祺安文档外发管理
技术白皮书

北京弘信安科技有限公司

目录

1．产品简介

1．1 概述

祺安文档外发管理系统针对网络中重要的电子文档需要外发给协同单位使用，而又需要保护自身的文档内容不随意扩散而设计的安全产品。可对外发文档进行加密保护和权限控制，使用方便，不改变文档格式，不影响使用者操作。控制的权限包括：是否只读使用、是否允许打印、控制从加密文档向非加密文档粘贴内容、控制另存、截屏等操作。系统帮助用户确保外发电子文档信息的完整性和保密性，有效控制了企业内部重要电子文档的信息泄露。

1．2 需求背景

何人、何时需要文档外发：出差人员，有合作关系的伙伴，需要发送原始文件给对方（例如要和对方进行协同完成工作），又不希望对方能够长期使用或泄密；例如以下场景：

设计制造企业有图纸需要发送给协作厂商开模或打印，需要使用原始的设计图纸；

律师有法律文件需要第三方阅读；

投资商有项目方案需要多方讨论并提供修改建议。

1．3 系统设计理念

能让外发文档在合作单位用户便于使用和修改，又能保证外发文

档的内容不被随意扩散是文档外发管理系统的设计遵旨。文档外发管理的设计理念是：通过动态加解密技术在在外发客户的计算机上实时构建一个透明加解密环境，做到外发文档落地即密文存放，打开实现透明解密。同时根据外发的权限有效控制文档使用时间、只读、打印、另存、截屏、复制粘贴等操作。

