网络优先数字出版时间:2014-2-18
网络优先数字出版地址:http://www.cnki.net/kcms/detail/45.1075.N.20140218.1419.009.html
广西科学院学报 2014,30(1):12~15
Journal of Guangxi Academy of Sciences Vol.30,No.1 February 2014

广西电子政务外网政务部门数字认证服务体系设计
Design of Government Digital Authentication Service System in Guangxi E-government Extranet

文 静,李 森
WEN Jing,LI Sen

(广西经济信息中心,广西南宁 530022)
(Guangxi Economic Information Center,Nanning,Guangxi,530022,China)

摘要:【目的】设计与实现广西电子政务外网政务部门数字认证服务体系。【方法】依托广西电子政务外网和广西电子认证注册服务中心,设计政务部门数字认证服务体系,并提出各政务部门可根据自身需求和业务规模选择自行建设或辅助建设的方式实现认证服务体系。【结果】依据政务部门数字认证服务体系,各政务部门可以选择服务体系实现方式,在对其应用系统进行相应的安全整改后,与广西电子认证注册服务中心系统交互,完成身份认证、数字签名及电子印章等各种安全应用服务。【结论】数字认证服务体系的设计与实现能有效的解决身份鉴别及安全传输、数字签名等电子政务安全问题。

关键词:认证注册服务中心(RA) 数字认证 电子政务 目录服务系统
中图分类号:TP309 **文献标识码**:A **文章编号**:1002-7378(2014)01-0012-04

Abstract:【**Objective**】Guangxi e-government extranet government departments digital authentication service system is designed and realized.【**Method**】Based on Guangxi e-government extranet and Guangxi registration authority system, we design the digital authentication service system for government affairs department. Various government departments can choose construction or auxiliary construction mode to realize the authentication service system according to their own requests and scale.【**Result**】According to digital authentication service system of government department, various government departments can choose the service system and modify the application system. Then, through interacting with Guangxi registration authority system, the safety services such as identity authentication, digital signature and electronic seal can be achieved.【**Conclusion**】Digital authentication service system can solve the identity authentication and secure transmission, digital signature and other e-government security problems efficiently.

Key words:registration authority(RA),digital authentication,e-government,LDAP

【研究意义】随着电子政务信息化的飞速发展,各政务部门依托政务外网开展应用的业务系统越来越多,如何为这些应用系统的合法使用者提供身份鉴别和为系统数据交换提供安全可靠的传输,成为电子政务建设中亟需解决的问题。【前人研究进展】政务外网作为政府部门非涉密的业务应用专网,与政务内网物理隔离,与国际互联网逻辑隔离,主要用于运行政府部门不需要在电子政务内网上运行的业务和面向社会服务的业务[1]。国家政务外网建设了政务外网电子认证服务体系,目标是满足现阶段基于国家政务外网业务应用对身份认证的要求,在政务外网范围内提供电子认证服务[2]。【本研究切入点】本文依托广西电子政务外网和广西电子认证注册服务中心进行设计的政务部门数字认证服务体系,能对各政务部门应用在政务外网上业务

收稿日期:2013-11-27
修回日期:2013-12-20
作者简介:文 静(1980-),女,工程师,主要从事计算机网络与信息安全等方面的研究。

系统的用户身份认证和数据传输加密等方面提供安全保障。【拟解决的关键问题】通过探讨政务部门服务体系自行建设和辅助建设2种实现方式,对身份认证系统的实现进行举例说明,为政务部门构建数字认证服务体系提供依据。

1　服务体系设计

1.1　服务体系构架

国家政务外网广西电子认证注册服务中心数字认证服务系统(以下简称广西RA系统)作为政务外网认证体系在广西的延伸,按照国家政务外网的统一运行规范和要求,为全区政务外网用户提供数字证书服务,满足各级政务部门对电子政务应用业务系统安全运行的需要。广西RA系统依托国家政务外网电子认证系统(以下简称国家CA系统),采用基于数字证书技术的身份认证系统和国家政务外网电子认证管理认证策略进行建设和管理,由广西电子政务外网管理中心进行运维管理,可为自治区的政务人员提供数字证书服务,并通过本地的目录服务系统(Light weight Directory Access Protocol,LDAP),为本地的应用提供就近的证书、证书黑名单下载服务,是政务部门数字认证服务体系在广西电子政务外网的实现基础。如图1所示,广西RA系统的LDAP和国家CA系统的LDAP之间存在主从关系,广西RA系统的LDAP通过从国家CA系统的LDAP同步数据,发布数字证书和证书注销黑名单数据,为各业务应用提供数字证书校验依据。

