电子政务外网安全支撑平台模型①

张元金

(广东肇庆广播电视大学, 肇庆 526060)

摘 要: 电子政务外网是展示政府形象、服务百姓的一个窗口, 目的是资源共享、高效便民, 显然安全问题尤为重要. 为解决政务外网的安全问题, 从技术层面上提出了一套电子政务外网构架的安全系统设计方案. 分析表明, 采取应用密码服务、统一用户管理、统一身份认证、统一资源与授权管理等一系列安全举措, 可以有效保证政务外网的安全可靠.

关键词: 信息化; 电子政务; 身份认证; 数据中心

Platform of E-Government Extranet Security Support

ZHANG Yuan-Jin

(Guangdong Zhaoqing TV University, Zhaoqing 526060, China)

Abstract: E-government extranet is a window to display the image of the government, service people. Its purpose is resource sharing, efficient convenience, the security is particularly important. In this paper, in order to solve the security problem of e-government extranet, we put forward the design scheme of security system. Analysis shows that, by applying cryptographic service, unified user management, unified identity authentication, unified resource and authorization management and a series of safety measures can effectively guarantee the safety and reliability of e-government extranet.

Key words: informationization; e-government; identity authentication; data center

1 引言

电子政务是伴随着社会的信息化而产生的. 随着电子政务以及网络技术和通讯技术的完善, 政府也在向着办公自动化, 部门信息传递网络化, 公共服务在线化, 政府资源高度共享发展[1]. 而政务外网建设是政府系统信息化建设的基础, 它为政务部门的业务系统提供网络、信息、安全等支撑服务, 为老百姓提供政务信息服务. 现阶段还有许多政府职能部门的工作还沿用传统的面对面服务, 效率低且不说, 还存在很多无法协调的问题. 为了尽快实现政府办公的信息化进程, 加强政府与老百姓的沟通交流, 保证高效便民的电子政务工作能顺利开展, 建设安全可靠的电子政务外网很有必要. 电子政务外网的搭建设计方案也成了近年来的研究热点. 针对目前政府部门的办公现状, 提出一种电子政务外网安全支撑平台的设计方案[2].

2 安全应用支撑平台系统设计

2.1 应用密码服务系统模型

密码服务系统为安全应用支撑平台中各个系统提供基础密码服务. 实现客户端密码设备、认证设备及服务端密码设备的接入和资源管理、调度, 为各类应用系统提供支持 Windows、Linux 等主流操作系统平台和 J2EE、.Net 等多种基础架构平台的密码服务接口[3].

密码服务系统由客户端和服务端密码设备、密码服务调度管理和密码服务接口软件模块、密钥管理服务接入模块组成. 其中密码设备包括集中密码服务设备、单机密码服务设备(如服务器密码机、PCI 密码卡和 USB 密码机)等, 认证设备包括 Usbkey 和认证卡等产品.

集中密码服务设备采用服务调用或服务代理方式

① 收稿时间:2014-02-28; 收到修改稿时间:2014-03-24

提供密码服务, 为本安全域内分布的主机(网络信任设备、应用服务器、客户端)在线提供密码支持, 包括数据加解密、数字签名、签名验证、数据摘要和完整性验证、随机数生成等密码支持服务.

单机密码服务设备(如 PCI 密码卡)采用代理或接口调用方式为主机提供密码服务, 包括数据加解密、数字签名、签名验证、数据摘要和完整性验证、随机数生成等密码支持服务, 如图 1 所示.

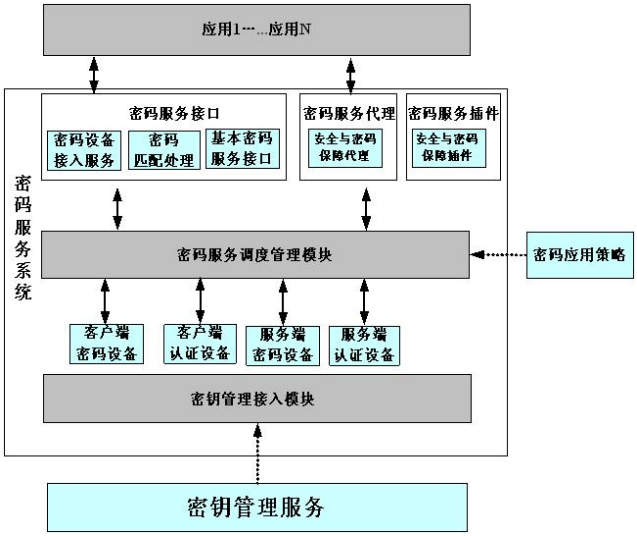

图 1　密码服务系统结构模型

2.2 统一用户管理系统模型

为保障政务系统的安全正常使用和信息的一致性, 需要将分散的用户信息整合集中进行统一管理. 统一用户管理系统是对信息系统中的用户身份进行统一管理的信息系统. 统一用户管理结合电子认证基础设施, 通过体系一致的用户管理系统, 对各类应用系统所需要的用户信息进行统一管理, 提供用户信息同步、用户属性管理、用户身份管理和用户群组管理等功能, 对不同安全域的用户信息进行同步, 保障用户身份的安全和一致性[4].