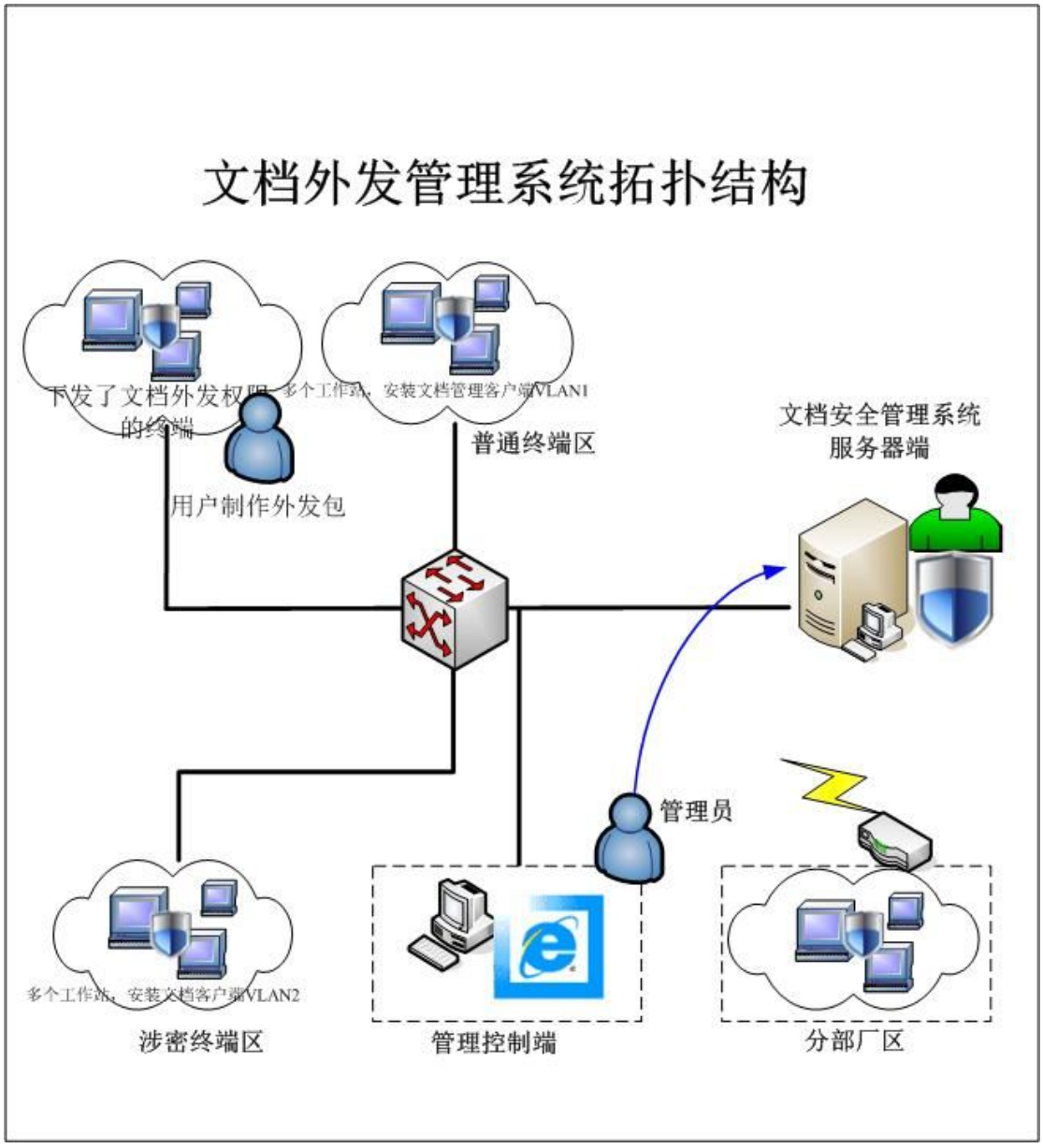
1．4 系统适用范围

文档外发管理系统采用内核级加密技术及权限控制技术实现对文档有效防护。主要实现对涉密行业或各大、中型企业机密信息的防护，该系统使用范围广泛，如政府、军工、各设计院、研究所及各大中型企事业单位，通过对核心机密信息的防护来提高企业竞争力。

2．系统构成及功能

系统整体采用业界主流的 C/S 和 B/S 结合的开发模式。系统由如下部件组成：外发包制作客户端、服务器、控制台、外发环境包。管理员通过 B/S 浏览器方式登陆控制台，定制、外发策略和系统设置等。客户端服务器之间通过 C/S 方式交互，更新外发策略等设置，并据此进行加解密核心工作。

系统拓扑结构如下：



系统主要功能如下：

文档外发可以解决单位内部的重要文档发给合作伙伴后，文档内容不被泄露。通过在单位内部制作加密文档外发包，发送给合作伙伴，合作伙伴运行指定的阅读器，可浏览修改指定外发包中的加密文档。系统的外发控制文件采用加密方式带出、在外发环境中也遵循落地密文原则，支持所有格式的数据文件的带出及带回。

功能描述如下：

外发文件透明使用，不改变用户使用习惯，使用原有关联程序打开相应文档。

外发环境验证，需要密码、U 盘，机器信息等验证方式，才能访问外发包中的加密文档。

文档访问控制，控制文档外发权限相关使用权限避免内容泄露：打印、使用分钟数、使用次数、只读、禁止密向非密粘贴、禁止截屏、禁止另存等。

外发文件修改后带回，修改后的外发文件，能自动保存在原始外发包中，可顺利带回。

3．系统特点

3．1 外发各种软件适应性强

系统的外发控制文件采用加密方式带出、在外发环境中也遵循落地密文原则，支持所有格式的数据文件的带出及带回。产品目前支持 OFFICE、WPS、VC 、各种 CAD、UG、SOLIDWORK、PROE、ADOBE READER 等上百种已有软件的外发。