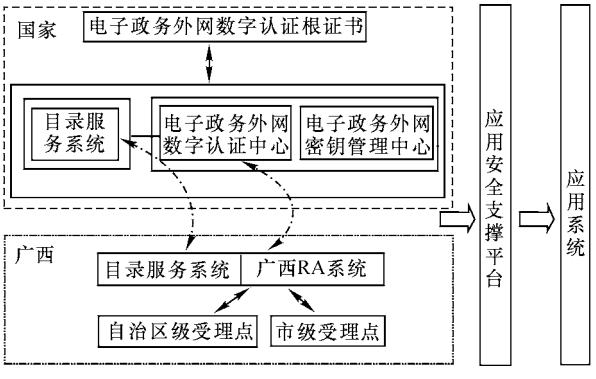

图1　广西RA系统逻辑结构

1.2　数字证书服务

广西RA系统与国家CA系统连接,提供基本的证书信息管理服务,包括注册、签发审核、证书签发、更新申请、更新审核、证书更新、废除申请、废除审核、证书废除、重发申请、重发审核、证书重发、信息注销。另外,还可以提供从目录服务、在线证书状态查询服务、时间源服务、时间戳服务等。

1.3　基于数字证书的应用

基于数字证书可开展的安全业务应用主要有:

(1)身份验证。包括应用系统用户身份验证和虚拟专用网络(Virtual Prirate Network,VPN)用户身份验证。应用系统用户身份验证是对登录用户的身份进行验证,判断是否为合法用户。将现有的"用户名+口令"的验证身份方式替换为"数字证书"方式。只有拥有合法证书的用户,才能登录到系统并执行相应的操作。VPN用户身份验证是根据国家电子政务外网安全建设要求,移动办公用户进入电子政务外网VPN专网时,必须使用数字证书进行身份验证。采用的任何VPN方式(包括SSL VPN和IPSec VPN等)都必须支持政务外网数字证书。

(2)单点登录。以数字证书为核心,以应用安全支撑平台提供的单点登录方案为基础,提供多样化、符合信息化现状的单点登录解决方案。

(3)授权管理及访问控制。基于数字证书建立授权管理系统,可以为政务外网用户、设备、服务器、机构等实体签发权限属性证书,并对属性证书进行发布和管理,为各项业务应用提供统一的权限管理和访问控制提供支持。

(4)数字签名。基于数字证书,提供数字签名、数字信封等服务,满足用户在政务应用中行为不可抵赖、信息完整性、私密性等需求。

2　服务体系实现

2.1　广西RA安全应用基础设施

基于广西RA系统,根据服务体系设计,广西电子政务外网管理中心进行了安全应用基础设施建设,包括身份认证系统、数字签名系统及电子印章系统,可以为广西各政务部门提供身份认证、数字签名及电子印章等各种安全应用服务。如图2所示,广西RA安全应用基础设施主要包括安全认证网关、数字签名服务器、电子印章系统和防火墙等。

2.2　政务部门服务体系实现方式

由于各政务部门的电子政务应用情况不同,数字认证服务体系的实现方式也不一样。一般可以分为2种情况:一是自行建设,适用于用户数量大、应用多且复杂的单位;二是辅助建设,利用广西RA系统的基础设施进行建设,适用于用户数量少、应用简单的单位。前者更灵活、安全和具有自主性,后者节省成本。

