SDC

技术白皮书

CNSINDA深信达

目　录

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第一章. 概述

1.1 常见的机密电子文件泄密途径

近年来，电脑以及互联网应用在中国的普及和发展，已经深入到社会每个角落，政府、经济、军事、社会、文化和人们生活等各方面都越来越依赖于电脑和网络。电子政务、无纸办公、MIS、ERP、OA 等系统也在企事业单位中得到广泛应用。

但在这个发展潮流中，网络信息安全隐患越来越突出，信息泄密事件时有发生。众所周知，电子文档极易复制，容易通过邮件、光盘、U 盘、网络存贮等各种途径传播。企事业的机密文档、研发源代码、图纸等核心技术机密资料，很容易经内部员工的主动泄密流转到外面，甚至落到竞争对手手中，给单位造成极大的经济与声誉损失。

常见的泄密的途径包括：

- 内部人员将机密电子文件通过 U 盘等移动存储设备从电脑中拷出带出；
- 内部人员将自带笔记本电脑接入公司网络，把机密电子文件复制走；
- 内部人员通过互联网将机密电子文件通过电子邮件、QQ、MSN 等发送出去；
- 内部人员将机密电子文件打印、复印后带出公司；
- 内部人员通过将机密电子文件光盘刻录或屏幕截图带出公司；
- 内部人员把含有机密电子文件的电脑或电脑硬盘带出公司；
- 含有机密电子文件的电脑因为丢失，维修等原因落到外部人员手中；
- 外部电脑接入公司网络，访问公司机密资源盗取机密电子文件泄密；
- 内部人员将通过 Internet 网络存储，进行保存；

等。

1.2 防泄密的现状

为解决这些泄密风险问题，许多单位采取拆除光驱软驱、封掉 USB 接口、限制上网等方法来进行限制；或者安装一些监控软件，监控员工的日常工作，使其不敢轻举妄动；或者安装各种网络信息安全防护产品，如防火墙，入侵检测，防病毒产

品等来防范黑客攻击和病毒侵袭。但人们很快发现，限制上网、封闭 USB 接口、拆除光驱软驱、安装监控软件等等做法一方面严重影响工作的便利性，且容易引起员工的抵触情绪，甚至可能会带来法律方面的问题；另一方面无法杜绝有意的内部泄密行为，同时存在因噎废食之嫌。

大量事实也证明这些方法效果不是很好，主要存在的弊端为：

- 影响员工工作情绪甚至造成法律纠纷；
- 增加企业运营成本，降低工作效率；
- 无法防止软件研发人员泄密；
- 精力都花在泄密后的事后追溯上；

1.3 深信达 SDC 机密数据保密系统

深信达公司研发的 SDC（Secret Data Cage）机密数据保密系统，采用世界上先进的第三代透明加密技术---内核级纵深立体沙盒加密技术，是专门为解决源代码、图纸、文档等机密数据泄密问题而设计的一套防泄密系统。

现在的企业都有自己的局域网，一般主要核心机密数据存放于服务器上，一部分存储在员工在自己的电脑上。SDC 的保密设计理念是：

当员工工作的时候，在员工电脑上虚拟出一个对外隔绝的加密的沙盒，该沙盒会主动和服务器进行认证对接，然后形成服务器-客户端沙盒 这样一个涉密的工作空间，员工在沙盒中工作，这样一来：

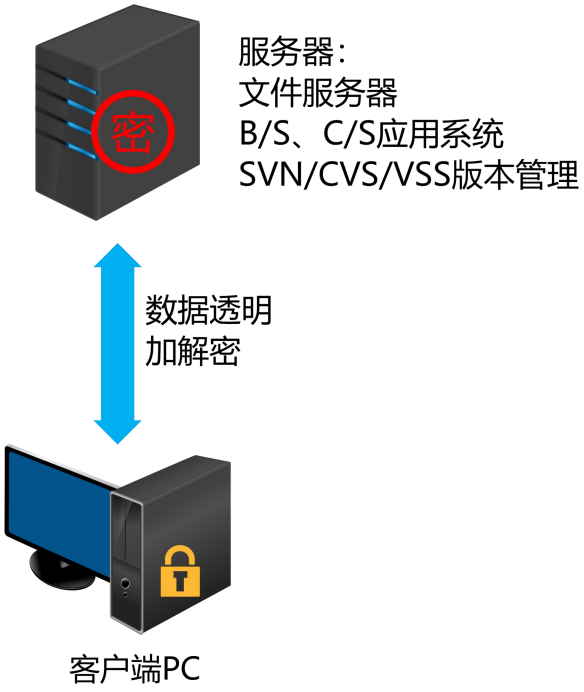
--服务器上的机密数据在使用过程中不落地，或落地即加密；

--员工电脑上的所有开发的成果只能存放到服务器上，或者本地的加密沙盒中；

--沙盘与外界隔离，不会产生泄密。

SDC 加密的沙盒，是个容器，什么都能装；加密自身不关心个体是什么，所以与进程无关，与文件格式无关，与文件大小无关，且不会破坏文件和修改文件内容。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638



