项目成果

综合管控平台的建设与实施，不仅是信息系统的设计与开发，更多地是业务模式和管理方法的创新与推广，该项目主要成果包括：（1）推进了中航动控“战略－预算－绩效”联动体系建设，促进战略、预算、组织绩效的联动落地。（2）解决了异构网络下跨地域业务协同，通过系统集成实现动控板块的集中运营管控和异地工作协同。（3）固化了业务流程并规范了管控过程的相关表单。（4）通过各项管理制度、平台运行要求的制订为中航动控落实整体管理策略和系统推广运行保驾护航。

应用效果

通过统一平台的建设，明确了各成员单位与总部进行战略对接、项目计划管控颗粒度、绩效考核等关键问题，实现了总部与各厂所之间的业务协同，打通了企业战略－运营－项目－绩效的业务通道，形成了一体化的管控模式。通过项目计划编制和反馈，实现了项目计划与企业战略的数据集成，以及项目驱动关键指标与行动方案的达成。

在综合管控平台建设的过程中，中航动控梳理了企业战略、经营、项目管理的业务模式，明确了各成员单位与总部进行战略对接、项目计划管控颗粒度、绩效考核等关键问题，为后续的管理提升奠定了坚实的基础。通过“战略－运营－项目”业务模型的落地，提高了两级管控水平，将企业战略切实落实到日常经营中的各个方面，实现了战略的动态闭环管理，提高了跨地域业务沟通和协同工作的效率。

（责编　谷雨）

基于PKI/CA构建国防军工可信网络环境

Construct National Defense Credible Network Based on PKI/CA

中航工业直升机设计研究所　许俊华　米卫平

中航工业直升机设计研究所是中国航空工业集团公司成员单位，隶属于中航直升机有限责任公司，在天津滨海新区和江西景德镇建立了完整的设计试验体系，对异地间网络安全提出更高的要求。

PKI/CA 是中航工业统一身份认证的基础，为统一身份认证提供可信增强的身份标识。为了加快与金航网业务实现身份互信互通、资源互享，以及开展研究所内信息系统的安全加固等保障服务，中航工业直升机所以密码技术为核心，以国家相关法律法规为依据，以金航网 PKI/CA 根中心为基础，利用公开密钥基础设施构建一套双中心（证书管理中心、密钥管理中心）、双证书（签名证书、加密证书）、双密钥（加密密钥、签名密钥）二级架构 PKI/CA 信任体系（即二级 CA 中心）。该体系实现信息系统可信身份统一标识、可信身份统一签发等。

在直升机所的总体指导下，中航工业信息技术中心（金航数码）、格尔软件协助完成 PKI 网络信任体系的建设，基于 PKI/CA 体系，以业务应用为基础、以数字证书为认证要素、以角色访问控制为手段，综合运用安全技术及产品构建一套 PKI/CA 应用安全支撑体系，该体系结合了操作系统安全、网络接入安全、应用接入安全和数据交换安全等核心技术，实现为操作系统、网络系统、应用系统提供身份认证、访问控制、责任认定以及安全审计等全面安全保障服务的目标。

项目亮点

（1）CA 数字证书与网络准入控制联动。

通过将 802.1x 协议与数字证书相结合，实现对接入内网的终端身份进行实名认证。当终端接入内网时，需要提交数字证书并通过准入系统的认证授权后，方可连入网络，同时基于数字证书实现全程实名制审计。

（2）应用的安全防护。

CA 系统与门户系统完成整合，实现了用户身份的统一管理、统一认证、统一授权等安全服务，利用数字证书实现增强的身份认证服务，采用数字签名技术来保证业务的不可否认性和责任认定的权威性，采用组合加密和数字信封方式保证应用数据在流转和存储中的机密性和完整性。