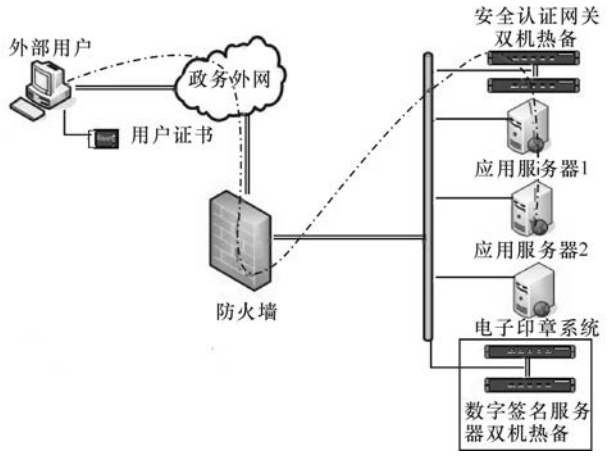

图 2 广西 RA 安全应用基础设施示意图

2.2.1 自行建设

政务部门单位根据需求自行采购安全认证网关、数字签名系统、电子签章系统等设备进行服务体系的建设,仅需要广西 RA 系统发放数字证书和提供有效证书列表。安全认证网关提供对外身份认证服务,同时支持基于 PKI/CA 数字证书和用户名/口令的身份认证方式,可单独使用也可组合使用。数字签名系统由数字签名服务器和数字签名客户端组成,均可独立提供数字签名、数字信封等服务。电子签章系统主要采用数字签名技术,实现在电子文档和电子表单上的电子签章和手写签名的功能。

政务部门端的安全认证网关和数字签名服务器需要从广西 RA 系统 LDAP 读取证书列表,故必须保证它们之间的互联互通。如图 3 所示,安全认证网关有串接和旁路 2 种部署方式,串接指在应用服务器之前的关键网络路径上部署,其部署更安全。旁路部署则比较灵活和方便。

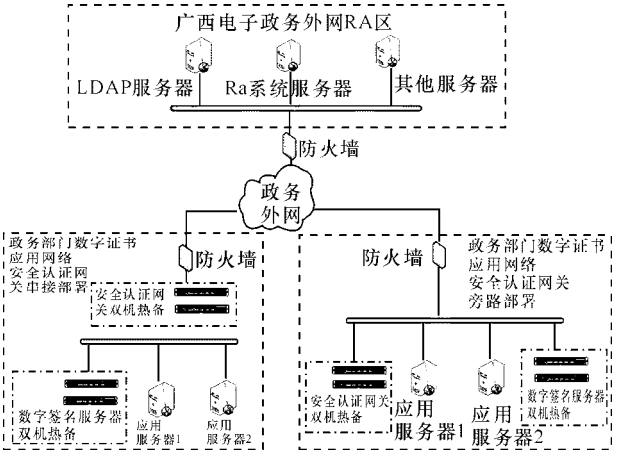

图 3 自行建设的系统部署示意图

2.2.2 辅助建设

政务部门利用广西 RA 安全应用基础设施提供的免费服务建设自己的服务体系,可以根据自身需要建设身份认证系统、数字签名系统和电子印章系统中的一项或多项。采用这种建设方式的政务部门需按照广西 RA 安全应用基础设施的管理办法进行建设,主要工作包括网络互连和应用接口开发。政务部门端的应用服务器必须与广西 RA 安全应用基础设施端的安全认证网关、电子印章系统和签名验证服务器进行通信,故必须保证它们之间的互联互通。应用服务器与广西 RA 安全应用基础设施端服务器之间的通信支持明文和密文(SSL/TLS)2 种方式,明文通信速度快,但没有密文安全,建议采用 SSL/TLS 加密通讯方式。应用接口开发需按照广西 RA 提供的开发文档进行应用系统的改造。

3 服务体系实现举例

如图 4 所示,各政务部门建设数字认证服务体系的身份认证系统,需要对其应用系统进行相应的安全整合,才能与广西 RA 系统交互,完成用户的身份认证。

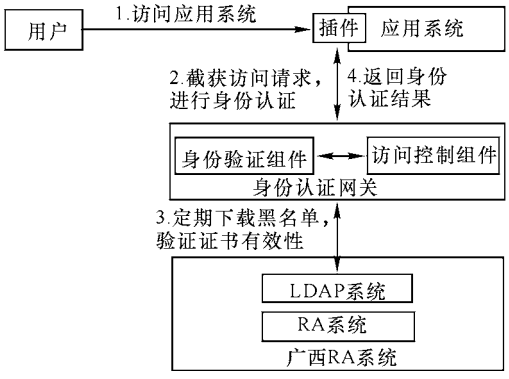

图 4 应用系统安全整合示意图

3.1 应用系统改造

改造方式具体有 3 种:①代理方式,指应用服务器端需安装过滤器插件,当用户访问应用时由过滤器转到安全认证网关作认证,此方式适合后台应用可以改造的情况。②模拟代填方式,指将服务器的策略下载到客户端来实现模拟代填,此方式适合零改造应用。③报文认证方式,指在应用服务器端向安全认证网关发送认证报文,网关认证后返回认证结果,此方式适合新建应用系统或应用系统前后台都可以改造的情况。