SDC 沙盒示意图

客户端在接触涉密资源时，自动启动一个加密的沙盒，沙盒相当于容器，可将涉密软件与文件放入沙盒容器中加密。且该容器是透明的，使用者感觉不到它的存在。

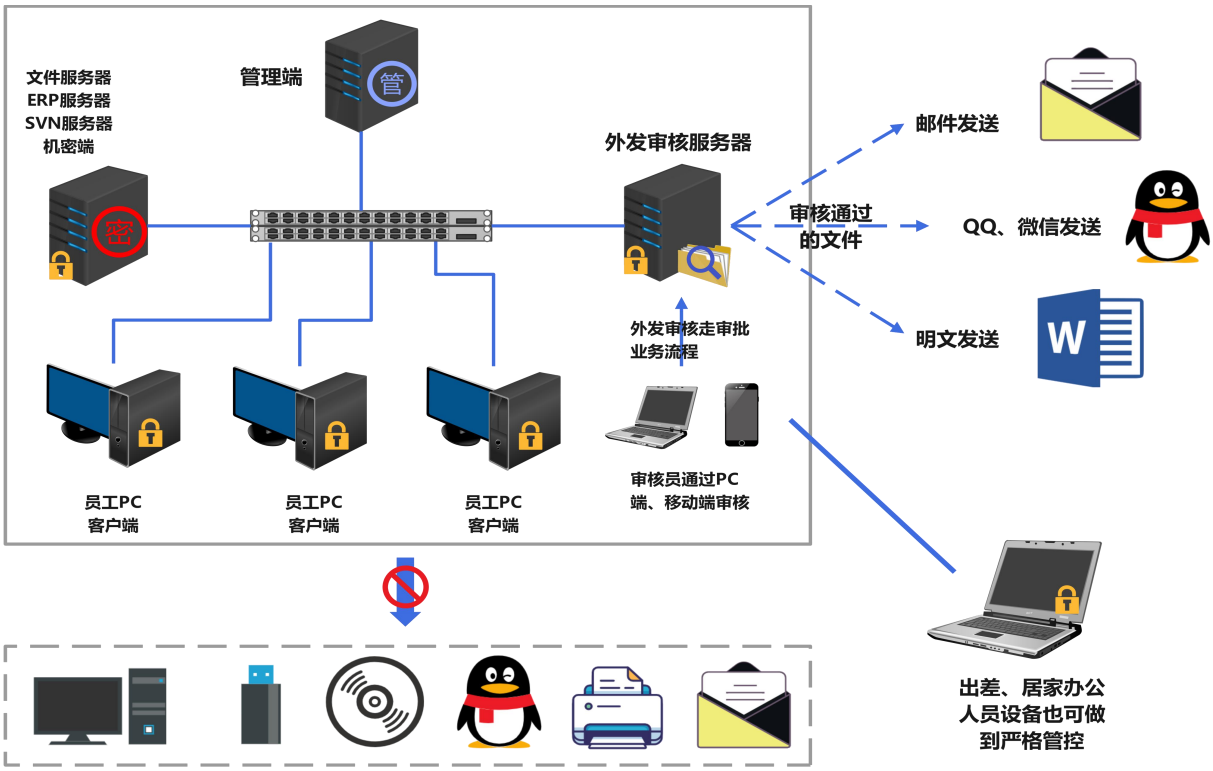
SDC 采用最先进的内核级纵深加密技术（磁盘过滤驱动，文件过滤驱动，网络过滤驱动等）进行开发设计的，充分考虑了可扩展性与易用性。系统本身集成网络验证、文件加密、打印控制、程序控制、上网控制、服务器数据保护等，能有效防止外来 PC、移动存储、光盘刻录、截屏等泄密行为发生。

SDC 沙盒软件主要特点为：

- 全透明加密，不影响员工工作效率与操作习惯；
- 保护所有文件格式，包括所有文档格式、所有源代码格式、图纸格式；
- 安全稳定，不破坏文件；
- 只保密机密数据(源代码，图纸)而不监控不泄密的上网，尊重了员工隐私。
- 外发文档审计，加密，防泄密处理；
- 外发邮件申请，审计业务流。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

使用深信达 SDC 沙盒数据保密系统，可以切实保护企机密数据的安全。



SDC 机密数据防泄密系统示意图

适合的行业包括：

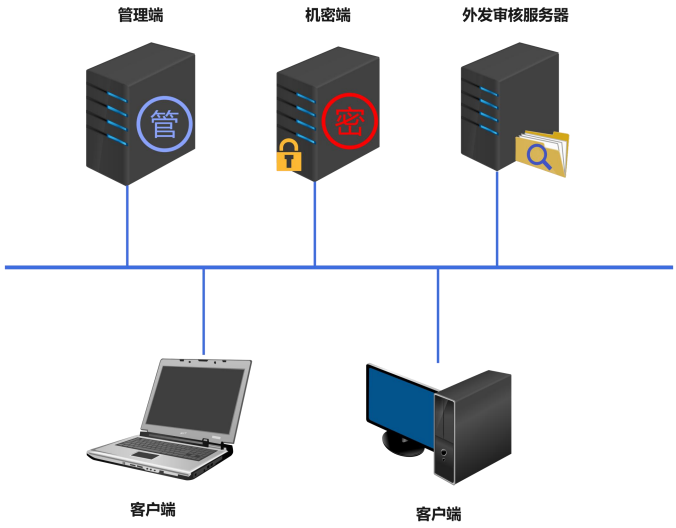
- 软件、通讯、游戏、制造、电力、金融等拥有研发设计部门的企事业单位；
- 拥有自己的研发部门，具有一定的技术优势企业；
- PDM/ERP/文档管理/OA 等应用系统的开发商；
- 所有需要对自己的机密信息保密的企事业单位。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第二章 SDC 系统介绍

2.1 SDC 系统架构

深信达 SDC 机密数据保密系统分管理端、机密端、外发审核服务器、客户端四部分。管理端是整个系统的控制中心，系统中只有一个；机密端是存放机密数据的服务器，一个系统中允许有多台机密服务器；外发审核服务务器是对外发文件进行审核；客户端是安装在员工 PC 上的防泄密策略的执行程序。根据需要，管理端，机密端，外发审核服务器可以安装在同一台电脑上。



SDC 防泄密系统架构图

• 管理端：

对系统中的机密端，客户端进行策略管理，组织管理；客户端日志收集；

企业加密密钥管理；客户端卸载管理；机密服务器，外发审核服务器认证管理；

• 机密端：

保存机密数据的服务器，对来访用户进行严格审计，加密认证。可以是文件共享服务器，ERP，PDM 服务器，文档管理系统。或者是 VSS，CVS，SVN 文件版本管理服务器。非客户端无法访问机密端。

