技术白皮书

华途文档安全管理系统

(Vamtoo—DSM)

华途软件 技术中心

电话：400-675-9090

传真：0571-89988028-800

网址：http://www.huatusoft.com

邮箱：info@huatusoft.com

地址：杭州市西湖区萍水西街 80 号创新软件产业园 1 号楼 20 楼

西区总经理　蔡良 13808214206 QQ：68298345

目录

1. 华途文档安全管理系统

1.1 应用背景

计算机的应用对于普通人员来说已成为一种必备的工作技能，随着计算机硬件技术的完备，可进行存储数据(文件)的功能已经超过人们的想象，再加上网络技术的普及，使人们在任何地点、任何时间均能以快捷的方式获取自己想得到的东西。

计算机系统以及计算机网络，在提高了数据和设备的共享性的同时，也为非法窃取国家机密或者企事业单位内部机密数据打开了绿灯。为了防止数据外泄，企事业单位往往不惜成本，购入防火墙，入侵检测，防病毒，漏洞扫描等被动式的网络安全产品。事实上信息的安全仅仅依靠上述的手段是远远不够的。

目前现有企业电子文档的管理有如下的一些特性：

1. 文件密级无明确的规定和标识；
2. 分散保存，多人分散管理；
3. 明文方式，被获取后易泄密；
4. 无法确认每个文档的利用者；
5. 无法根据需要细分用户权限；
6. 文件使用无期限和次数控制；

随之相对应带来的安全隐患如下：

1. 需保密管理的文件不明确；
2. 文件未经保密处理，易泄密；
3. 未对使用者进行严格的认证；
4. 文件使用权限无法分别控制；

5. 无法根据需要限时限次使用；

6. 文件使用无记录，缺乏审查。

FBI（Federal Bureau of Investigation 美国联邦调查局）和 CSI（Computer Security Institute 计算机安全学会）曾对 484 家企事业单位进行了网络安全专项调查，调查结果显示：超过 85%的安全威胁来自企事业单位内部。在损失金额上，由于内部人员泄密导致了 6056.5 万美元的损失，是黑客造成损失的 16 倍，是病毒造成损失的 12 倍。

机密信息可以通过各种手段轻易的从企事业单位拿走，这些包括网络共享，光盘刻录，U 盘复制，打印，传真，邮件发送等。对于企事业单位来说，这样的危险时刻随时存在。

可见，如果文件本身没有经过任何的安全处理，要防范文件信息不被恶意的获取是非常困难的，因此只有对文件本身进行加密才能达到企事业单位的要求。

虽然对计算机数据外泄途径已非常清楚，企事业单位可以采取相应的技术措施来防止数据的外泄，但这些技术措施和手段仅局限于在计算机操作系统、硬件和网络技术上，且这些技术措施并不能从根本上完全解决问题，而引起的一些后果却给企事业单位带来不良的影响，反而造成不必要的损失。

针对上述情况，华途软件推出了基于网络技术的、通用的计算机华途文档安全管理系统，协助企事业单位完善安全防范措施。目前，华途文档安全管理系统在众多的企事业单位已得了成功应用，使这些企事业单位机密信息得到了有效的保障。

1.2 产品概述

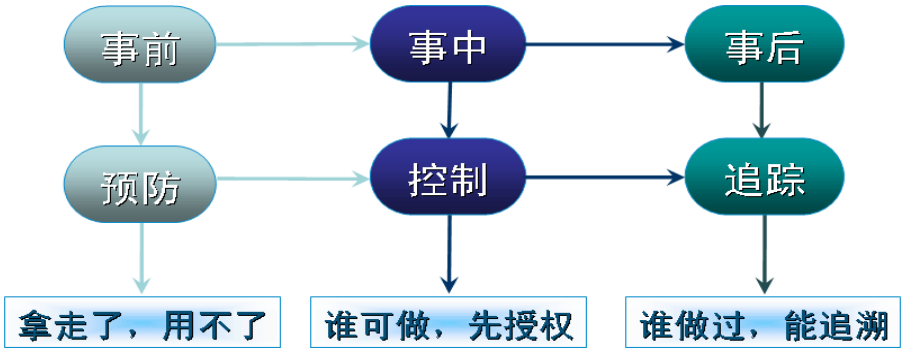
随着电子信息化程度的不断提高，政府军工、企事业单位等各类组织机构越来越多地利用计算机来处理一些机密信息，加强交流、方便沟通的同时增加了信息的非法泄密及内部越权使用等安全风险。传统电子文档几乎不受任何权限限制，明文存放、随意阅读、修改、复