统一用户管理系统提供用户、应用、资源等的注册和管理功能, 以及用户属性与证书的绑定功能. 采用分级部署和分级管理, 遵循 “谁的用户谁管理, 谁的资源谁授权”的原则, 各部门设置相应的管理人员对信息进行管理, 实现信息的汇总, 为统一认证系统提供数据支撑, 如图 2 所示.

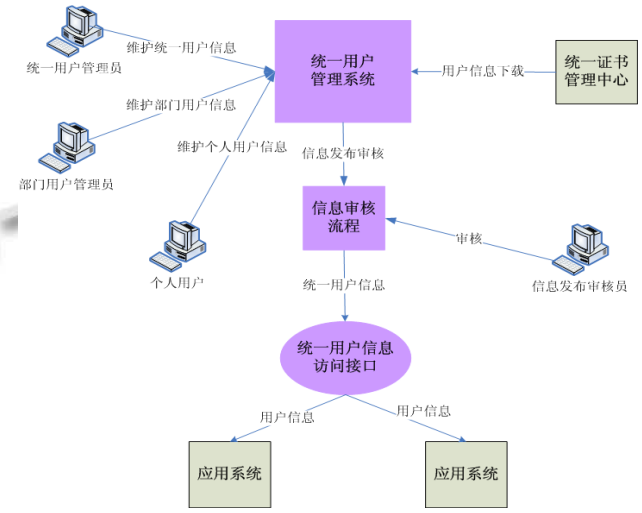

图 2　统一用户管理系统结构模型

2.3 统一身份认证系统

统一身份认证, 是判断一个用户是否为合法用户的处理过程, 它主要为用户提供基于数字证书的身份认证和多应用系统的登录功能. 统一身份认证服务系统的一个基本应用模式是统一认证模式, 它是以统一身份认证服务为核心的服务使用模式. 用户登录统一身份认证服务后, 即可使用所有支持统一身份认证服务的管理应用系统. 身份认证服务包括的功能[5], 如表 1 所示:

表 1　身份认证服务功能表

序号	主要功能项	功能描述
1	通信服务	接收客户端上传的身份认证请求, 对其身份进行有效性验证, 并返回验证结果. 接收应用服务器端对认证票据的有效性核查(应用服务器也可以自行验证票据).
2	验证证书有效性	验证客户端接口上传到认证服务器(或是认证网关)的证书, 检查证书是否过期、是否合法的颁发机构所颁发、是否被吊销.
3	查询证书状态	通过从目录服务(LDAP)查询下载 CRL 或是利用 OCSP 服务验证证书是否被吊销, 为证书验证模块提供依据.
4	票据管理	若用户身份验证有效, 系统将为没有用户产生一个合法的票据, 并在系统中进行维护管理, 为应用应用系统提供查询判定依据.

5	认证客户端	部署在用户终端, 部署在用户终端的客户端工具将采集用户的身份信息(含证书), 上报服务器进行身份验证. 客户端将定期访问服务器, 更新认证票据.
6	客户端接口	由应用服务器调用, 通过访问认证服务器实现对票据的合法性验证.

2.4 统一资源与授权管理系统模型

统一资源及授权管理服务由资源管理、角色管理、策略管理、授权(权限)管理、策略/权限发布服务、鉴权服务等多个部分组成. 资源管理实现对应用资源的统一管理, 为授权提供基础数据. 角色管理根据人员的职务、密级等进行分类后抽象出统一的角色, 实现角色增、删、改、查等管理功能[6].