• 外发审核服务器：

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

对外发的邮件，文件进行审核，对于涉密文件可自动加密。外发结果记录。

• 客户端：

透明加密解密，真正和格式无关的加密；

可信网络认证，机密资源认证；

打印控制，禁止打印，指定打印机打印，打印水印设置，打印内容日志回传；

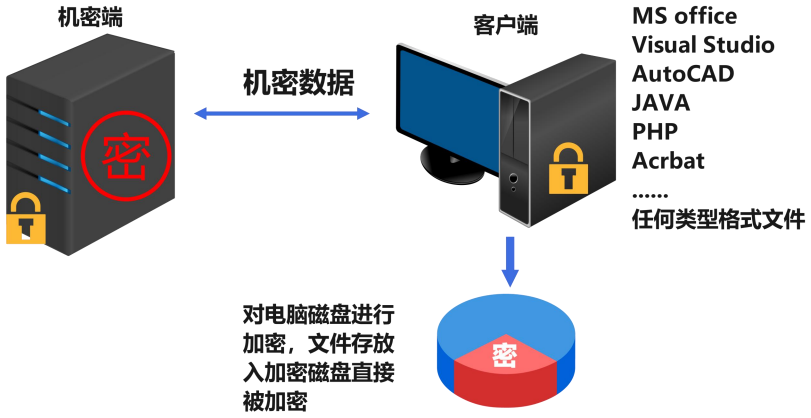
离线控制；

文档外发等。

2.2 SDC 系统功能

2.2.1 客户端涉密文件自动加密

SDC 采用内核级纵深加密技术，对所有涉密文件都进行透明加密处理，真正做到不区分文件格式，不区分软件类型。Office 系列，PDF 等常用文档、AutoCAD 等制图类软件、Microsoft Visual Studio，Eclipse 等软件开发工具，一律自动加密，包括源代码、源图纸、且编译中间文件都可自动加密，不影响本地编译，不影响性能。对于需要提交服务器进行编译的也能轻松适用。



客户端透明加密解密示意图

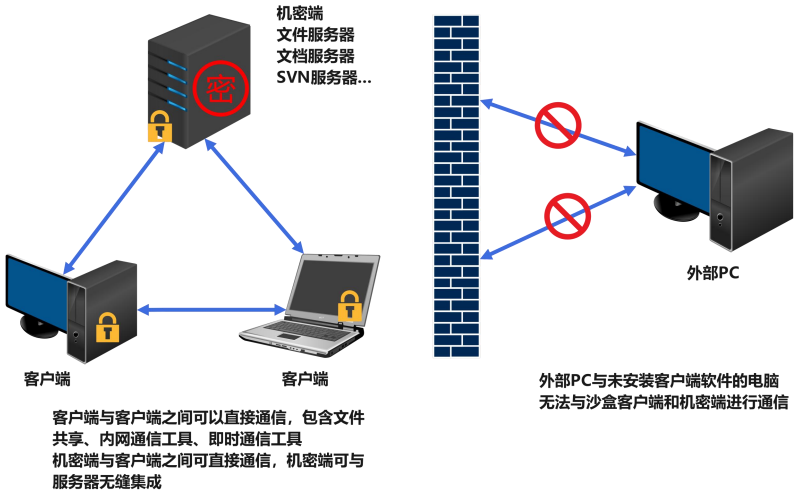
加密的数据不能通过移动存储(如 U 盘)、光盘、网络、邮件、文件另存、内容复制、截屏录屏等泄密途径泄密，即使硬盘丢失都不会造成泄密。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

2.2.2 涉密网络内部通畅，隔离外来 PC

机密服务器和进入涉密沙盒模式下的客户端，形成一个涉密地，安全的网络空间，在涉密网络内部，信息传输是透明的，流畅的。传输方式包括文件共享，C/S（客户端和管理端）B/S（浏览器/服务器）构架的应用，和布置 SDC 前比，没什么区别。涉密网络内，飞秋，IPMSG 等局域网内部聊天工具照常可以使用。

但是，没有进入沙盒模式的客户端，或者外来 PC 接入网络，由于无法通过认证，立即被隔离，成为孤岛，不能访问机密服务器，不能访问其他涉密客户端，局域网通讯工具也无法和涉密的客户端进行对话。



外来 PC 被隔离示意图

2.2.3 非涉密受限白名单

在策略允许前提下，客户端在涉密工作的同时，在保证不会泄密的前提下，允许安某些程序进行非涉密上网。在策略允许的前提下，上网可以进行的行为包括：

--浏览互联网进行必要的资料查询；

--QQ、MSN、飞信的使用；

--非涉密邮件的使用，如 WebMail 或者 OutLook/Foxmail 的非涉密收发邮件；

上述非涉密上网过程中，涉密的文件内容无法通过复制粘贴，文件上传，鼠标

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

拖拽，屏幕截取等方式被非涉密程序使用。

举例说明：用户正在编辑涉密的一个 AutoCAD 图纸，此时可以通过 IE 上互联网查找资料，通过 QQ 和业内人士讨论，但是涉密 AutoCAD 中的图片、文字、文件等都无法通过 IE 和 QQ 发送出去。QQ 的截屏等任何截屏软件，录屏软件都无法截去涉密 AutoCAD 画面。