制、打印或分发等，这些正是导致信息泄密的主要原因，如何防止未经授权非法使用及越权使用文档所造成的信息泄密，是目前企业迫切需要解决的问题。

华途文档安全管理系统（Document Security Management System，简称 Vamtoo-DSM）采用动态文档透明加密技术、虚拟化技术、身份认证技术及硬件绑定技术，结合多维密级和权限管理，针对内部员工和部门差异化及自主管理需求，在透明加密基础上对重要数据进行精细化细粒度权限管理。

2.设计理念

DSM 的设计理念：



3.系统组成及架构

3.1 系统组成

DSM 主要由四部分组成，系统服务、管理模块、客户端模块、审批系统及移动应用。

系统服务模块：

系统服务运行在企业的服务器上，包括验证服务、日志服务、更新服务、审批服务、日志报警服务、文件授权服务。主要负责提供网络支持，保证客户端获得及时的用户信息和权限。同时监控客户端的具体操作，将整个系统的运行情况记录在数据库中。

管理模块：

管理程序可以运行在网络环境内任何一台机器，提供友好的人机交互界面，主要功能用于系统参数设置、应用程序策略配置、设置打印机白名单、根据企业的组织结构建立部门和用户信息、设置分级管理员、设置用户权限，定制客户端安装盘，远程安装，系统监控以及日志管理。

客户端模块：

客户端程序又分为下述部分：

1) 加密模块

该模块是 DSM 的核心模块，主要的功能就是控制文件的加解密以及相关的操作（如复制，OLE 嵌入，文件授权、打印（水印、快照）、拖拽、删除文件、程序禁用、截屏等）。

2) 通讯模块

与服务器通信，更新客户端，以及获得必要的操作权限。

3) 外发模块

在客户端将加密文件打包外发，以及进行必要的外发权限设定。

4) 插件

为了方便客户的操作，DocGuarder 在系统的资源管理器中添加了右键插件。用于标示文件状态和进行加密，解密，等级调整，文件外发等操作。

审批系统:

DSM 系统提供了强大的审批功能。系统支持按照用户情况自定义审批流程，流程支持多级并发，不同的用户可提交不同的流程。审批管理员可在线对待审批申请进行处理，系统将自动反馈相应处理结果。并对通过审批的用户自动完成相应的结果。

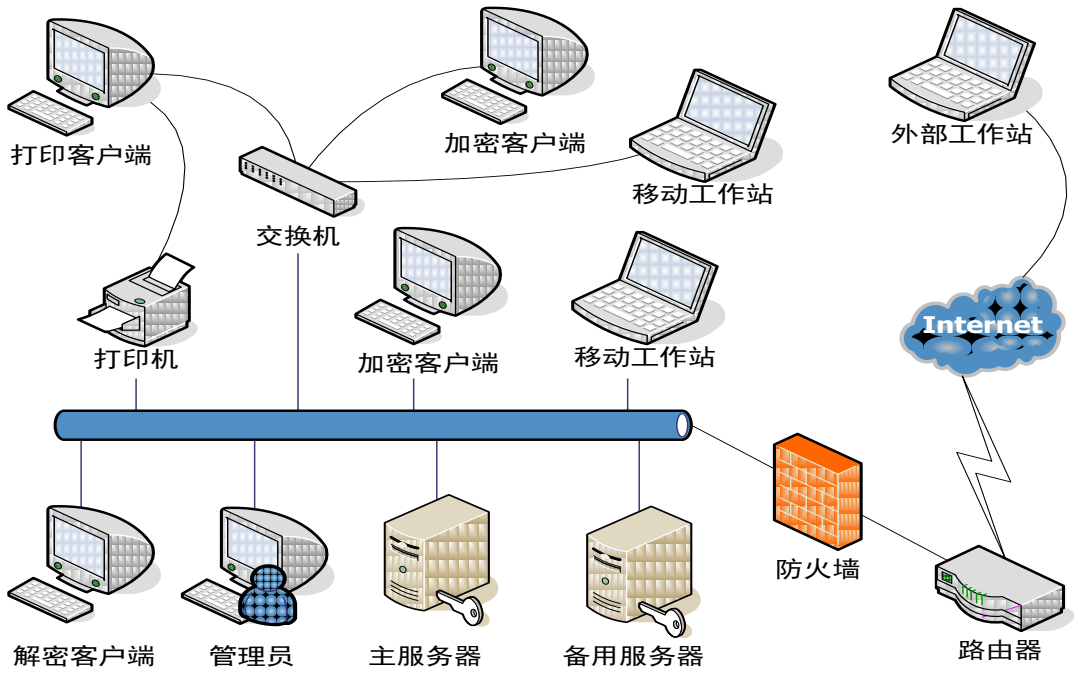
DSM 目前支持解密审批、外发审批、邮件审批、离网审批和补时审批。

移动应用:

DSM 系统支持基于安卓、IOS 系统的密文预览及密文审批功能，使得高层领导在外出办公情况下可及时处理公司内部业务流程，确保业务连续性。

3.2 功能架构

DSM 采用 B/S、C/S 混合架构，由服务端(分布式验证服务、日志服务、更新服务、管理控制台和审批系统<B/S>)、客户端(C/S)两部分组成。适用于任何基于 TCP/IP 协议的网络体系（局域网或广域网）。以下是系统结构图：



DSM 采用等级管理模式，系统管理员可以设定不同的子管理员（如：超级管理员、文件管理员、等级管理员等）。客户端登录时，可直接使用 Windows 当前登录的域用户帐号或者本机帐号作为 DSM 文档安全系统的帐号进行校验。可以针对公司内部域管理模式设置系统的权限，也可以根据公司架构设定多个子管理员进行管理。

3.3 产品部署

DSM 支持域推送安装、远程卸载、客户端远程强制更新、客户端开机自动更新等多种灵活的系统部署方式。可大大减轻企业管理人员对该系统的维护工作量。

DSM 支持服务器的多级分布部署。对拥有多个厂区且分布在不同区域的大型企业而言，该功能可充分满足其使用需求。服务器分布后，所有子服务器的用户列表、用户权限、系统操作日志等均可与主服务器保持同步。产品部署如下图所示：

4.产品亮点

4.1 零感觉加密

DSM 客户端可在不知不觉中完成文件的加密工作，不会影响涉密客户机应用程序的工作界面，也不会改变使用者的操作习惯。同时 DSM 加解密过程执行速度快，系统运行过程占用的系统资源少（CPU，内存），不会影响使用者原有的工作效率。

4.2 适用范围广

DSM 支持所有应用程序控制，如设计类的 Pro/E、UG、CATIA、AutoCAD 等，办公类 Office 系列等，汇编类 VC、VB 系列等可以产生文件的程序，并且可以与 PDM 系统（如 TeamCenter、SolidWorks 等）无缝集成……适用范围非常广。

4.3 自动加密

DSM 客户端在涉密客户机启动后自动运行，无需人工干预。DSM 运行后将自动对控制列表中的受控软件系统进行强制加密。

4.4 永驻系统

DSM 客户端属于内嵌式软件系统，系统一旦安装，将永驻在涉密客户机的操作系统之中。DSM 安装后，在操作系统的安装/卸载界面中将不出现该系统的安装条目。DSM 卸载需要权限和专供的卸载工具；对加密进程进行保护，系统运行后，进程不能被强行终止；系统采用特征注入技术，可防止用户将受控程序改名后绕过安全系统的控制。

4.5 防范严密

DSM 针对以下安全漏洞进行了全面堵截：

——系统操作漏洞（内容复制、屏幕截取与录制、OLE 插入、内容拖拽等）；

——打印控制漏洞（物理打印机、虚拟打印机文件转化等）；

——邮件发送漏洞（SMTP-mail、WEB-mail、程序内邮件等）；

——存储控制漏洞（软/硬盘、U 盘、刻录设备、1394 /红外/蓝牙设备等）；

——文件传输漏洞（FTP 传输、HTTP 传输、P2P 传输、IM<QQ、MSN>传输等）；

——程序控制漏洞（涉密程序改名、阻止进程加载、终止进程、卸载客户端等）；

——数据删除漏洞（删除、彻底删除等）。

4.6 安全性

DSM 采用数字版权保护(Digital Right Management，DRM)理论技术，支持国密算法，以 256 位密钥结合硬件环境，针对不同的操作系统和应用软件进行加密控制，同时允许企业自定义密钥。DSM 所控制的文件在保存(或自动保存)过程中，自动给文件注入密钥信息形成加密文件。该种加密方式符合国际密匙原则，破解级别达到 3 级(说明：1 级最高，5 级最低)。

