

电子政务系统支撑平台架构研究及应用

张迪¹ 李泽椿² 傅德胜³ 于新文²

摘要

提出了一种针对电子政务系统建设的应用支撑平台的架构模型.该应用支撑平台,在授权管理、 workflow 系统及系统授权机制等方面为应用系统的完善和扩展提供统一标准和有力支撑.实践证明,应用支撑平台有效地支持了电子政务应用系统的快速开发、灵活部署和高效安全运行.

关键词

电子政务;应用支撑平台;授权管理; workflow; 授权机制

中图分类号 TP311.52

文献标志码 A

0 引言

Introduction

电子政务应用支撑平台是从政府业务流程中提炼出各相关职能部门公用的数据及相应的数据处理服务,构建以业务为中心的系统,实现统一数据采集、存储和访问机制.电子政务应用支撑平台的建设,可以缩短项目上线周期,提高项目质量,降低项目风险,同时为应用系统的完善和扩展提供统一的标准,在源头上最大程度地消除信息孤岛.

1 应用支撑平台总体设计

Overall design of application support platform

1.1 应用支撑平台总体体系结构

应用支撑平台提供包括服务层、应用层和展示层 3 个层面的服务,总体体系结构如图 1 所示.

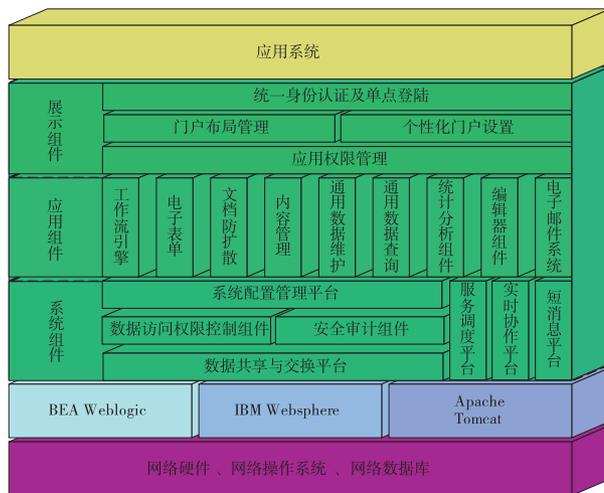


图 1 电子政务应用支撑平台总体体系结构

Fig.1 Overall architecture of application support platform for e-government system

收稿日期 2009-06-22

作者简介

张迪,女,博士生,研究方向为电子政务、软件开与管理、防灾减灾中的信息技术. zhangdi@cma.gov.cn

李泽椿,男,工程院院士,主要研究方向为应急技术、数值预报

1 南京信息工程大学 大气科学学院,南京,210044

2 中国气象局,北京,100081

3 南京信息工程大学 计算机与软件学院,南京,210044

1.2 系统管理组件

系统管理组件是整个系统建设的基础,包括用户组织机构建模、资源权限管理、数据和日志管理等基础组件,借助于这些基础的组件产品可以快速构建新的系统以及对旧的业务系统进行调整.系统管

理组件主要包括以下内容。

1.2.1 用户组织机构建模

它实现了对机构、人员、角色信息及其相关关系信息的描述和定义。机构配置管理主要用于定义部门的组织机构图,通过定义部门的属性及其之间的关系,可以形成树状组织机构图,机构配置中包含部门名称、部门简称、部门编号、部门排序号、所属部门及职能、电话等部门的描述性内容;人员配置主要定义人员属性,包含人员 ID、人员编号、所属部门、拥有角色、替代人员及房间号、电话等个人的一些描述信息;角色配置用于映射实际组织机构中的岗位,角色定义主要与权限管理相联系,授权通常要到角色,这里定义的角色主要是一个统称,比如处长等,并不代表真实的岗位,只有将他与部门机构关联后才能具体代表某一个真实岗位,这种关联关系在人员配置管理中进行体现。