当然，如果觉得该员工上网会影响工作效率的话，通过策略设定，可以把外网完全断开。安全隔离上网功能，极大地提高了员工查找资料的便利性。

安全隔离非涉密受限上网示意图

2.2.4 涉密文件外发

当业务需要把涉密文件拿出涉密环境时，必须走 SDC 的外发审核流程才能脱密。SDC 系统提供了明文外发、加密外发和邮件外发三种方式。下面简单做下介绍。

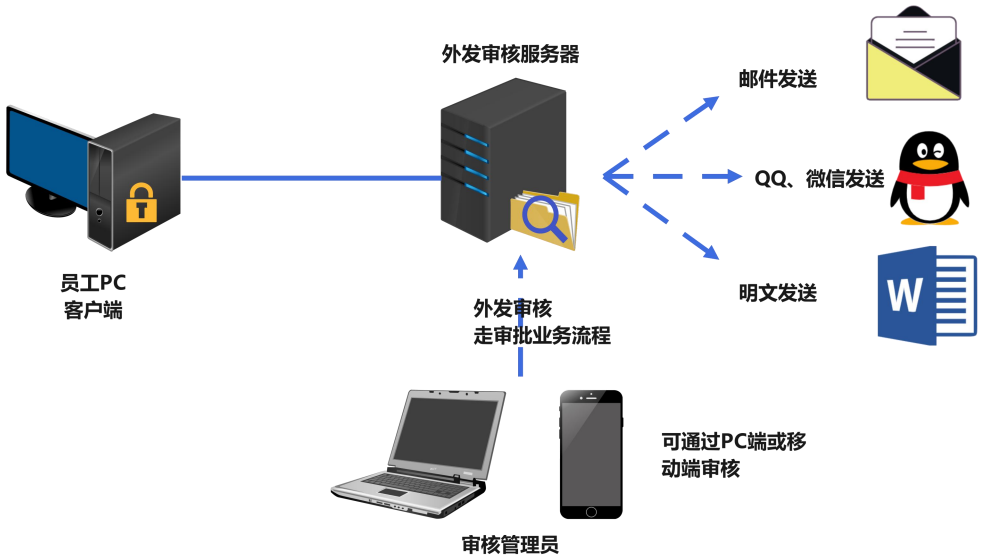
明文外发：

当业务需要把涉密的文件以明文的形式拿出涉密环境户时，通过明文外发审批流程，经审批后的涉密文件，可通过邮件、QQ、U 盘等方式与客户交互。

审批支持多级审批，如组员->组长->经理->副总的多级审批模式

加密外发：

当业务需要，需要把涉密的文件发给客户，同时还希望控制该文件的使用范围，则可以使用加密外发业务流程。加密外发的文件发到客户处，被客户使用时，需要密码验证，并且可以设定使用次数，使用时间，能在哪台 PC 上打开等，该文档是否允许修改，复制，打印等，也可以设定。

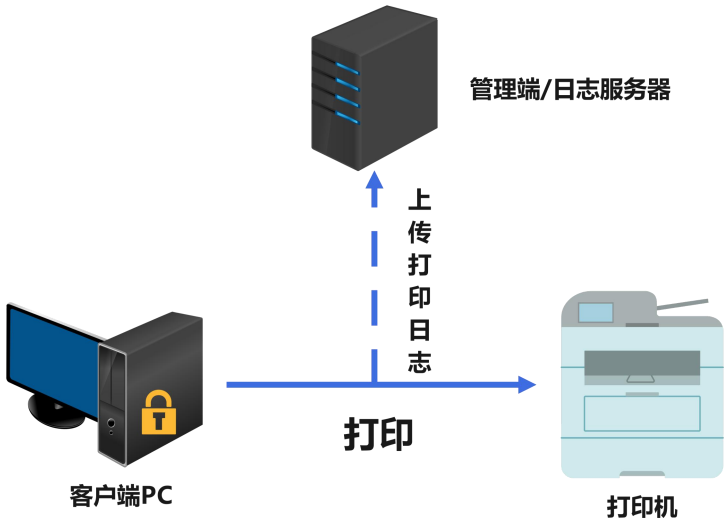


以上二种涉密文件外发审核流程，都是申请-〉审核-〉外发，并且日后有日志可以审核。

总之，涉密数据根据需求需要离开机密环境时，需要走审核流程。当然，企业管理者如果觉得流程麻烦，可以只看发送日志，简化审核流程。

2.2.5 打印内容日志

系统默认策略是不允许打印，当需要打印时，可以指定打印机进行打印，但是打印的首页面内容将被记录并传会服务器，以备日后审计。



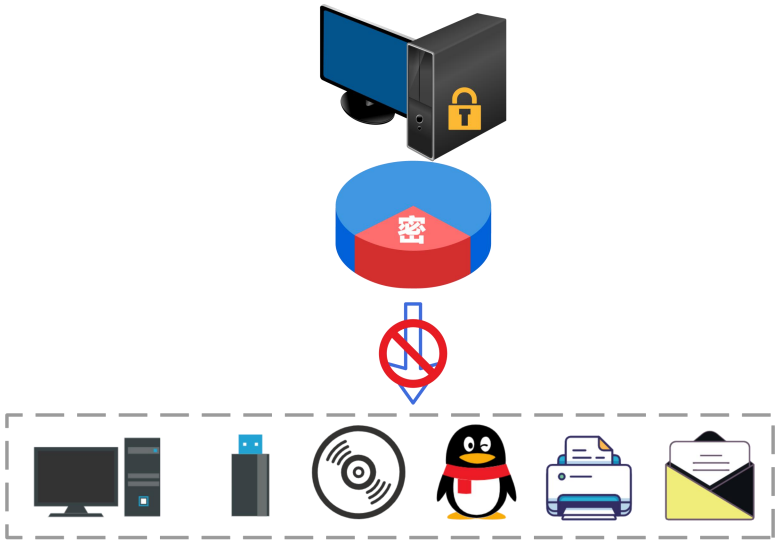
苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

