基于校园一卡通系统架构的4A安全管理流程研究

顾 瑞

(南京审计大学 信息化办公室,南京 211815)

[摘 要] 校园一卡通系统覆盖了高校教学、生活等各个方面,是高校所有业务系统中最基础也是最重要的业务系统。确保一卡通系统的稳定和安全一直以来都是高校信息化工作的重点。文章在分析了高校一卡通系统架构以及安全管理现状的基础上,设计了基于校园一卡通系统架构下的4A安全管理流程,从而更好地确保校园一卡通系统的安全和稳定。

[关键词] 一卡通;安全;4A
doi:10.3969/j.issn.1673-0194.2018.15.068
[中图分类号] TP393 [文献标识码] A [文章编号] 1673-0194(2018)15-0169-04

0 引 言

近几年来,随着信息技术的飞速发展,许多高校都加快了信息化建设的步伐,尤其是信息化建设的重要工程"校园一卡通系统"建设,也在各大高校广泛开展。按照"一卡在手,走遍校园"的建设理念,许多高校陆续完成了本校一卡通系统的建设工作,实现了身份认证和校园支付两大一卡通系统的基础功能,因此,校园一卡通系统已经成为高校最基本和最核心的业务系统。如何更加科学、有序、合理地管理好校园一卡通系统,确保校园一卡通系统的稳定和安全,已经成为高校信息化工作者的工作重点。为此,许多高校颁布了一系列安全管理制度,投入大量的人力、物力和财力,加强一卡通系统的安全管理工作。

1 校园一卡通系统架构

虽然每个高校的信息化水平有高低不同,但是在进行一卡通系统建设时的基本思路都是一致的,都是围绕身份认证和校园支付两大一卡通系统的功能,以非接触的CPU卡、M1卡、手机NFC等各类介质,整合消费、门禁、图书借阅、水电控等系统,替代学生证、工作证、图书证、就餐卡等各类卡片,提供消费支付、图书借阅、门禁考勤、身份识别等基础服务,从而实现"一卡在手,走遍校园"的建设目标。

高校的一卡通系统[1]的总体架构如图1所示,最左边的图显示了高校的各个应用系统,中间的图显示了高校的数字化校园平台,右边的则是一卡通系统的架构图,图中清晰地显示了高校一卡通系统的内在架构以及和数字化校园平台、及各个应用系统的关系。高校一卡通系统和校园各个应用系统、以及数字化校园平台一样,都是部署在学校网络、服务器和存储等基础硬件资源上,一卡通系统通过与数字化校园平台进行对接,身份认证和与各个应用系统进行数据交换,从而实现一卡通系统的各个应用。

[收稿日期] 2018-02-12
[基金项目] 江苏省高校自然科学研究重大项目(12KJA630001)。

目前我国电气自动化控制系统的应用在各行各业都很广泛,并一定程度上满足了行业市场的基本需求,但是面对市场竞争越来越激烈的趋势,其开放化、智能化、通用化、安全化的发展趋势必须得到相应的重视,从而使电气自动化控制系统功能得到大幅度的提升。

主要参考文献

[1]梁凤珍,赵慧峰.浅析电气自动化技术在化工生产中的应用及发展趋势[J].科技创新导报,2012(29).
[2]郭红生.电气自动化工程控制系统的现状及其发展趋势[J].科技创业月刊,2011,24(12).
[3]冯睿鹏.电气自动化控制系统的应用及发展趋势[J].化工设计通讯,2016,42(1).
[4]王友富.电气自动化控制的应用及发展趋势研究[J].低碳世界,2016(8).
[5]刘惠彦.电气自动化工程控制系统的现状及其发展趋势[J].科技创新与应用,2013(18).
[6]吴大鹏.电气自动化工程控制系统的现状及其发展趋势[J].中国水能及电气化,2016(2).