1.2.2 资源管理

主要对模块、标签、页面、操作按钮等系统的组成元素进行配置。通过资源管理可以描述系统内容的组织层次结构,通过定义资源的分组和分层结构,使资源体现在导航界面时按照配置好的层次管理展现。资源配置管理增强了系统的灵活性和可扩充性,实时将开发完成的模块发布到系统中。

1.2.3 权限管理

主要用于对系统模块集中进行授权,通过该模块可以直接定义数据库的人员、角色、权限以及对应关系,该配置将管理集中化,便于进行集中控制。

1.2.4 数据字典管理

主要定义枚举字段包含的值,如:类型、职称等,这里将系统涉及的所有关键字进行集中维护,增强了系统的一致性。通过将系统涉及的关键属性值参数化,可以极大增强系统的灵活性、健壮性和可扩展性。

1.2.5 个性化设置。

主要为普通用户进行个性化的设置提供途径,主要包含单位、地址、电话号码、传真号码等个人自己维护的常用信息;出差时用于移交工作的出差授权配置;用于更改用户登录帐户和口令的帐户更改管理。

1.3 统一认证授权组件

主要基于统一用户管理、政府公钥技术设施、策略管理系统,提供单一认证机制、权限管理、加密管理和审计机制。所有应用系统都通过该模块获得认证和全局的权限信息,并对其行为进行审计。系统在

统一的位置存放用户信息、访问控制列表(即 ACL)和数字证书,对于每种资源都定义了可以执行的权限。ACL 表里记录了用户对每个资源的访问权限。用户在访问系统的时候要提供凭证,该凭证可以是传统的口令,也可以是数字证书。认证系统通过 ACL 检查对某种资源的访问权限。对资源的所有操作需要通过审计子系统记录安全审计信息。

1.4 安全审计组件

对数据管理过程中发生的任何动作进行自动记录监控。在利用数据库日志的基础上,提供独立的审计管理平台,并将审计记录布置在应用层,这与布置在数据层上的数据库日志形成互补性支持。审计记录构件自动拦截用户的所有操作需求,以及操作过程与数据库的反馈信息,实时动态记录,建立审计日志数据库,日志的纪录内容包括登陆信息、数据操作信息及错误相关信息。

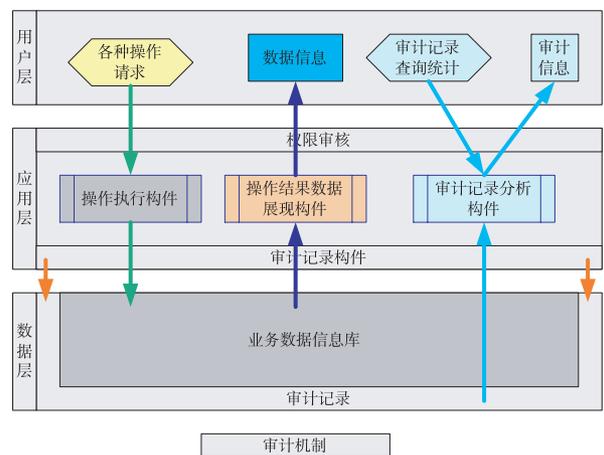


图2 电子政务应用支撑平台安全审计组件结构

Fig.2 Security audit component structure of application support platform for e-government system

1.5 数据访问组件

为系统实现跨数据库访问提供支持。数据访问组件内置对多种数据库的访问适配器,可以通过切换设置开关使系统和多种数据库互连。通过数据访问组件,可以使系统建立在异构的数据库基础上,实现跨数据库应用。

1.6 数据交换组件

为系统提供分布式系统部署和与其他系统互连的能力,通过数据交换组件可以实现分布式系统之间的数据传递和交换。交换格式采用国际通用的 XML 格式。内置数据的加密和解密操作,对传送数据的加解密过程,采用事务处理及回滚策略,防止意

外发生时产生的数据丢失和误操作.

