

doi: 10.7690/bgzd.2014.03.010

金戈 I/O 信息输入输出管理系统

彭鹏, 石向炜, 薛俊民, 安维嵘

(中国兵器装备集团公司信息中心, 北京 100089)

摘要: 为有效促进保密管理工作的规范化、制度化、信息化和流程化, 并大幅提高管理工作的效率和水平, 将计算机技术与保密相关业务流程管理相结合, 运用到军工单位信息输入输出管理系统建设中。以某军工集团公司总部为例, 阐述建设金戈 I/O 信息输入输出管理系统的必要性, 提出金戈 I/O 系统建设目标及思路, 总结金戈 I/O 系统技术实现与特点。应用结果表明: 该系统能实现硬件与软件相结合的系统化管理, 满足集中管控的要求, 使内网信息输入输出管理高效、安全、可控。

关键词: 信息输入输出; 信息化; 身份认证; 系统集成

中图分类号: TJ03 **文献标志码:** A

JinGe I/O Input and Output of Information Management System

Peng Peng, Shi Xiangwei, Xue Junmin, An Weirong

(Information Center, China Ordnance Equipment Group Corporation, Beijing 100089, China)

Abstract: To effectively promote the standardization, institutionalization, informatization and process of the security management, and greatly improves the efficiency and level of management, computer technology and security related business process management are combined, applied to information input and output management system of the military unit. In this paper, taking certain military group headquarters as example, the author explains the necessity of construction of JinGe I/O input and output of information management system, put forwards the target and mentality of the system construction, concludes the system realization and characteristics on technology. The results of application show that, the system can realize the management system by the combination of hardware and software to meet the requirements of centralized control, so that the intranet information input and output management is efficiency, safety, controllable.

Keywords: information input and output; informatization; identity authentication; system integration

0 引言

传统的信息输入输出涉密信息系统需分别进行流程审批与实际操作^[1-2], 安全保密管理的时效性、有效性存在很多需要改进的地方, 而信息输入输出管理系统则通过管理手段和信息化手段的结合, 将流程审批与实际操作融合到一起, 兼顾了信息输入输出流程管控的高效与有效。笔者以某军工集团公司涉密信息系统——“金戈”网(简称“金戈 I/O 系统”)为例, 对金戈 I/O 信息输入输出管理系统的设计与应用进行研究。

1 建设金戈 I/O 系统的必要性

建设金戈 I/O 系统前, 某军工集团公司总部各部门(以下简称各部门)分别部署 1 台输入输出机, 由专人负责输入输出。信息输出时, 信息流向为: 先将涉密系统中要输出的信息以邮件形式发送到本部门信息输出专用邮箱中, 由输入输出负责人将文件下载后, 刻录成光盘, 交给输出发起人; 审批流程以纸质表格形式体现, 按不同密级由相关领导进行审批。信息输入时, 信息流向与信息输出相反, 外来光盘经杀毒、恶意代码查杀等过程后, 将文件导入到部门专用邮箱中, 再发邮件给发起人; 审批

流程与信息输出类似, 也要按不同密级进行审批。

另外, 在分散管理的情况下, 各部门为了提高工作效率, 还配置了涉密及非密 U 盘, 供输入输出使用。其中涉密 U 盘需在涉密网络中注册才能使用。但在这种情况下, 信息输入输出仍存在诸多问题:

1) 审批流程与文件输入输出流程脱节。

文件输入输出流程与审批流程结合不紧, 在某种程度上存在“两张皮”现象, 审批效率不高, 容易造成差错, 通过审批的文件可能与实际输入输出的文件不一致。

2) 输入输出未进行集中管理。

文件输入输出由各部门负责, 未在总部范围内集中管理, 未达到相关标准、技术要求及管理规范的要求, 不利于集团公司的军工保密资格一级认证。

3) 耗费较多人力物力, 工作效率低。

各部门分散管理文件输入输出, 每个部门都需要分别部署输入输出专用机, 并由专人负责, 增加了人力物力, 且工作效率不高。

4) U 盘等存储介质分散管理, 存在安全漏洞。

每人都配备了涉密及非密 U 盘, 便于进行数据输入输出; U 盘的丢失及误操作, 都容易引起失泄密事件, 存在重大安全漏洞。U 盘误操作, 在客户

收稿日期: 2013-11-03; 修回日期: 2014-01-20

作者简介: 彭鹏(1982—), 男, 辽宁人, 学士, 工程师, 从事计算机科学与技术研究。

端留下接入痕迹,也不满足军工保密资格认证要求。

通过信息化管理手段可以很好地弥补这些不足。信息化的管理手段可以将业务人员与管理人员从简单而枯燥的审批单打印、签字等工作中解放出来。利用 Web Service 技术及系统间的集成,金戈 I/O 系统把流程审批与实际操作有机地联系起来。由于信息系统的严谨性,信息输入输出工作流程都有严格的次序,不存在人为的干扰因素,可以很好地规范工作过程^[3]。