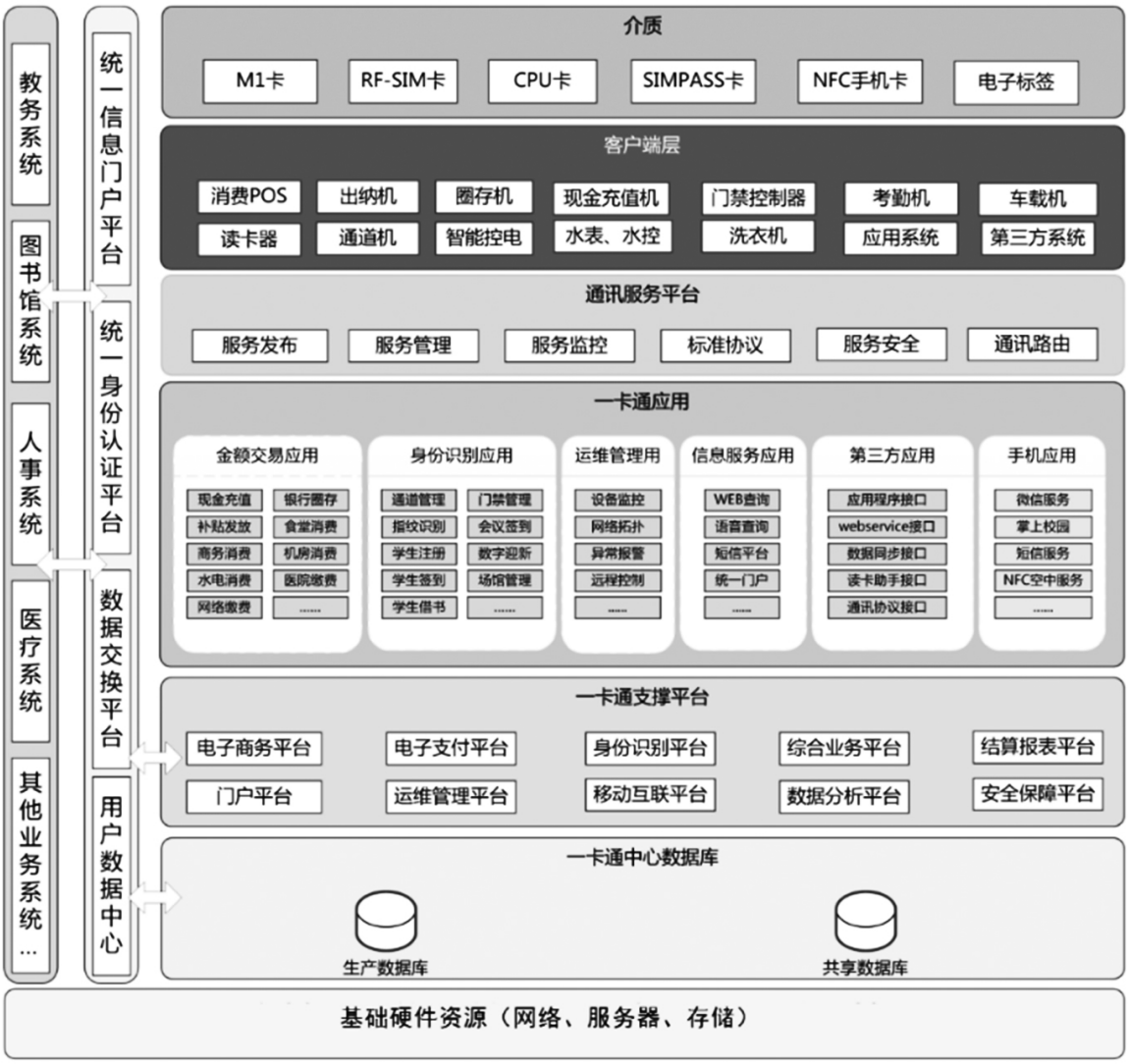

图 1　一卡通系统架构图

如图 1 所示，校园一卡通系统由六个组成部分，即一卡通数据中心平台、一卡通支撑平台和一卡通应用平台、通讯服务平台、客户端层和介质。

(1)一卡通数据中心平台即一卡通中心数据库，存放着所有一卡通生产数据和与其他应用系统对接的共享数据，校园卡应用的商务管理、银行转账、身份识别管理等各种应用子系统的建立都以该平台为基础。

(2) 一卡通系统支撑平台，包含对一卡通系统的管理和维护，数据交换、交易及同步，用户及设备的管理、系统参数的设置和环境的设定，系统各模块的工作状态监控和工作模式的设定，密钥管理等功能。