2.2.6 离线客户端

对于需要出差或者带回家的笔记本电脑，可以设定为离线客户端，在规定的时间内，可以继续使用本地的涉密数据。离线使用时，所有涉密文件都还处于加密状态，工作人员可以继续正常作业。但如果超过设定的期限，所有涉秘密数据都自动关闭，整个系统将处与保护状态，直到返回公司接入网络连接服务器后，才能正常工作。

如果万一笔记本电脑丢失或被盗，由于对方没有解密口令，所有涉密数据都处于保护状态，重新安装系统，硬盘插拔等，都无法获取电脑中的机密数据。

当客户端策略过期而又无法回公司时，系统管理员可以对其进行策略延长。



2.2.7 涉密文件加密导出导入

客户端可以把某文件加密导出，然后发给另一个客户端，再解密导入，整个过程不泄密。

应用场景一：

2 个人出差到外地，这 2 个客户端都是离线的，通过这个加密导入导出功能，能实现这 2 个客户端之间涉密数据交换。

应用场景二：

一个人出差外地，现场根据客户需求开发调试，调试好了的东西，需要提交给

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

客户，如果直接让解密，无法控制该人把其他涉密文件拷贝出去。所以这个时候，出差人员把要给客户的文件加密导出，然后发回公司，公司审核后，解密，走审核流程，然后把明文发给客户，形成有效控制。

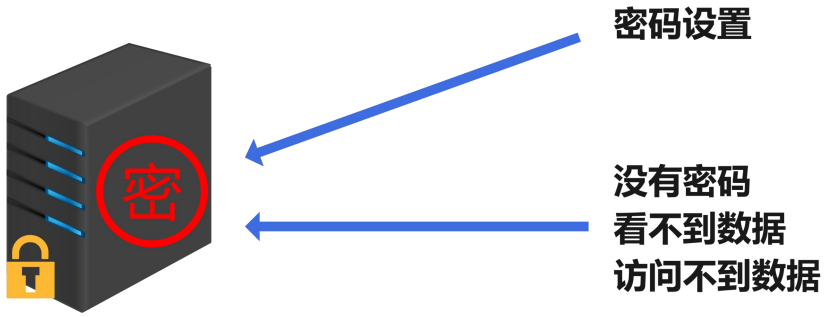
应用场景三：

2 个独立的分支公司(跨互联网)，其中一个公司要把一个涉密文件发给另一个分公司，然后导入。

客户端涉密文件交互

2.2.8 服务器端数据保护

对于存储在机密服务器上的数据，如 SVN 的存储目录，也可以进行保护，防止有人非法直接登录服务器，把数据从服务器上拷贝走。



服务器端文件保护

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第三章 SDC 系统特点

3.1 沙盒加密是个容器，和软件类型无关，文件类型无关

SDC 采用第三代透明加密技术--内核级纵深加密技术，加密沙盒是个容器，和应用软件类型，以及文件格式无关，不破坏文件自身内容。并且抗破解能力强，完全能满足研发机构的源代码保密，和图纸保密需求。

目前为止，SDC 已经实施的客户中，开发环境包括：

-Microsoft Visual Studio 平台的 MFC/ATL C++，C#.NET, VB 等的编写代码，编译调试。

-Java，JSP 等开发工具 Eclipse，JBuilder，Websphere 等环境下的代码编写，开发调试。

-各种小工具进行 PHP，ASP，CGI，C 等开发，调试。

-嵌入式开发工具：WindRiver, Tornado, AVCMonitor,

Source Insight/ComAssistant

等

图纸设计研发类支持：

-支持 AutoCAD，SolidWorks，UG 等所有图纸设计工具的开发，调试，不区分文件类型，软件类型。

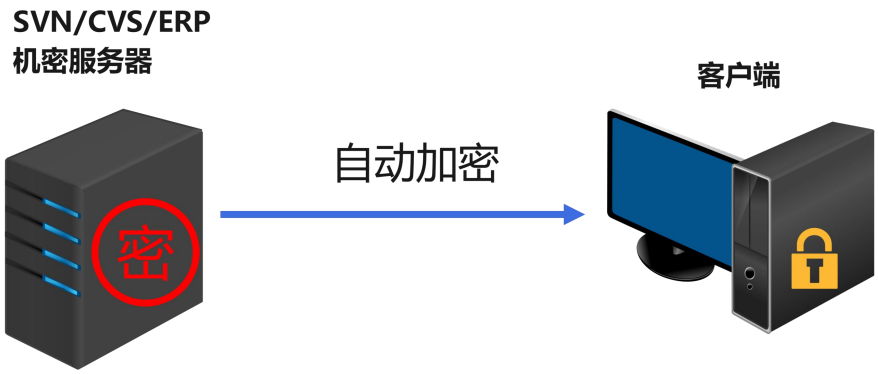
3.2 能和文件共享服务器，应用服务器无缝结合

深信达 SDC 机密数据防泄密系统能和现有的文件共享服务器，文档服务器，ERP 服务器，PDM 服务器，OA 等 B/S 架构系统，C/S 架构系统，VSS,CVS,SVN 版本服务器等无缝结合。原有系统如是 Windows 平台，则不需要任何修改。服务器端支持 Windows 平台。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

3.3 安全稳定，不破坏数据

涉密文件在服务器上是明文，到达客户端自动加密。服务器上的数据要备份的，服务器上存放的是明文数据，从根本上保证了数据的连续，稳定性，减少了对加密软件的依赖性。另外，由于采用的是第三代透明加密技术，所以不管文件多么大，多么复杂，不会因为 SDC 系统造成文件破坏破损。