3．2 细粒度的文档权限管理

外发文档权限控制准确，不用担心复制、另存、截屏等方式的明文泄露。外发文件无法自由复制到客户环境中，安全性高。

3. 3 外发控制安全可靠

支持硬件（任意 USB 存储设备、机器信息）与外发文件的安全绑定

传输和访问过程中，外发文件始终保持加密状态，杜绝各种黑客软件的窃取和拦截

文件被安全外发后，只有指定的外协厂商能够修改或以只读权限查看。其他任何用户和厂商在获取外发文件后将无法应用和解密，有效杜绝了外发文件的二次扩散和泄密。

3. 4 操作简便易用的管理平台

基于 B/S 的管理平台，管理员在任何一个计算机上都能通过 IE 浏览器登录管理控制台进行管理，不用单独安装管理控制台端。

外发包制作、使用、带回简单快捷。

4．产品技术优势

4. 1 绝对领先的加密内核，具有相对独立的文件系统

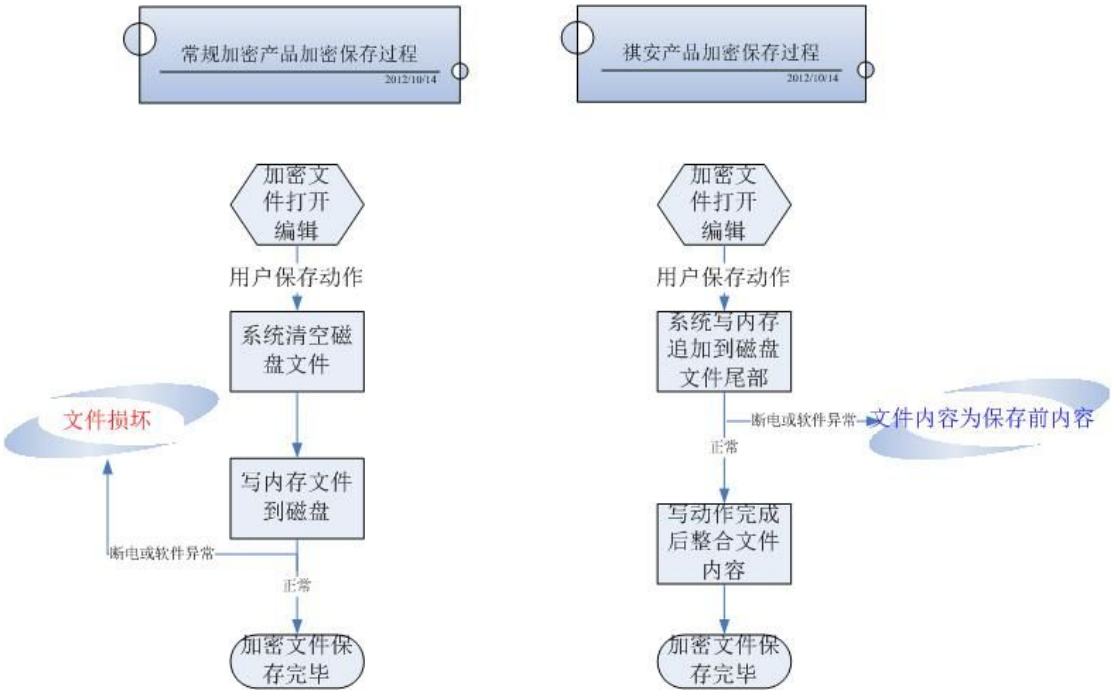
系统底层设计是真正的 LAYER FSD 架构，具有特殊的相对独立的文件系统独立的缓存控制机制，体现在加解密的高稳定性和可靠性上。文件数据保存按位校验，不再依赖于 WINDOWS 自身的文件系统，所以兼容所有杀软。不依赖于 WINDOWS 缓存管理，不用强行刷缓存，所以告别文件的损坏。

较早前的加解密产品的最高境界是单层双缓存驱动加密，使用WINDOW 自身文件系统，当文件写入磁盘时在接口处做数据过滤进行加密处理。没有自己的缓存控制机制，为了解决单缓存的漏洞和杀软干扰的不稳定性，在缓存中强行划分明文和密文缓存区，但又出现了另一个严重的问题，因为缓存是WINDOWS 自带的，研发根本无法解决对缓存进行全面的控制，只能强行划分。所以明文和密文数据交互时需要强行刷缓存，刷缓存造成了数据的损坏，同时该技术也无法全面解决杀软的兼容。

4. 2 独创的加密文件增量保存技术

加密文件编辑后保存，采用了全新的序列模式，加密文件保存数据在磁盘上存储在上一次数据文件的后方，保存动作彻底完成后，才会合并加密文件，能根本保证加密文件的完整性。即使文件在加密保存过程中突然断电，我们也不会造成任何数据的损坏，这点是以前的加密软件无法突破和实现的。假设一款应用软件在未安装加密系统时自身突然一场或断电就会坏文件，装上加密系统后我们也保证这个软件的数据不会损坏。