1) 审批流程电子化。将纸质表单电子化存储,依赖信息技术,丰富查询统计手段,同时推进办公自动化水平,推动网上办公和无纸化办公。

2) 系统集成提高用户感知。通过系统集成,融合了 OA 办公系统、身份认证系统、“三合一”系统、光盘刻录与审计系统的优势功能,实现了硬件与软件相结合的系统化管理,各系统间的衔接紧密,输入输出信息在系统间透明传输,提高了用户感知度。

3) 用户认证安全可靠。用户使用 USB-Key 登录金戈 I/O 系统,采用与现有涉密信息系统、协同办公等应用系统相同的安全认证机制(USB-Key 作为用户登录系统的唯一身份凭证),确保在协同办公系统中发起信息输入输出的用户,与登录金戈 I/O 系统用户的一致性,保证了用户安全认证的唯一性、安全性和准确性。

2 金戈 I/O 系统建设目标及思路

2.1 建设目标

金戈 I/O 系统的建设目标是相关标准、技术要求及管理规范的要求,结合某军工集团公司情况,在现有涉密信息系统基础上建立既符合保密要求,又能提高业务工作效率的输入输出信息管理系统。

金戈 I/O 系统还需实现如下技术目标:

1) 支持集中管控,统一管理; 2) 分布式应用; 3) 安全软件的集成性^[1-2]; 4) 多用户并发; 5) 高可用性; 6) 独立安全域。

最后,该系统的业务目标是:

1) 信息交换全流程管控; 2) 用户身份电子认证功能; 3) 符合用户对已有涉密信息系统(协同办公系统)的操作习惯,界面友好、易于使用; 4) 降低人工及办公成本,提高工作效率。

2.2 建设思路

金戈 I/O 系统是某军工集团公司信息输入输出交换平台、智能管理平台、安全保密管理平台,它以独立安全域、电子化审批流程、集中管控、用户电子身份认证为重点,达到高效、安全、可控的信息输入输出,如图 1。

金戈 I/O 系统优化了已有的信息输入输出流程,实现了电子化审批,设置了独立安全域,满足

安全保密管理要求;通过集中管控、用户电子身份认证等技术手段,实现了输入输出信息的集中管理、集中审计,以及以用户 USB-Key 为唯一凭证的智能登录(登录后即为本人对应的输入输出功能操作模块)。上述总体建设,达到了某军工集团公司涉密网络信息高效、安全、可控的输入输出要求。

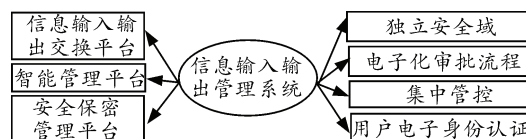


图 1 金戈 I/O 信息系统组成示意图

3 金戈 I/O 系统技术实现与特点

3.1 技术实现

在某军工集团公司涉密信息系统内网(以下简称“内网”)的 DMZ 区(DMZ 是英文“demilitarized zone”的缩写,中文名称为“隔离区”,也称“非军事化区”。它是为解决安装防火墙后外部网络不能访问内部网络服务器的问题,而设立的一个非安全系统与安全系统之间的缓冲区。)划分一个数据交换虚拟局域网(virtual local area network, VLAN),根据需求部署一定数量的中间交换机和数据交换计算机,目前根据输入输出途径分离、涉密非密信息分离的原则,部署了涉密、非密中间交换机各 1 台,涉密、非密数据交换计算机各 1 台。中间交换机,用于将外部光盘转换为金戈 I/O 系统专用光盘,数据交换计算机是内网与外部信息输入输出的终端。

进行内网信息输入输出时,须将本人的 USB-Key 插入到数据交换计算机上,登录数据交换计算机进行身份鉴别后,方可使用金戈 I/O 系统,系统通过 Web Service 方式调用 OA 系统中的邮件功能,将系统专用光盘上的输入文件发送到本人邮箱中,或将审批后的文件下载并刻录到系统专用光盘中(数据交换计算机不保存输入输出文件,直接从光盘中读入文件或直接刻录文件到光盘)。信息输入时,承载数据的普通光盘要转换为金戈 I/O 专用光盘,信息输出的光盘也为金戈 I/O 专用光盘。金戈 I/O 专用光盘上有条码及数字字母编号,标识光盘的唯一性,并记录在金戈 I/O 系统日志中备查。

3.2 技术特点

1) 安全性:划分了独立安全域,设置访问控制策略,与内网其他信息系统分离,具有严格的审计功能,如输入输出端口管控、用户操作行为审计功能、数据输入输出的病毒查杀及光盘刻录审计等功能。金戈 I/O 系统的架构,通过交换机的 VLAN 机制,实现了安全子域内的集中管控;严谨的部署,确保了病毒查杀的异构性,提高了系统信息的安全防护水平。