(3)基于一卡通系统支撑平台之上，是一卡通应用平台，包括消费支付服务、商务管理、银行转账、身份识别管理、学生业务等各系统以及各第三方系统接入；根据统一的接口标准和接入规范。

(4)通信服务平台，负责提供统一的通讯服务接口，确保各类一卡通终端介质安装协议标准与一卡通应用平台的通讯，从而实现各种服务。

(5)客户端层包含了所有一卡通系统的硬件终端，包括各种消费类应用和身份识别类应用终端。

(6)介质层包含了所有一卡通的卡片介质，包括 M1 卡、CPU 卡、NFC 手机卡等。

2　高校一卡通系统的安全管理现状

由于一卡通系统由六个组成部分，每个部分都很重要，一旦出现安全问题后果不堪设想，因此，高校的信息化工作者非常重视一卡通系统的安全管理工作，通常会按照一卡通系统的架构，构建安全管理体系[2]。虽然各个高校的一卡通系统安全管理体系存在差别，但归纳起来，该体系主要由四个部分组成，即硬件平台安全、数据库安全、系统平台安全和校园卡安全。

(1) 硬件平台安全包括支撑一卡通系统的所有硬件设备的安全，即网络安全、服务器安全、存储安全。硬件平台安全是一卡通系统安全的基础，是高校信息化工作者的工作重点，许多高校

通过配置安全设备,制定安全策略和硬件容灾方案,确保硬件平台的安全。

(2) 数据库安全是确保所有一卡通业务数据和公共数据的完整,不被窃取、丢失和损害。数据库安全是一卡通系统安全工作的核心,高校信息化工作者通常通过制定数据备份方案、部署防病毒软件以及采取数据加密技术来确保数据的安全。

(3)系统平台安全是确保一卡通系统所有业务的安全稳定,它包括一卡通系统的支撑平台安全和各个应用系统的安全。高校信息化工作者通常采取系统打补丁、升级等方式修复应用系统漏洞,从而确保系统平台的安全。

(4)校园卡安全是确保一卡通系统的校园卡介质的数据安全,防止校园卡被复制、篡改和盗用。由于 M1 卡秘钥已经被破解,存在安全隐患,现在大多数高校都采取了 CPU 卡作为校园卡的介质,并通过各种加密方式,从而确保校园卡的安全。

为了构建一卡通安全体系,保障一卡通系统的安全,许多高校纷纷投入大量的人力、物力和财力,按照一卡通系统的架构,通过制定安全管理策略、购置安全设备、部署安全管理策略,配备专门的安全管理人员来保障一卡通系统的安全。但是,一卡通系统的安全事件仍层出不穷,一卡通系统依然会经常遭受来自内外部的威胁和攻击,系统中病毒、数据被窃取的现象屡屡发生。究其原因,可以归纳成以下两点:

(1)一卡通系统本身的特点导致一卡通安全事件频发。由于一卡通系统与其他应用系统不同,它不是一个孤立的系统,它是一个功能全面、结构复杂、整合各个应用的综合系统,任何一个子系统的安全受到威胁都会影响到一卡通系统的安全,所以很多一卡通系统的安全问题都是因为其子系统遭受安全攻击而引起的。

(2)没有考虑“人”的因素,导致一卡通系统安全事件频发。高校的安全管理体系是按照一卡通系统的架构来构建的,也就是站在“物”的角度来考虑,着眼点通过对系统内所有的“物”进行安全防护,从而达到安全的目的。而 95%的安全事件都是人为造成的,也就是无论是来自一卡通系统外部的用户和内部系统的使用者、管理者和维护者,都会影响系统的安全,造成不同程度的危害。

因此,高校的一卡通系统安全管理工作除了围绕一卡通安全体系构建以外,还必须从以上两点原因入手,采取相应措施,才能更好地保障一卡通系统的安全,4A 安全管理则是从这两点原因入手,来构建安全体系,保障一卡通系统的安全。