较早前的加解密产品加密文件保存完全是使用 WINDOWS 的文件保存机制，保存任何文件都是先将原始文件清空，然后将当前文件在内存中的数据写到磁盘文件中，在此过程软件异常或断点，此文件必损坏。



从上图比较可看出，对于一个大文件，保存过程相对较长，在此过程中软件异常或断电，我们的产品对于该文件的完整性是有保障的。

4. 3 独特的加密文件权限控制技术

采用驱动级的权限控制注入和防注入技术，不会被杀毒软件和主动防御软件反挂钩。安全行业内的安全问题一直是客户在不断探讨的问题，本产品解决了行业内产品的所有安全漏洞，有的漏洞是操作方式造成的，有的漏洞是技术层次造成。目前行业漏洞：受信进程改名、伪装受信进程、进程注入、消息捕获、OLE 窃取、加密软件评测工具、剪贴板脱钩文件内容被复制出来（除本产品外所有加密软件都无法解决的问题，解决此问题通常是脱钩时强制关闭加密文件，但是又有程序单独对付这种强制关闭文件的方式，所以仍然复制出明文内容，这种处理方式并不是根本解决客户端非常不稳定经常出错，文件损坏）、

伪装授信子进程、UNHOOK 脱钩另存为明文（应用层加密软件技术层次漏洞），冰刀等底层工具提取打开加密文件变明文（单层单缓存驱动加密漏洞）、socket 通讯破解、网络脱卷保存明文……不一一列举。

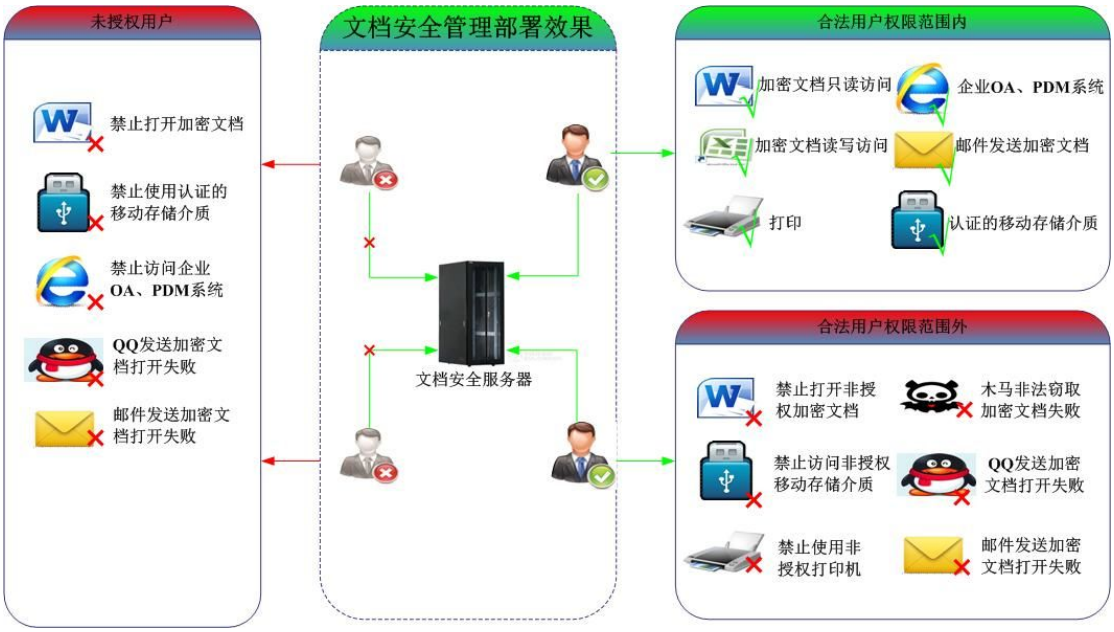
4. 4 外发环境在 WIN7 及 X64 位环境下表现同样优秀稳定

运行环境支持 Windows2000/XP/2003/2008/VISTA/WIN7。并能运行于以上操作系统的 32 及 64 位软硬件平台

无论在任何平台下系统表现非常优异，32 位系统和 64 位系统表现同样出色。不会出现因为操作系统的不同，环境复杂情况而出现各种不稳定现象，更不会因为平台的不同，产品的不稳定在使用过程中造成数据的损坏。