DSM 通过对内存进行安全保护，防止非涉密程序的读取操作，确保涉密信息不被泄漏。

DSM 保证企业密钥全球唯一，即使是同样安装 DSM 的另一家企业，也无法浏览和操作本企业经 DSM 加密的文件。

同时，DSM 允许企业自定义密钥。经企业自定义密钥后，即使开发商华途软件也无法解密该企业加密文件。

4.7 兼容性

DSM 完全兼容现有网络、硬件系统，如路由器、网关及防火墙；完全兼容已知的安全软件，如杀毒软件、防火墙软件，加密进程不会被安全软件误判为病毒或木马并被清除或终止；也兼容最新的 Windows 系统平台，如 Windows Vista、Win7 等。

4.8 集成性

DSM 可集成 PDM 系统、ERP 系统、OA 系统、CPC 系统、设计分析系统等使用广泛的管理系统，对控制列表中不存在的管理系统，DSM 提供现场集成功能，能充分满足企业的复杂需求，可谓集成能力强，集成范围广。

4.9 可维护性

DSM 采用集中管理方式，客户端的策略变化、权限变化等操作均可在管理控制台完成；当有新版本发布时，只需将新版本程序放入服务器，客户端即可自动更新，无须人工更新每个客户端，系统维护工作量非常小。

4.10 可交流性

DSM 提供如下几种与外界交流的手段：

方式一：文件经系统外发功能外发，此种方式最安全，可有效堵截泄密漏洞；

方式二：文件经解密后外发，此种方式需配合相关制度或流程；

方式三：文件经安全邮件外发，此种方式需要预先设定安全邮箱清单；

方式四：文件转化为 PDF 格式后外发，此种方式可配合相关制度，指定专人完成。

4.11 系统部署

DSM 支持域推送安装、远程卸载、客户端远程强制更新、客户端开机自动更新等多种灵活的系统部署方式。可大大减轻企业管理人员对该系统的维护工作量。

DSM 支持服务器的多级分布部署。对拥有多个厂区且分布在不同区域的大型企业而言，该功能可充分满足其使用需求。服务器分布后，所有子服务器的用户列表、用户权限、系统操作日志等均可与主服务器保持同步。

4.12 自动扫描

对涉密客户机上的历史文件，DSM 提供文件初始加密功能。DSM 自动对涉密客户机上的指定格式文件进行自动的全盘扫描并加密，无需人工干预。

4.13 离线控制

DSM 可远程制作、发放、更新与卸载离网许可，设定涉密客户机离线策略，包括离网使用时效、次数等。

同时，DSM 提供文件离线外发功能，允许使用者将加密文件（无需解密）发送到企业

外部，外部使用者可按规定的时间和次数来使用该加密文件，且不能进行二次传播。

4.14 密级控制

企业在 DSM 中可以根据管理需要定义文档密级，可按部门或角色设定密级，也可按文档机密程度进行分级，如通用、保密、机密、秘密、绝密等，从而控制加密文件在企业内部的打开权限、打印权限、密级调整权限以及文件解密权限。例如：可定义部门领导只能解密本部门文档，而企业高层领导可解密所有密级文档。

4.15 故障容错

DSM 允许在发生网络连接意外(如交换机故障、服务器硬件故障或网线连接故障等)时，利用故障保持功能保证客户机在故障期间的正常使用。同时，DSM 允许当主服务器发生硬件或系统故障时，所有客户机自动连接至备用服务器，从而保障工作的顺利进行。

4.16 日志审计

DSM 提供完备的日志管理，可记录文件日志、管理日志、打印日志、授权日志等详细日志，并提供日志查询、导入、导出功能，确保文件与操作的可追溯性。

5.技术特性

华途文档安全管理系统（DSM）采用动态文档透明加密技术、虚拟化技术、身份认证技术及硬件绑定技术，结合多维密级和权限管理，针对内部员工和部门差异化及自主管理需求，在透明加密基础上对重要数据进行精细化细粒度权限管理。

6.应用价值

6.1 防止企业文档外泄

实时加密企业文档，未经授权，离开公司环境无法使用。

6.2 防止核心信息被攫取

采用强制自动加密和完善的文档密级管理机制结合 ,核心涉密文档 ,可按人员授权使用。

6.3 防止企业内部越权使用文件

通过权限管理机制，限定不同部门对企业文档的使用权限，有效控制机密文件的使用范围。

6.4 防止合作伙伴再次扩散泄密

通过文件外发管理系统，限定外发文档的使用时间、次数，并可限制指定电脑使用。

6.5 解决黑客木马病毒泄密文件

从数据源头上对企业文档进行保护，防止信息被窃取之后非法使用。

6.6 详尽的日志保证泄密可追溯

完善的日志管理功能和详细的日志记录，实现了泄密渠道的可追溯性。

华途软件西区总经理 蔡良 13808214206 QQ：68298345