3 4A 安全管理概述

如上节所述,一卡通系统架构包括各个彼此独立的应用系统,如通道系统、门禁系统、图书借阅等,每个系统的功能不一样,用户类别、用户权限、安全策略都不一样。但是任何一个应用系统出现安全问题,都会影响一卡通系统的安全,所以无论对于系统管理人员还是维护人员来说,确保一卡通系统尤其是各个应用系统的安全,一直都是一件工作量巨大缺收效甚微的工作。因此,建立统一的安全管理平台就显得尤为重要,而 4A 安全管理平台的建立则有效地解决了这一难题。

4A[3]是四个英文单词“Acount”(账号)、“Authentication”(认证),“Authorization”(授权),和“Audit”(审计)的首字母组成的。4A 安全管理的核心是构建一个统一的安全管理平台,包括统一的身份管理、统一的认证安全管理、统一的授权安全管理和统一的安全审计管理四个部分,如图 2 所示。

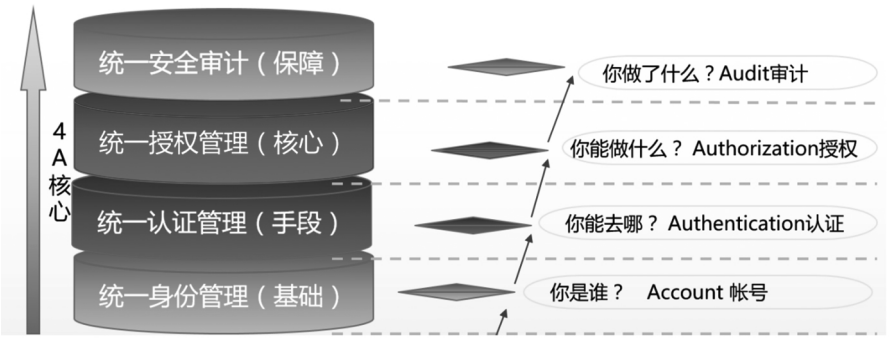

图 2 4A 的核心架构图

统一身份管理是 4A 管理的基础,即对于和系统相关的所有人员的身份进行分类管理,通过账号来解决“你是谁”的问题。以高校的一卡通系统为例,其与之相关的人员的身份有很多类型,有教师、学生等一卡通系统的用户,也有一卡通系统的日常业务操作员、还有一卡通系统的应用管理人员,以及运维管理人员等,为了更好地确保一卡通系统的安全,杜绝人为因素危害到系统的安全,必须首先做好人员的身份管理工作。

统一认证管理是 4A 管理的手段,即所有与系统相关的人员都在一个平台下进行统一的认证。通过认证解决“你能去哪的”的问题。根据不同的人员身份,确定其认证方式,即一般的静态口令、安全性较高的动态口令,数字证书等。认证以后用户根据其身份,确定能访问指定的系统资源。以一卡通系统为例,与系统相关的人员身份不同,所以其认证方式也不一样,对于一般的业务操作人员,只要一般的静态口令就可以了,而对于系统管理员甚至是维护人员,则需要安全性较高的动态口令。每个用户认证以后能访问哪些一卡通系统里的资源,也是通过授权来决定。

统一授权管理是 4A 管理的核心。即对通过一个平台进行统

一认证后的用户进行权限分配，从而明确他的操作权限。统一授权管理是用来解决“你能做什么”的问题。对于一卡通系统来说，不同身份的用户其系统的功能权限、角色权限和数据资源权限都各有不同，统一授权管理实现了一卡通系统所有用户的权限分配，明确不同的人哪些可以做，哪些不能做，从而从源头开始杜绝人为因素对系统安全的威胁。

统一安全审计管理是 4A 管理的保障。统一安全审计是指对整个 4A 管理平台的所有部分进行审计，包括账号管理、认证管理和授权管理，通过统一安全审计，可以对 4A 管理平台内所有的人为操作以及系统事件进行记录，从而更好地保障 4A 管理平台整体的运行，解决了“你做了什么”的问题。