1.7 workflow 系统

包括 workflow 引擎、workflow 定义和管理工具等部分,提供标准的 API 接口. workflow 管理系统定义工作的流转路径以及每个步骤的执行人,与外部的应用进行集成,使不同的系统可以共享 workflow 引擎,具有统一的待办工作、流程跟踪等功能.

1.8 电子表单系统

采用 XML 描述表单外观和表单数据. 图形化的电子表单设计工具,可以通过鼠标拖拽的方式设计电子表单,具有强大的编辑功能,能够设计出丰富格式的电子表单,同时,能够支持计算、校验的设置和脚本的开发. 电子表单系统结构如图 3.

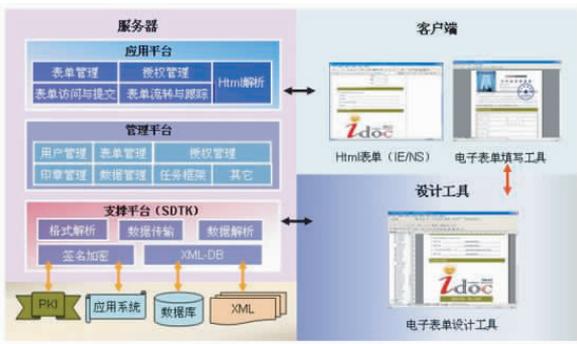


图 3 电子政务应用支撑平台电子表单系统结构
Fig.3 Electronic form framework of application support platform for e-government system

1.9 编辑器组件

编辑器组件可以无缝和 MS Office 进行集成. 通过编辑器组件的嵌入可以让用户在不脱离操作界面的情况下对文件进行编辑,所有修改过程都保留修改痕迹. 系统的清稿功能可以将所有痕迹隐藏,方便进行文件阅读. 配合服务器的数据接收服务,点击保存时,编辑的文档将自动被保存到服务器或数据库中. 编辑器组件对外留有多个接口,方便对文件内容进行控制.

1.10 数据检索统计配置组件

根据系统的数据字典,为用户提供动态的数据查询检索,统计配置手段,使得用户能简单地自由定义任意方式组合的查询、统计条件,指定查询、统计的数据源和相关字段,支持全文检索、追加检索、多关键字组合检索等. 用户可定义查询、统计结果的报表样式. 根据用户的配置自动生成查询、统计语句,将数据结果按照用户定义的方式进行展示. 用户可以保存自定义的配置结果,以备日后使用. 数据查

询、统计的结果将可以打印,并可以支持包括 EXCEL、HTML、TXT 等格式的输出.

1.11 统一消息平台

为用户搭建了一个全方位、立体式的消息传输通道,用户可以点对点、点对面进行消息沟通. 其他系统的消息(待办提醒、订阅信息、通知等)可以通过消息平台发送到用户的多种客户端(协作客户端、邮箱、手机等). 统一消息平台支持 HTTP、HTTPS、RMI、SMTP、SOAP 等多种传输协议,支持 WEB SERVICES,支持 CA 证书及 SSL 链路加密及对关键数据的签名和加密.

2 应用支撑平台关键技术

Key technology of application support platform

2.1 授权管理

采用系统管理、人事管理、业务授权管理三权分离的原则,不同类型的权限管理工作可以由三类角色的用户分别完成,整体结构如图 4.

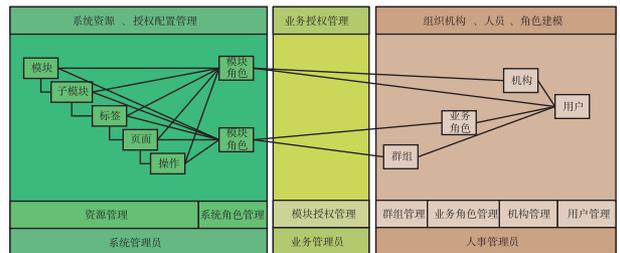


图 4 电子政务应用支撑平台权限管理系统结构
Fig.4 Authorization control framework of application support platform for e-government system

系统管理员负责资源配置、系统角色管理及相应的权限设置. 资源配置是将系统中的所有资源(模块、子模块、标签、页面、操作)配置到系统中,并按一定的关系组织起来;系统角色管理是为各模块创建系统角色,系统角色与具体人员及业务无关. 权限设置是通过设立系统角色和资源的对应关系完成系统级的授权工作.