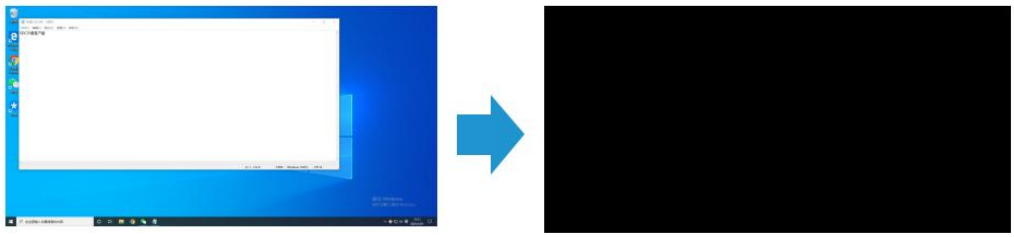


3.4 使用便利，操作机密数据的同时，可以上网

SDC 系统采用的是立体型全方位防泄密方案，一旦进入涉密状态，不改变原来的操作习惯。在策略许可前提下，允许通过非涉密受限上网，实现可以上网查阅资料而不泄密，收发邮件而不泄密，QQ 聊天而不泄密。

3.5 超强的反截屏

SDC 系统对涉密文档的屏幕也做了保护，防止被截屏。截屏键，截屏软件，录屏软件都无法截取涉密文档的屏幕图



反截屏效果说明图

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第四章 关于深信达

5.1 深信达介绍

深信达信息技术有限公司是专注于信息安全领域研发的高科技企业，在信息防泄密，主动防御领域等领域，处于国际领先水平。公司拥有一支由全国最顶尖的安全专家组成的开发团队，在数据保密，主动防御等方面，取得了一系列拥有独立知识产权的研究成果。我们基于多年的信息安全领域的研究与开发经验，为国内政府、电信、金融、制造、能源、教育等行业客户提供信息安全解决方案以及风险评估，咨询等服务。

公司目前的主要产品为：

SDC 机密数据保密系统(Secret Data Cage 简称 SDC)：该系统采用第三代透明加密技术--内核级纵深防御架构，技术先进，保密到位，在源代码，图纸，文档的保密市场中，优势明显，先后成功为国内数家大型企业和国家涉密机关实施了数据保密方案。

CBS 赛博锁：该系统对工业控制系统、物联网设备等微系统、嵌入式系统进行防克隆、防破解、防数据泄露和防病毒保护。

MCK 云私钥主机加固系统：解决服务器的数据安全风险，核心是通过安全容器中间件技术，建立内核级纵深立体防护体系，保障服务器的安全稳定运行。系统设计理念颠覆了传统的系统管理员权限最大的理念，即使是木马病毒或黑客掌握了系统的管理员权限，仍然能有效保持服务器的稳定运行，确保存储的业务数据免受篡改和偷窥风险。

SDC 安全上网解决方案：在企业内网中部署一个沙盒安全上网主机服务器，当员工需要访问外网时，员工终端安装一个沙盒，在沙盒内访问外网。沙盒内所有行为都受管控，终端的本地数据与沙盒隔离，沙盒在访问外网时本地数据不会泄漏，可以有效预防间谍软件对外发消息（盗版问题），也能有效预防病毒入侵。