授权管理是系统的核心, 将用户身份与角色进行绑定, 为访问控制裁决提供依据. 统一资源及授权管理服务逻辑结构如图 3 所示:

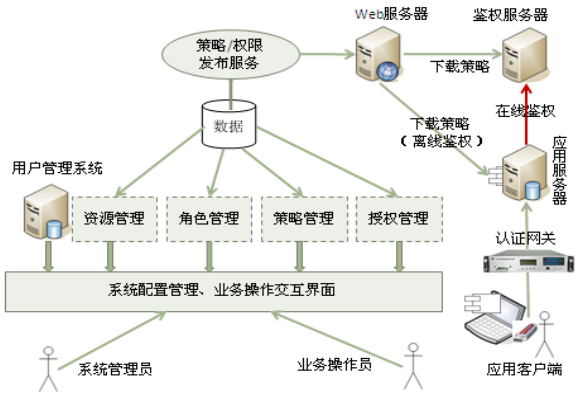

图 3 统一资源及授权管理系统逻辑结构模型

统一资源及授权管理服务主要包括以下功能, 如表 2 所示:

表 2 统一资源及授权管理服务功能表

序号	主要功能项	功能描述
1	资源管理	提供资源注册、修改、删除功能. 资源可按安全等级进行分类管理. 系统支持资源的树型管理. 资源可以为应用资源(文件、URL、数据库表、记录以及应用的菜单、按钮、表格等)和网络设备资源(IP 地址、端口号).
2	角色管理	可以根据人员的职务、密级或是根据资源的权限设置不同的逻辑角色. 系统支持角色的增、删、改操作.
3	权限(授权)管理	将用户身份与角色进行绑定. 系统也可以支持将角色与资源绑定.
4	分布式授权(委托授权)	资源管理员可以将自身所拥有的资源委托给下级管理员进行授权.
5	策略管理	授权和权限裁决按照什么策略进行, 需要统一制定和发布.
6	权限及策略发布	授权的结果或鉴权裁决的策略将以安全的方式在目录服务或是 WEB 服务器发布, 对应用系统或鉴权发布提供查询下载.
7	鉴权服务(权限裁决)	裁决用户是否具有访问指定资源的权限, 为应用系统提供用户访问资源的依据, 从而实现访问控制. 鉴权提供离线(在应用服务器上鉴权)和在线鉴权(通过鉴权服务器进行鉴权)两种方式.
8	客户端接口	应用系统通过客户端接口访问鉴权服务.
9	系统配置管理	实现对系统进行配置和管理.

2.5 访问控制系统模型

身份认证一般与访问控制是有联系的, 访问控制是指根据用户的身份及访问权限, 依据对它的授权执行业务过程、访问资源, 实施资源访问控制, 资源访问控制涉及的主体包括用户、应用系统、设备和进程等, 资源访问控制涉及的客体包括应用系统、业务功能、文件夹、数据库、设备和进程等, 资源访问控制涉及的业务过程包括访问、发布、查询、创建、读写、修改、删除、发送、接收、审批、打印、交换等. 在用户访问业务应用时, 通过身份鉴别后, 访问控制系统根据用户不同粒度的权限配置策略, 对用户所能访问的系统和具体功能进行判定, 实现按需互通和受控访问[7].

通过应用密码安全保障系统的粗粒度访问控制结合应用系统自身的细粒度访问控制, 实现完整的应用系统资源访问控制, 访问控制系统结构如图 4 所示.

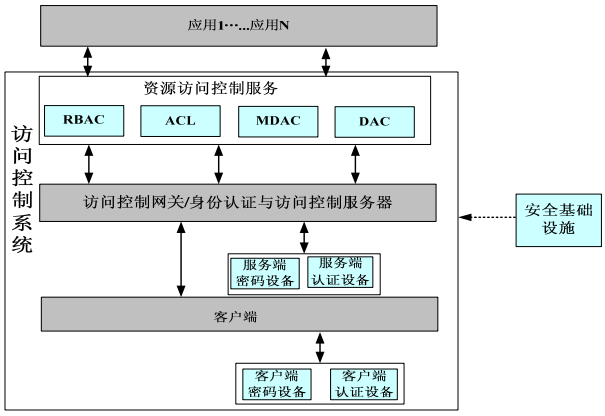

图 4 访问控制系统结构模型

2.6 统一安全审计和责任认定

安全审计系统对用户访问资源(应用主机、应用和安全域)的行为进行记录和审计, 对违规操作提供责任认定依据, 并制定审计数据上传到审计中心的接口和数据规范, 对审计信息进行授权访问控制, 保证审计记录不被篡改、伪造和非授权删除, 为系统的安全状态监控、故障快速定位、事件关联分析、系统分析报表等提供技术支撑.