人事管理员负责人员注册、部门调整及岗位信息的配置.

业务管理员负责完成具体的授权工作,可以指定某类用户在具体模块中具有的权利. 每类权限管理都可以实现逐级授权.

通过上述的授权机制良好解决了资源和人员之间复杂的对应,极大降低系统维护的复杂度,并通过多岗位相互制约提高了系统的安全性.

2.2 workflow引擎技术

workflow引擎包括数据模型及控制模型2个部分.

数据模型包括机构模型和信息模型. 机构模型描述的是单位或者部门的组织机构关系, 包括部门信息、工作组信息、人员信息、角色信息; 信息模型定义workflow引擎中的各种控制数据, 包括业务过程信息、业务活动信息、业务活动前依赖规则、业务活动后流转规则、任务指派规则、人员任务列表、人员已完成任务列表. 通过数据模型, 可以方便地描述关键业务的业务规则、活动的依赖关系以及任务的指派等特征. workflow系统提供上述信息的定义和维护功能.

控制模型将机构模型和信息模型有机地结合在一起, 根据定义的业务规则对业务过程中的各项业务活动的流转以及任务指派等工作进行控制和协调. 控制模型是workflow引擎的控制中心, 提供系统调度、任务管理、任务指派、依赖检查、转发控制等功能. 机构模型和信息模型通过可视化建模工具实现, 是workflow引擎构造时的定义中心; 控制模型通过引擎控制器实现, 是workflow引擎在运行时的控制中心. workflow引擎系统体系结构如图5.

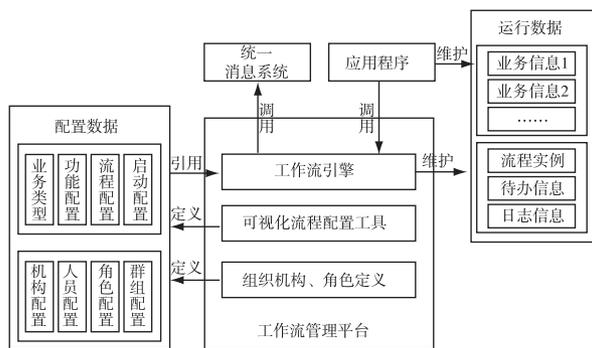


图5 电子政务应用支撑平台workflow系统体系结构

Fig. 5 Workflow framework of application support platform for e-government system

通过上述workflow引擎技术, 提高了政务管理的灵活性和适应性, 可平滑实现组织结构调整和业务流程变更, 降低政务业务改革成本, 同时可以量化考核每个处理环节的效率, 为提高流程执行力和绩效管理提供技术保障.

2.3 系统授权机制

授权机制采用基于角色的访问控制、强制安全策略和应用系统内部授权机制3种方式.

2.3.1 基于角色的访问控制(RBAC)

目录服务中保存统一的ACL信息, 记录用户或

角色对资源的访问权限, 相应的UML模型如图6. 在图6的模型中, Principal表示可授权的对象, 用于授权、认证; User表示用户, 用于授权认证; Group表示用户组, 用于授权认证, 组中可以包含组, 也可以包含用户; ACL表示访问控制列表; ResourceType表示资源类型, 相同的资源类型具有相同的permission集合. 授权可以基于用户, 也可以基于角色. 一个用户的权限是直接对他本人的授权以及他所属于的角色的权限的总和.