U 盘沙盒：深信达 U 盘沙盒移动安全办公环境系统(沙盒防泄密系统)由管理端，

客户端二部分组成。管理端是整个系统的控制中心，可以编辑定制修改客户端策略；客户端是内嵌在 U 盘里的安全办公环境。

服务器机密数据防泄密保护组件(DLP)：该插件适合作为 CRM、OA、ERP、PDM、文档管理系统等的防泄密组件，能有效防止涉密数据扩散。

企业 U 盘存储管理系统：企业内的 U 盘只能在企业内部使用，拿出单位立即为密文。外部 U 盘在企业内是只读的或者禁止使用的。

深信达文件保险箱：提供用来防止个人信息泄密的的系统，该系统免费，目前拥有数万用户。

有偿技术支持：

1）文件透明加密驱动库以及源代码。本技术虽然属于第二代文件透明加密技术(IFS 或 Minifilter)，但运行稳定，目前国内数家透明加密厂家正在使用中。

2）反截屏技术模块库，反截屏技术国内业界公认第一，目前也正在为数家安全企业做技术支持。

5.2 联系我们

商务联系电话： 0512 -68186638

技术支持 Mail: support@shenxinda.com

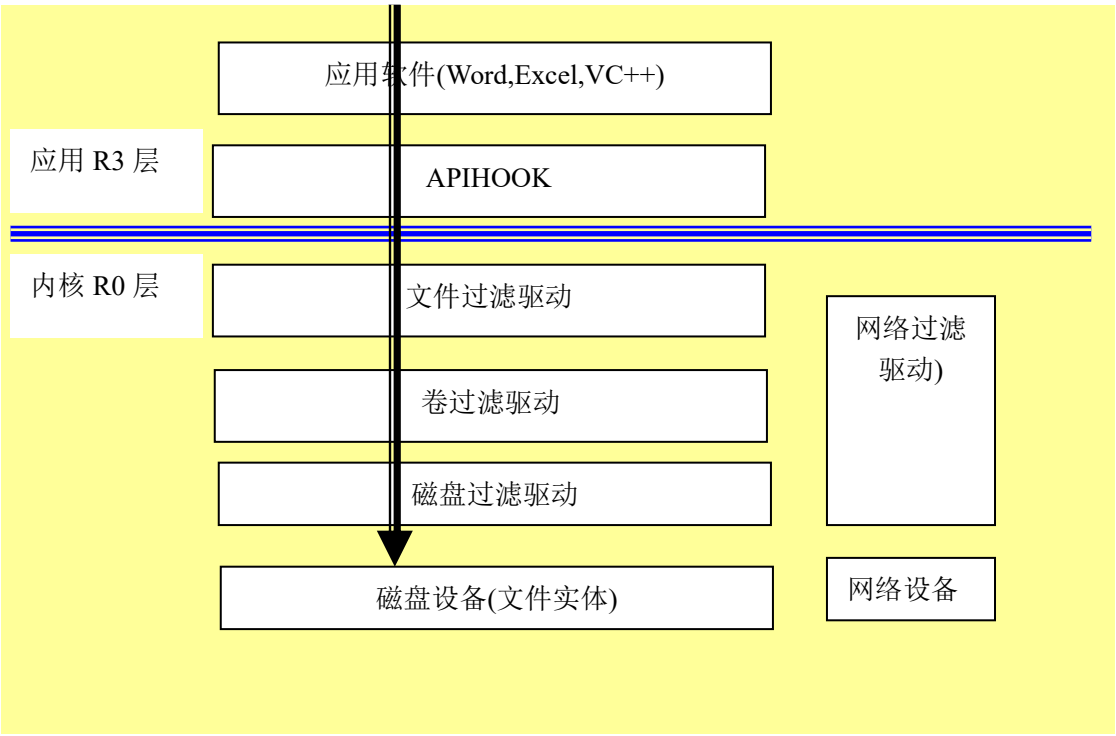
商务支持 Mail: sales@shenxinda.com

地址：苏州高新区竹园路 209 号创业园 1 号楼 3F

附录一：透明加密技术发展

透明加密技术是近年来针对企业数据保密需求应运而生的一种数据加密技术。所谓透明，是指对使用者来说是透明的，感觉不到加密存在，当使用者在打开或编辑指定文件时，系统将自动对加密的数据进行解密，让使用者看到的是明文。保存数据的时候，系统自动对数据进行加密，保存的是密文。而没有权限的人，无法读取保密数据，从而达到数据保密的效果。

自 WindowsNT 问世以来，微软提出的分层的概念，使透明加密有了实现的可能。自上而下，应用软件，应用层 APIhook(俗称钩子), 文件过滤驱动，卷过滤驱动，磁盘过滤驱动，另外还有网络过滤驱动，各种设备过滤驱动。其中应用软件和应用层 apihook 在应用层(R3), 从文件过滤驱动开始，属于内核层(R0)。



数据透明加密技术，目前为止，发展了 3 代，分别为：

第一代：APIHOOK 应用层透明加密技术；

第二代：文件过滤驱动层（内核）加密技术；

第三代：内核级纵深加密技术；

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第一代：APIHOOK 应用层透明加密技术

应用层透明加密技术俗称钩子透明加密技术。这种技术起源于 win98 时代，后来随着 windows2000 而流行起来。就是将上述两种技术（应用层 API 和 Hook）组合而成的。通过 windows 的钩子技术，监控应用程序对文件的打开和保存，当打开文件时，先将密文转换后再让程序读入内存，保证程序读到的是明文，而在保存时，又将内存中的明文加密后再写入到磁盘中。应用层 APIHOOK 加密技术，特点是实现简单，缺点是可靠性差，速度超级慢，因为需要临时文件，也容易破解。但由于直接对文件加密直观感觉非常好，对于当初空白的市场来讲，这一旗号确实打动了不少企业。

第二代：文件过滤驱动加密技术

驱动加密技术是基于 windows 的文件系统（过滤）驱动技术，起源于 WindowsNT 发布之后，其工作在 windows 的内核层，处于应用层 APIHook 的下面，卷过滤和磁盘过滤的上面。设计思想是建立当应用程序(进程)和文件格式(后缀名)进行关联，当用户操作某种后缀文件时对该文件进行加密解密操作，从而达到加密的效果。

内核层文件过滤驱动技术，分 IFS 和 Minifilter2 类。IFS 出现较早，Minfilter 出现在 xp 以后。两者的区别可以理解为 VC++和 MFC 的区别，IFS 很多事情需要自己处理，而 Minifilter 是微软提供了很多成熟库，直接用。由于 windows 文件保存的时候，存在缓存，并不是立即写入文件，所以根据是否处理了双缓 bug，后来做了些细分，但本质还是一样，都是问题的修正版本而已。但由于工作在受 windows 保护的内核层，运行速度比 APIHOOK 加密速度快，解决了很多问题和风险。

文件过滤驱动技术实现相对简单，但稳定性一直不太理想。

第三代：内核级纵深沙盒加密技术

之所以叫内核级纵深沙盒加密技术，主要原因是使用了磁盘过滤驱动技术，卷过滤驱动技术，文件过滤驱动技术，网络过滤驱动(NDIS/TDI)技术等一系列内

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

核级驱动技术，从上到下，纵深防御加密。该技术也起源于 WindowsNT 之后，但由于技术复杂，开发要求高，公开资料少，而发展较慢。但随着微软公布了部分 Windows 源代码之后，此技术开始逐渐成熟。内核级沙盒加密，是当使用者操作涉密数据的时候，对其存储过程进行控制，对其结果进行加密保存，每个模块只做自己最擅长的那块，所以非常稳定。加密的沙盒是个容器，把涉密软件，文件扔到容器中加密。而这个容器是透明的，使用者感觉不到它的存在。，

第三代透明加密技术的特点是，涉密数据使用前，先初始化涉密沙盒，沙盒加密一旦成功，之后所有的数据都是数据实体，不针对文件个体，所以无数据破损等问题。特点是速度快，稳定。

第一代，第二代本质都是采用的针对单个文件实体进行加密，如 a.txt 内容为 1234，加密后变成@#$%% +标记。@#$%%是把原文 1234 进行加密之后的密文。而标记的用途是用来区分一个 a.txt 文件是否是已经被加密。当系统遇到一个文件的时候，首先判断这个标记是否存在，如果存在，表明是被系统加密过的，则走解密读取流程，如果不是加密的，就无需解密，直接显示给使用者，只是当保存的时候，再进行加密，使其成文密文+标记。