5. 部署效果

系统帮助用户确保电子文档信息外发的完整性和保密性，有效控制了内部人员有意无意的信息泄露行为，防止企业内部重要信息的泄漏和扩散。



主要从以下几方面阐述部署效果：

1. 帮助企业规范文档权限，提升内网信息安全等级

企业信息管理的三要素中，数据的管理要采用主动式的管理方式，产品规范了数据访问的边界，即文档能被哪个用户访问，以及访问的权限、访问的人员范围，越权后将无法访问。企业控制的机密文件在创建、存储、应用、传输等环节中均以加密形式存在，杜绝使用黑客等工具的窃取，即使窃取也无法使用

2. 构建内部信息综合管理平台，有效解决内网安全管理问题

产品集成了文档权限控制、文档外发控制、邮件外发控制、业务系统安全访问网关、移动存储介质接入认证功能，有效解决了内网安全管理范围内的诸多根本问题。

3. 加强对重要文档保护，防止资产泄露造成的各种损失

电子文档安全系统将企业数据信息的安全保护从“区分”的安全等级提升到了“细分”的安全等级。通过加密技术，将数据的潜在用户“区分”为授权用户和非授权用户，并且只有授权用户可以使用。

在这个基础上，系统又将授权用户的应用权限进行了细分，全面支持是否允许打印、是否允许加密文档剪切、复制、粘贴、另存、是否允许截屏、是否允许从加密文档向非加密文档粘贴、文件复制等多种权限，实现员工应用权限的最小化满足。

4. 以客户为中心，策略灵活定制

电子文档安全系统采用前瞻性的以客户为中心的架构设计。它能够最大程度利用客户已有的 IT 资源，并根据客户的不同阶段需求定制不同的功能模块，以满足企业更多需求。产品还能灵活扩展加密未来可能出现的软件，以及应对现有软件升级带来的新情况。

5. 透明支持企业业务流程中，文档流转的完整性及保密性

产品提供的业务系统安全访问网关，针对客户实际环境中使用着 OA、PLM 等系统，可做到上传到业务系统中的文档为明文、下载客户端本地的文档为密文，未安装文档客户端的计算机无法访问业务系统。

7．产品运行环境

配置表：

- 系统安装软件光盘
- 系统监控端安装、使用手册
- 系统服务端安装手册
- 系统管理员用户使用手册

系统软硬件环境要求如下：

<table>
<tr><td colspan="4">服务器</td></tr>
<tr><td>基本监控端数量</td><td colspan="2">0</td><td>允许监控端最大数量</td><td>2000</td></tr>
<tr><td rowspan="3">硬件基本配置(2000 点推荐)</td><td>CPU</td><td colspan="3">Intel®Pentium 4 2.4G，双 CPU</td></tr>
<tr><td>硬盘</td><td colspan="3">200GB</td></tr>
<tr><td>内存</td><td colspan="3">4GB</td></tr>
<tr><td>操作系统</td><td colspan="4">WindowsXP/2003/2008</td></tr>
<tr><td>数据库系统</td><td colspan="4">MYSQL、SQLSERVER、ORACLE</td></tr>
<tr><td colspan="5">监控端及外发环境</td></tr>
<tr><td rowspan="3">硬件配置(推荐)</td><td>CPU</td><td colspan="3">Intel®Pentium II 或更高</td></tr>
<tr><td>内存</td><td colspan="3">1GB 以上</td></tr>
<tr><td>硬盘</td><td colspan="3">监控程序所在磁盘有 600MB 以上可用空间</td></tr>
<tr><td>操作系统</td><td colspan="4">WindowsXP/2003/2008/VISTA/WIN7。并能运行于以上操作系统的 32 及 64 位软硬件平台</td></tr>
<tr><td colspan="5">管理控制台</td></tr>
<tr><td>浏览器</td><td colspan="4">IE6 及以上版本,推荐 IE7 及以上或 Google Chrome</td></tr>
</table>