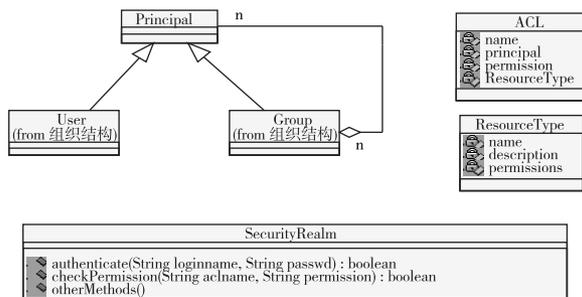


图6 电子政务应用支撑平台权限设置模型

Fig. 6 Authorization deployment model of application support platform for e-government system

2.3.2 强制安全策略

系统管理员可以在系统一级添加强制的权限控制措施, 如本单位的某类文档一定不允许共享给其他单位等. 强制安全策略和基于角色的授权配合使用, 形成更加严密的授权方案.

2.3.3 应用系统内部的授权机制

上面的两种机制提供的是对公共资源(功能、统一的文档库等)的授权. 应用程序在业务逻辑内可以有自己的权限管理, 这些信息由应用程序分别管理.

通过上述授权机制, 简化了权限管理, 避免直接在用户和数据之间进行授权和取消; 有利于合理划分职责, 用户只有其所应具有权限, 避免越权行为; 为应用系统的分级管理提供技术支撑.

3 结论

Conclusion

本文设计的电子政务应用支撑平台, 在中国气象局电子政务系统建设中得到了很好的应用. 实践证明, 应用支撑平台有效地支持了电子政务应用系统的快速开发、灵活部署和高效安全运行, 整合了系统内各应用系统和数据资源, 满足了信息共享、业务联动、标准统一和流程规范的需求, 架构了一体化的电子政务综合处理平台. 在具体的开发和应用过程

中,还应进一步建立健全科学管理体系、安全保障体系和运行管理体系,为电子政务的持续发展和规范运作提供服务和保障.

参考文献

References

- [1] Hsinchun B. Digital government; e-government research case studies and implementation [M]. New York: Springer, 2008: 615-645
- [2] Ozel S A, Altıngöde I S, Ulusoy O, et al. Metadata-based modeling of information resources on the web [J]. Journal of the American Society for Information Science and Technology, 2004, 55 (2): 97-110
- [3] Zachman J A. A framework for information systems architecture [J]. IBM System Journal, 1987, 26 (3): 276-292
- [4] 毛才高,倪春洋,黎连业. 电子政务系统建设与实施 [M]. 北京: 科学出版社, 2007: 11-24
MAO Caigao, NI Chunyang, LI Lianye. Development and implementation of e-government system [M]. Beijing: Science Press, 2007: 11-24
- [5] 范玉顺. workflow 管理技术基础: 实现企业业务过程重组、过程管理与业务过程自动化的核心技术 [M]. 北京: 清华大学出版社, 2001: 133-151
FAN Yushun. Basis of workflow management technology—core technology on achievement of business process reengineering, process management and business process automation [M]. Beijing: Tsinghua University Press, 2001: 133-151
- [6] Wil van der Aalst, Kee van Hee. Workflow management: model methods and system [M]. Beijing: Tsinghua University Press, 2004: 216-236

Study and application of support platform architecture for e-government system

ZHANG Di¹ LI Zechun² FU Desheng³ YU Xinwen²

1 Graduate School in Nanjing University of Information Science & Technology, Nanjing 210044

2 China Meteorological Administration, Beijing 100081

3 Department of Computer Science and Technology in Nanjing University of Information Science & Technology, Nanjing 210044

Abstract In this paper, a kind of architecture model of application support platform for e-government system is presented. The application support platform provides uniform standards and strong support for improvement and expansion of the application system in areas of authorization management, workflow system and authorization mechanisms. It has been proved by practice that the application support system can provide effective support for the e-government application system in terms of its rapid development, flexible deployment, and efficient and safe operation.

Key words e-government; application support platform; authorization management; workflow; authorization mechanism