4　4A 管理平台工作流程

如上所述，4A 管理平台主要以“人”为对象，强调通过对人的身份、权限、行为的管理和审计，来确保系统的安全。

在一卡通系统的架构下，4A 管理平台的工作流程如图 3 所示。

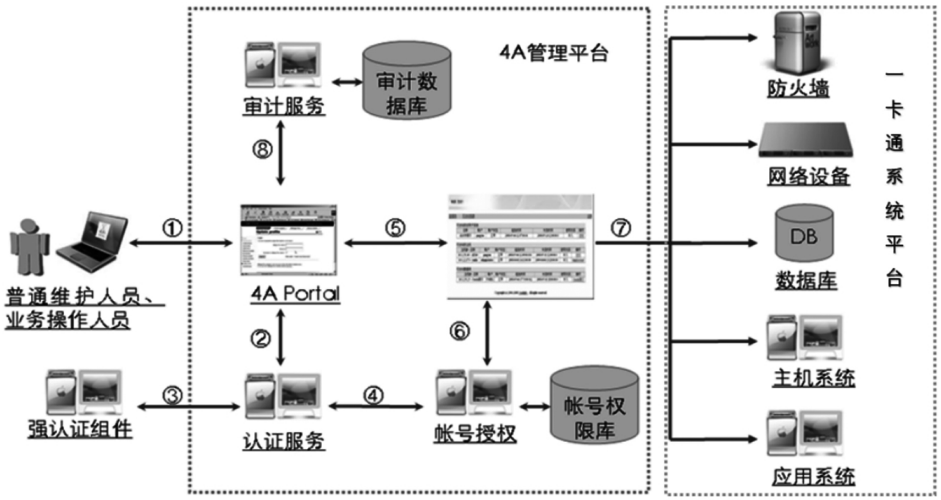

图 3　4A 管理工作流程图

对于一般教师、学生等用户，如果要查询一卡通相关业务，通常都是通过学校的数字化校园的统一的信息门户界面通过共享数据中心查询的，4A 管理平台主要是针对一卡通系统的普通维护人员和业务操作人员。

对于一卡通系统的普通维护人员和业务操作人员，要访问一卡通系统平台的资源，管理一卡通系统的各个应用，必须通过 4A 管理平台的工作流程，具体分为八个步骤：

(1)普通维护人员和业务操作人员必须登录统一的 4A Portal 认证界面。

(2)登录时，4A 认证界面会调用认证服务。

(3)认证服务会根据登录账户的类型确定是否要进行强制性认证，例如一般业务操作人员采用静态密码登录，普通维护人员采用动态口令登录。

(4)认证服务在确定认证组件后同时调用账户授权服务，从账户权限库中找到登录人员的账号权限信息，进行账号权限的分配。

(5) 普通维护人员和业务操作人员通过 4A Portal 认证界面认证后将会显示一个一卡通系统的资源门户网页。

(6)账号授权服务在接到认证服务的请求，从账户权限库中找到登录人员的账号权限信息后，会将普通维护人员和业务操作人员的对于权限信息反馈给一卡通系统的资源门户网页，在资源门户网页上展示所有符合该用户权限的一卡通资源。

(7)普通维护人员和业务操作人员通过资源门户网页可以访问和管理所需要的一卡通防火墙、网络、数据库、各个应用系统等系统资源。

(8)当普通维护人员和业务操作人员登录 4A Portal 认证界面时，4A 管理平台的审计服务也随之启动，对于进入 4A 管理系统的人员进行账号管理审计、账号授权审计、登录过程审计、身份认证审计和登录后行为审计，从而全方面监督管理 4A 管理平台里的所有过程。

4A 管理平台通过 8 个工作步骤，实现了对于一卡通系统的人员的安全管理和审计的作用，杜绝了因为人为因素对一卡通系统造成的安全威胁。

5　结　语

一卡通系统是高校的核心业务系统，其安全性和稳定性是学校所有事务正常运行的保证。传统的一卡通系统安全工作仅仅强调对“物”的防护，而忽略了对“人”的管理。4A 管理平台通过账号、认证、授权和安全审计的统一管理，实现了“人”对“物”最便捷、最合规的访问，是所有安全系统或设备中数量最大、最有效的安全系统。

主要参考文献

[1]史光耀. 校园“一卡通”系统方案设计及应用[D].北京：北京邮电大学，2010.

[2]蔡皖东.网络与信息安全[M].西安：西北工业大学出版社，2005.

[3]单晓毅，王鑫彦. 基于 4A 技术的统一身份管理在企业门户系统中的应用 [J].微型机与应用，2009，28(18)：71-74.