3.2 用户使用流程

各政务部门用户使用数字认证服务体系中的应用系统时,只需要启动客户端浏览器,在地址栏输入应用地址,应用将自动把用户请求重定向到安全认证网关;用户提交身份信息,若采用用户名/口令认

证,则输入用户名/口令信息,若采用证书认证,则选择可用证书;认证成功后,系统自动将用户重定向回应用并传递应用信息;用户可以进行正常访问操作。

4　结束语

政务部门依托广西电子政务外网开展信息化业务应用,建设相关的数字认证服务体系能有效地解决身份鉴别及安全传输、数字签名等电子政务安全问题,为电子政务建设提供有效的安全保障。目前已有部分政务部门按照本研究介绍的方式,依托广西 RA 系统构筑完成其自身的数字认证服务体系,在其内部业务系统应用效果良好。后续工作将考虑政务外网数字认证服务体系的统一管理规范和服务规范,努力满足政务部门的应用需求。

参考文献:

[1] 谈超洪,陈友初,李承林. 广西电子政务外网数据中心设计与实现[J]. 广西科学院学报,2008,24(4):364-366.

[2] 沈大风,吴亚非,任金强,等. 政务外网电子认证服务体系建设的思考与实践[J]. 电子政务,2010(7):44-49.

(责任编辑:陆　雁)

高端“外脑”助推广西科技水平上台阶

新闻时间:2014-1-13

主席院士顾问制度是我区于2009年启动的一项高端人才引进政策。记者1月8日从自治区科技厅了解到,启动自治区主席院士顾问制度5年来,广西先后聘请了116位两院院士担任自治区主席顾问。据不完全统计,5年来,院士顾问及其团队到广西考察、调研、指导、举办专题报告192人次,开展合作项目309项,指导申报国家级项目41项。在院士指导下广西获国家级各类平台18个,获得国家项目经费支持共5.81亿元。高端“外脑”的助力,全面提升了广西科技水平,为广西经济社会发展作出了重大贡献。

聘请主席院士顾问后,受聘的院士们高度关注广西经济社会的发展。他们积极建言献策,提供决策指导。其中针对“广西‘十二五’时期重大发展战略选择”、“广西应如何全面贯彻落实党的十八大精神,促进广西经济社会稳步发展,与全国同步全面建成小康社会”、“广西工业如何做大做强”等重大问题,院士们以书面形式向自治区党委、政府提出了宝贵的建议意见,为党委、政府的科学决策提供了强有力的智力支持。

在指导产业发展,助推广西经济结构升级方面,受聘院士顾问覆盖了广西食品、汽车、石化、电力、有色金属等千亿元产业。他们积极参与制定产业发展战略,解决重大关键技术难题,指导企业进行新技术、新产品的研发。其中,在机械产业领域,院士协同广西科研团队对广西的预应力锚具技术进行攻关,使广西的技术水平达到了国际领先水平,具有自主知识产权的预应力结构智能化监测等一批成果已应用于国内外80多项重大工程,产生了良好的经济效益,提升了广西预应力锚具的国际竞争力。在院士顾问的带领和指导下,广西在航空铝合金材料与加工技术、交通运输高端铝合金材料等方面得到突破性进展,广西团队能承担国家重大工程用高端铝合金材料的研发,为重大交通运输工程的核心客户长期提供具有高综合性能的产品,使广西铝业产品实现了初级产品加工到高端产品生产的转化升级。

而在农业领域,4年来,有13名农业院士顾问及团队专家到广西考察、调研、指导120多次,举办专题报告72场,交流座谈64次,对接单位上门交流50多次,合作项目45项,引进新技术18项、新品种83个,指导建设基地106个。推动了水稻、玉米两个产业“分中心”的建设以及两个国家综合试验站和1个自治区重点实验室、12个国家级科学观测站的建立,使广西从农业大省向农业强省迈出了坚实步伐。

院士们的加盟和支持,还促进了广西科研平台和人才团队的建设,提升了广西整体研究水平。在院士顾问的大力支持和推荐下,广西引进了国家千人计划获得者、国家杰出青年基金获得者、长江学者等一批高水平高层次人才,同时广西本土一批人才团队也得到锻炼成长,高层次人才的建设格局不断得到优化。

(摘自《广西日报》)