对审计信息进行授权访问控制, 保证审计记录不被篡改、伪造和非授权删除, 对审计记录的操作记录日志. 审计记录包括时间、地点、类型、主体、客体和结果等情况, 及时发现违规行为和追查事故原因, 生成多种类型的审计报告, 为安全事件分析和责任认定提供依据, 如图 5 所示:

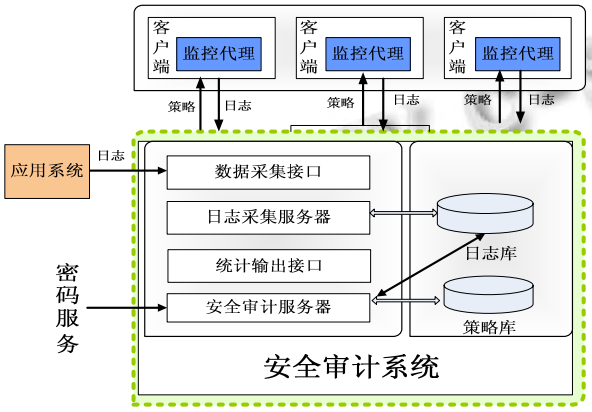

图 5 安全审计系统组成图

3 支撑平台的安全性分析

安全系统建设是电子政务外网建设的重要组成部分. 通过对电子政务外网平台的运行测试, 确实能保障应用系统和信息资源的安全, 实现安全和密码保障与应用的紧密衔接, 降低应用安全实现的难度、建设周期和实现成本, 实现可信、可核查、可评估和持续改进的应用安全支撑. 具体安全保障实现如下:

(1)构建统一的安全应用支撑平台, 为政府外网应用提供安全统一、符合标准、可动态配置、可伸缩、可扩展的, 标准、规范、统一的安全服务, 充分保障应用系统的安全和信息资源的保密. 安全平台提供包括统一用户管理、身份认证、授权访问控制、责任认定和加解密等服务. 形成应用集成基础技术环境, 实现能够为按需定制的应用集成提供服务体系. 实现网络政务资源安全、可信、可控的共享应用.

(2)建设电子认证基础设施, 通过证书注册和查询验证系统, 接入政府二级认证结点或上级电子认证结点, 为全市电子政务内网提供统一的数字认证管理和服务.

(3)建设密钥管理基础设施, 为系统内部署的密码设备提供统一的密钥服务, 对密码、密钥、密码策略和密钥设备实施集中统一管理.

该方案设计的电子政务平台已经投入使用, 经验证, 平台运行稳定, 安全性能良好, 既提高的政府工作效率, 又方便了百姓办事, 该方案达到预期的效果.

4 结论

以上论述了电子政务的安全系统中安全应用支撑平台的建设模型, 该模型有较高的技术先进性和可实施性. 在电子政务网络中进行的一系列的安全措施: 应用密码服务、统一用户管理、统一身份认证、统一资源与授权管理、访问控制系统、统一安全审计和责任认定等, 是目前实际网络应用中常用的手段, 能较好地保证电子政务网中各种的安全运行. 电子政务外网作为我国电子政务网络的重要基础设施, 是提高机关工作效率和公共服务水平、推进行政管理体制改革的重要保障[8]. 加快建设政务外网, 对于贯彻落实科学发展观, 构建社会主义和谐社会, 增强各级政务部门的执政能力, 提高执政水平、构建服务型政府都具有十分重要的意义[9].

但是公网网络环境的复杂多变, 以及很多信息系统的脆弱性, 决定网络安全威胁一直客观存在, 我们应该从技术层面和管理层面做好防范, 最大限度地保障政府的电子政务外网安全畅通, 保证我国政府工作

便捷快速有序地开展.

电子政务系统是我国信息化战略的实施重点, 而其安全体系的设计又是重中之重. 本文着重论述了电子政务系统中安全应用支撑平台方案设计, 可为构建安全高效的电子政务系统提供技术参考[10].

参考文献

1 许晓晓,步坤.电子政务与服务型政府.中国电子商务,2013,(20):63–64.

2 袁翔. 基于 J2EE 的综合管理信息系统.计算机系统应用,2013,22(10):69–73.

3 张晓枫.政府信息化建设研究.信息系统工程,2013,(10):134–134.

4 周安民. 电子政务信息网络安全.信息安全与通信保密,2013,(7):24–25.

5 邝岩,孔凡晶.电子政务中引入电子商务信誉模型研究.现代情报,2013,33(9):157–160.

6 李东,刘西林.基于 SOA 的电子政务个性化信息服务模型.科技管理研究,2013,33(24):219–222.

7 贾文伟,徐光宪.体育电子政务平台软件方案理想解评价方法.计算机技术与发展,2013,23(12):124–127,138.

8 王绪宛,雷蕾.区县级电子政务系统的设计与实现.微型电脑应用,2013,(11):43–45.

9 陈氢.基于信息链的跨部门政府信息共享架构研究.情报杂志,2013,32(11):164–168.

10 樊钉.信息熵视角下的电子政务建设.河北大学学报(哲学社会科学版),2013,(5):123–125.