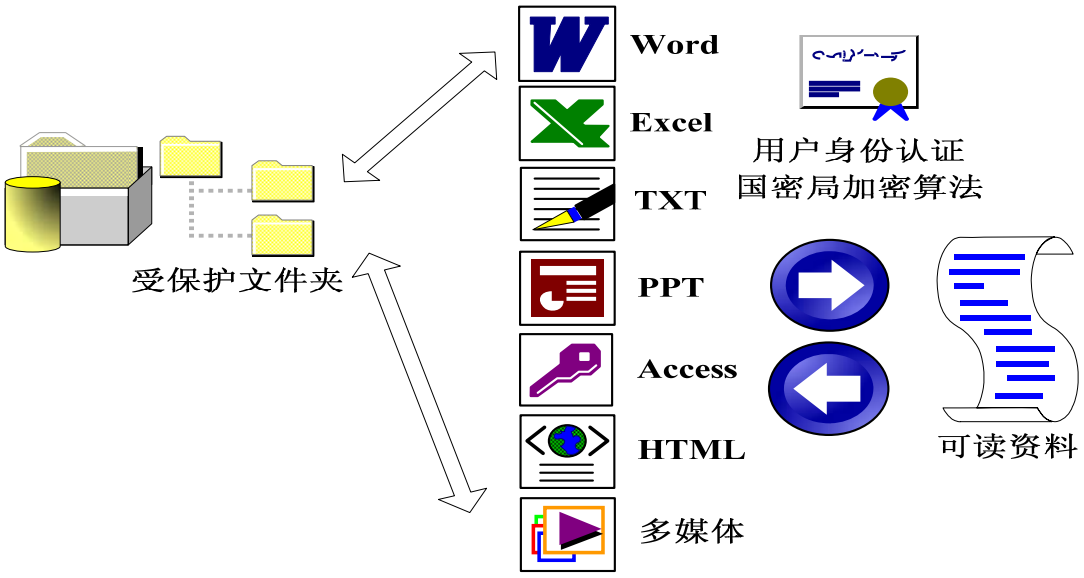
另外，本产品文件系统数据加密保护是建立在操作系统核心层的保护机制，与某些上层加密或采用虚拟硬盘技术的数据保护软件相比具有以下优点:

对应用层数据的加密时实时的、不需要用户参与的过程，在文档的编辑过程中，就已经对数据进行加密；另外，即使将 PC 内的硬盘挂接到其它机器上，也

无法解密受保护的数据。而一些产品只是对文件的头进行加密，文件的实际数据还是以明文的方式保存在硬盘上，降低了安全性。

二. 系统架构图





三．技术指标

- 可对各种文件进行加密，对Windows下所有应用程序的数据进行保护，支持的常见数据有Word文档、Excel文档、Access文档、PowerPoint文档、记事本文档、各种图像语音文件及多媒体数据、VC++工程代码、Delphi工程代码、Visio文档、Acrobat Reader（PDF）以及任何用户自己开发的应用程序所保存的数据等。
- 系统同时具备了数据保护的实时性、简易性和安全性，对于普通硬盘上的某个目录，一旦将其设置为受保护的目录，则无论通过何种软件，例如Windows资源管理器或MS WORD软件，将明文文档拷贝或保存到该目录的同时，本系统就会将数据自动加密；读文档的同时则进行解密，再将明文提交给Windows资源管理器或MS WORD软件。而且受保护的文档资料只在计算机内存中存有明文，系统退出或突然断电，计算机中都不会有明文存在，充分考虑到了用户关键数据的安全性。
- 加密算法采用国密办认证通过的算法（SSFF33或SSF28算法，速度为30-50Mbps）；通用对称密码算法为DES和3DES，密钥长度128位。不对称加密采用RSA加密算法进行加密，RSA密钥长度为1024比特，完全满足当

今计算机水平下的加密强度。

- 提供安全可靠的身份认证机制，未授权用户无法使用本系统，用户私钥保存于用户的UsbKey中，私钥不在计算机存储，减小密钥被盗用的可能性。
- 支持WindowsNT4.0、Windows 2000、Windows XP、Windows 2003操作系统，支持NTFS、FAT16、FAT32 等文件系统。
- 加密的介质不只限于硬盘，对于USB移动硬盘、软盘、可刻录光盘等介质中的数据，同样可以实现加密保护。

四. 产品应用领域

该计算机安全防护产品已经通过公安部的检测，并持有公安部颁发的计算机信息系统安全产品销售许可证，产品的应用领域包括:

- 电子政府的公文流转;
- 国家公安、安全部门内部信息网络安全;
- 重要行业的数据，如财务、税务、保险、金融等的核心数据;
- 核心的科技机密和情报，如科学院、各研究院所、大学等;
- 大型企业的关键数据，如电信、电力等;
- 其他关注自身关键数据安全的用户;