这就带来一个巨大的风险：如果是一个较大文件，加密过程中发生异常，标记没加上，那么下次读这个文件的时候，因为没有读到表记，而采用原文读取，然后再加密，那么这个文件就彻底毁坏了。这个现象在第一代 APIHOOK 透明加密技术的产品中特别明显，在第二代文件过滤驱动产品中，因为速度变快了，使文件破损发生概率减低了很多，但并没有本质解决这个问题。

另外，由于是进程和文件后缀名进行关联，也造成了一个缺陷：很多编程类软件，复杂制图软件的编译，晒图等操作，都是很多进程同时操作某个文件，这个时候进行进程和文件关联显然太牵强了，因为进程太多了。即使进行关联，多个进程交替访问文件，加密解密混在一起，极容易造成异常。所以才会出现 VC 等环境下如不能编译，调试等。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

其他方面，版本管理无法对比，服务器上存放的是密文（服务器存密文，是个极大的风险，目前没有哪家大企业敢这么做，毕竟太依赖加密软件，持续性没有了），大文件速度慢等，一系列问题，无法解决。

而第三代内核纵深加密技术是在前者 2 个基础之上发展而来的，每个过滤层都只做自己最擅长的事情，所以特别稳定，速度快，性能可靠，不存在第一代和第二代的问题。由于内核级纵深透明加密技术要求高，涉及技术领域广，极其复杂，开发周期长，所以国内的能做开发的厂商不多。目前，深信达公司推出的 SDC 机密数据保密系统，给人一眼前一亮的感觉，其产品是第三代透明加密保密技术的典型产品，其产品主要特点是：

（1）采用了磁盘过滤，卷过滤，文件过滤，网络过滤等一系列纵深内核加密技术，采用沙盒加密，和文件类型和软件无关，沙盒是个容器。

（2）在操作涉密数据的同时，不影响上外网，QQ,MSN 等。

（3）保密彻底，包括网络上传，邮件发送，另存，复制粘贴，屏幕截取等，特别是屏幕保密，做得非常炫。

（4）服务上存放的是明文，客户端存放的是密文，文件上传服务器自动解密，到达客户端自动加密。服务器上明文，减少了业务连续性对加密软件的依赖。

（5）不但可以针对普通文档图纸数据进行保密需求，同时更是研发性质的软件公司(游戏，通讯，嵌入式，各种 BS/CS 应用系统)源代码保密首选。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

第一代，第二代，第三代透明加密技术对比：

代次	第一代	第二代	第三代
名称：	APIHOOK 应用层透明加密技术。	文件过滤驱动层（内核）加密技术。	内核级纵深加密技术。
设计思路	应用层透明加密技术俗称钩子透明加密技术。这种技术就是将上述两种技术（应用层 API 和 Hook）组合而成的。通过 windows 的钩子技术，监控应用程序对文件的打开和保存，当打开文件时，先将密文转换后再让程序读入内存，保证程序读到的是明文，而在保存时，又将内存中的明文加密后再写入到磁盘中。	驱动加密技术是基于 windows 的文件系统（过滤）驱动（IFS）技术，工作在 windows 的内核层。我们在安装计算机硬件时，经常要安装其驱动，如打印机、U 盘的驱动。文件系统驱动就是把文件作为一种设备来处理的一种虚拟驱动。当应用程序对某种后缀文件进行操作时，文件驱动会监控到程序的操作，并改变其操作方式，从而达到加密的效果。	客户端在涉密的场合，启动一个加密的沙盒，沙盒是个容器，把涉密软件，文件扔到容器中加密。而这个容器是透明的，使用者感觉不到它的存在。采用最先进的磁盘过滤驱动，文件过滤驱动，网络过滤驱动等内核级纵深加密防泄密技术，每个模块只做自己最擅长的那块，所以非常稳定。
优点	直接对文件加密直观感觉非常好，对于当时空白的市场来讲，这一旗号确实打动了不少企业。	由于工作在受 windows 保护的内核层，运行速度较快。	单个文件，复杂文件，大文件，源代码开发复杂环境等，都特别适合。
缺陷	应用层透明加密（钩子透明加密）技术与应用程序密切相关，它是通过监控应用程序的启动而启动的。一旦应用程序名更	(1) 复杂软件经常会很多进程同时操作某个文件，如果这个时候，一个进程加密，另一个进程不加密，交替访问文	无此类不稳定问题。

	改，则无法挂钩。同时，由于不同应用程序在读写文件时所用的方式方法不尽相同，同一个软件不同的版本在处理数据时也有变化，钩子透明加密必须针对每种应用程序、甚至每个版本进行开发。	件，极容易造成异常。如不能编译，调试等。 (2) 涉及到 windows 底层的诸多处理，开发难度很大。如果处理不好与其它驱动的冲突，应用程序白名单等问题。	
进程关联	和进程绑定，容易被冒充。另外很多软件进程非常多，如 VC++的 MFC/ATL 的界面和 socket 编程，编译的时候，关联进程非常多，无法对应。		和进程无关，无冒充问题，因为都在容器中。
大文件破损	200M 以上文件，极容易破损。		无文件破损问题。
源代码保密	无法针对源代码开发人员保密，具体表现在，影响调试，影响版本管理，版本工具对比乱码等问题。 对于一般员工的操作有效，但无法针对源代码开发人员保密。		适合源代码开发。有大型成功案例。
复杂图纸软件保密	复杂图纸一般都是进程多，文件大，此产品问题太多了。		复杂图纸适合 DLP+。
软件版本升级	当软件升级如 VS2005->2008,AutoCAD 升级等，都需要重新设置。		不需要设置，因为和进程无关。
破解难度	非常容易破解，网上工具太多了。		很难破解，即使是懂电脑的程序员。

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638

部分成功客户：

苏州深信达网络科技有限公司 www.cnsinda.com
Email:sales@shenxinda.com Tel: 0512-68186638
CNSINDA 深信达