（3）应用系统“零”改造。

由于各应用系统建设时间各不相同，采用的技术平台和架构各不相

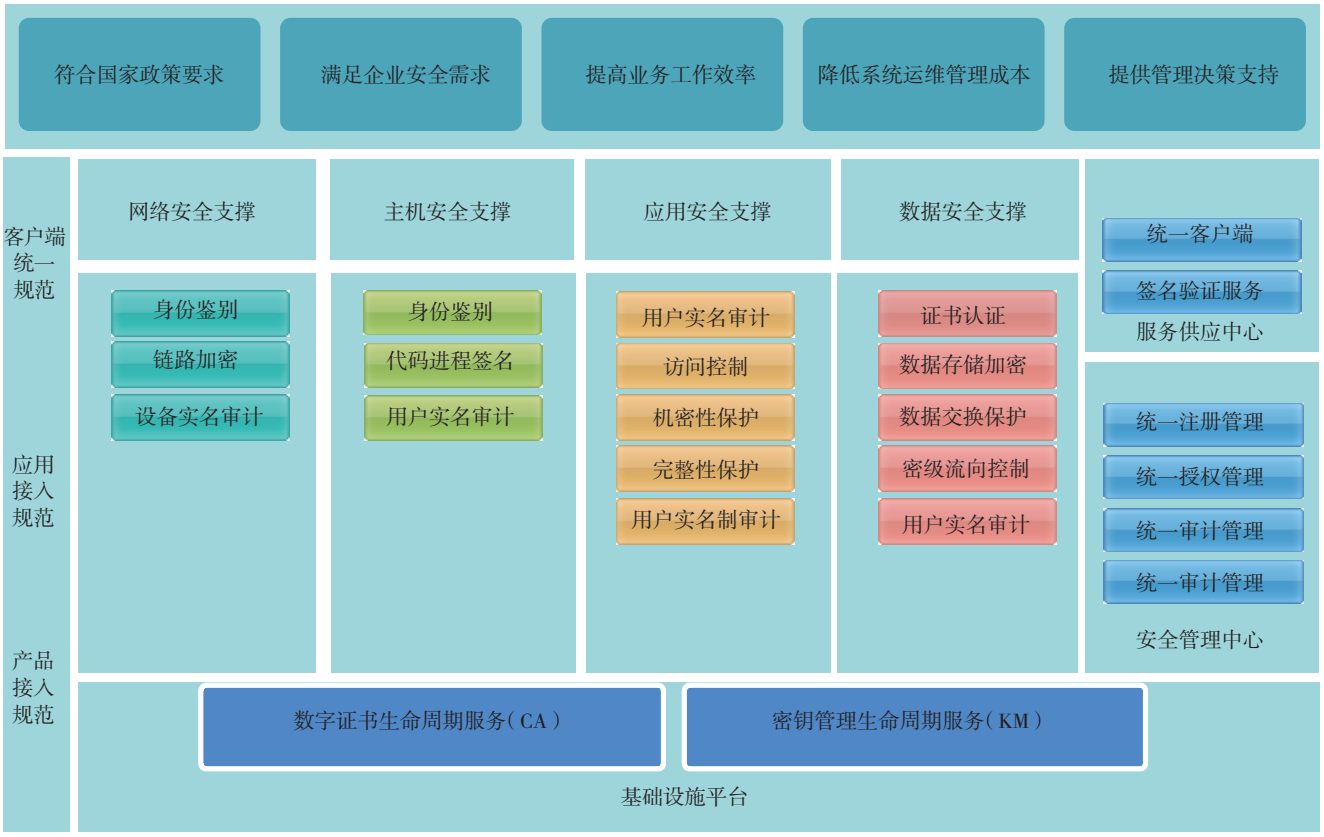

图1　基于PKI应用安全保障体系

同,尤其业务系统都是作业系统,很多应用系统无法进行二次开发与改造,因此就给 CA 系统整合带来了难题。在对现有应用安全集成设计时,研究开发了“应用代理认证”模式,能够实现不对应用进行任何改造即可实现基于数字证书安全认证接入,最大限度地减少数字证书应用接入过程对业务的影响。对于部分应用系统无法进行二次开发,对基于 PKI 技术的应用产品进行了深入的开发与研究,形成了一套标准、通用的解决措施进行合规性的支撑。

(4)全程加密,拒绝抵赖。

采用 CA 数字信封技术保障业务系统从发出到接收的全程安全,采用数字签名技术确保文件传输过程中的机密性、完整性和通信双方对文件发送、接收行为的不可抵赖性以及对通信双方身份的可信赖性等要求。系统所传输的文件在网络传输、服务器存储以及客户端存储时,都是以密文形式存在的。

(5)集中存储,流向控制。

基于数字证书的公私钥密码体系,采用集中加密存储、流向控制 / 审计等技术措施对内网文件交换进行安全管理。通过对人员定密、文件标密、数据加密并基于密级标识进行相应的访问授权及控制,实现内网数据的安全交换、安全存储以及交换后的实名制审计。

(6)构建一套完善 PKI/CA 网络信任体系。

通过利用 PKI/CA 技术为信息系统构建了一套信息安全基石,基于“安全基石”可以扩展或深化众多的安全应用。PKI/CA 网络信任体系以 1 个基础平台为支撑,以 2 个中心为支持,以 3 个规范为标准,以 4 个支撑为手段,为信息系统提供 5 项服务。其架构图如图 1 所示。

通过 PKI/CA 建立一套可信、可控和可管理的应用安全设施,形成从用户、主机、网络、应用、数据等全过程的可信运行环境。

应用效果

PKI 网络信任体系在政策法规上能实现快速分级保护、等级保护的相关要求,在管理上提高信息安全保障 / 管理水平。在技术上,从根本上增强信息安全保障水平;身份认证服务平台作为信息安全基础设施,为上层业务应用系统提供身份整合和认证、授权管理及决策和行为审计等安全服务。

它能够在广度和深度上提供充分的安全保障:广度上为网络设备、安全设备、操作系统、业务系统和管理信息系统提供认证、授权和审计服务;深度上为用户提供身份整合、多种认证方式的支持,以及提供细粒度的统一授权、用户行为的详细审计分析服务。

(责编　亿霖)