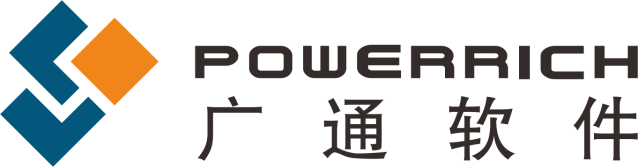
**智慧城市运营中心(IOC)共享交换模块**

**项目建议书**

****

深圳市广通软件有限公司对本文件资料享受著作权及其它专属权利，未经书面许可，不得将该等文件资料（其全部或任何部分）披露予任何第三方，或进行修改后使用。

二〇一九年四月

**目录**

[第一章 项目概况 5](#_Toc5284452)

[1.1 编制单位 5](#_Toc5284453)

[1.2 项目背景 5](#_Toc5284454)

[1.3 建设目标 6](#_Toc5284455)

[1.4 建设内容 7](#_Toc5284456)

[1.5 建设依据 8](#_Toc5284457)

[1.6 建设原则 9](#_Toc5284458)

[第二章 需求分析 11](#_Toc5284459)

[2.1 政务信息资源共享交换平台需求分析 11](#_Toc5284460)

[2.1.1 目录系统需求分析 13](#_Toc5284461)

[2.1.2 交换系统需求分析 18](#_Toc5284462)

[2.2 综合门户需求分析 25](#_Toc5284463)

[2.2.1 CA认证管理需求分析 25](#_Toc5284464)

[2.2.2 LDAP认证需求分析 25](#_Toc5284465)

[2.2.3 应用系统集成 25](#_Toc5284466)

[2.2.4 信息集成 26](#_Toc5284467)

[2.2.5 门户定制 26](#_Toc5284468)

[2.2.6 内容管理 26](#_Toc5284469)

[2.2.7 用户同步接口 26](#_Toc5284470)

[2.2.8 门户部件渲染 27](#_Toc5284471)

[2.2.9 门户设置 28](#_Toc5284472)

[2.2.10 单点登陆系统服务端 28](#_Toc5284473)

[2.2.11 单点登陆系统客户端 29](#_Toc5284474)

[2.3 运行管理平台需求分析 29](#_Toc5284475)

[2.3.1 基础环境监控 29](#_Toc5284476)

[2.3.2 智能监控 30](#_Toc5284477)

[2.3.3 基础环境运维 30](#_Toc5284478)

[2.4 信息与安全支撑平台需求分析 31](#_Toc5284479)

[2.4.1 平台配置管理需求分析 31](#_Toc5284480)

[2.4.2 监控管理需求分析 32](#_Toc5284481)

[2.4.3 安全管理需求分析 33](#_Toc5284482)

[2.4.4 流程建模需求分析 34](#_Toc5284483)

[2.4.5 权限管理需求分析 34](#_Toc5284484)

[2.4.6 服务管理需求分析 34](#_Toc5284485)

[2.4.7 参数配置需求分析 35](#_Toc5284486)

[2.5 标准规范体系需求分析 35](#_Toc5284487)

[2.6 性能需求分析 36](#_Toc5284488)

[2.6.1 总体需求 36](#_Toc5284489)

[2.6.2 具体需求 36](#_Toc5284490)

[2.7 安全需求分析 40](#_Toc5284491)

[2.7.1 物理安全需求 40](#_Toc5284492)

[2.7.2 网络安全需求 41](#_Toc5284493)

[2.7.3 系统安全需求 67](#_Toc5284494)

[2.7.4 应用安全需求 67](#_Toc5284495)

[2.7.5 管理安全需求 68](#_Toc5284496)

[第三章 总体设计方案 68](#_Toc5284497)

[3.1 概述 68](#_Toc5284498)

[3.2 总体框架 69](#_Toc5284499)

[3.3. 高性能设计 71](#_Toc5284500)

[3.3.1. 总体架构的高性能设计 71](#_Toc5284501)

[3.3.2. 应用服务器的高性能设计 72](#_Toc5284502)

[3.3.3. 数据库的高性能设计 73](#_Toc5284503)

[3.3.4. 多级缓存与静态化 74](#_Toc5284504)

[3.4. 关键技术路线 75](#_Toc5284505)

[3.4.1. B/S结构 75](#_Toc5284506)

[3.4.2. 基于Hadoop的大数据平台框架 77](#_Toc5284507)

[3.4.3. 基于Java EE开发 78](#_Toc5284508)

[3.4.4. 基于SOA架构思想的共享服务模式 79](#_Toc5284509)

[3.4.5. 采用XML格式作为消息传递标准 80](#_Toc5284510)

[3.4.6. 基于XML的信息交换 86](#_Toc5284511)

[3.4.7. 基于REST架构 88](#_Toc5284512)

[3.4.8. 基于云服务架构 88](#_Toc5284513)

[第四章 各子系统建设方案 89](#_Toc5284514)

[4.1 政务信息资源共享交换平台 89](#_Toc5284515)

[4.1.1 概述 89](#_Toc5284516)

[4.1.2 建设内容 89](#_Toc5284517)

[4.1.3 目录子系统 90](#_Toc5284518)

[4.1.4 交换子系统 103](#_Toc5284519)

[4.1.5 质量工单管理系统 127](#_Toc5284520)

[4.1.6 数据对账子系统 132](#_Toc5284521)

[4.1.7 统一审计日志系统 137](#_Toc5284522)

[4.2. 综合集成门户建设 146](#_Toc5284523)

[4.2.1. 建设目标 146](#_Toc5284524)

[4.2.2. 平台功能 146](#_Toc5284525)

[4.3. 运行管理平台建设 159](#_Toc5284526)

[4.3.1. 监控平台 159](#_Toc5284527)

[4.3.2. 运维平台 163](#_Toc5284528)

[4.3.3. 数学模型建模系统 168](#_Toc5284529)

[4.3.4. 定制化服务系统 171](#_Toc5284530)

[4.4 信息安全与支撑平台建设 173](#_Toc5284531)

[4.4.1 信息安全 173](#_Toc5284532)

[4.4.2 支撑平台 187](#_Toc5284533)

[4.5 标准规范体系建设 198](#_Toc5284534)

[4.5.1 符合国家相关标准和技术要求 198](#_Toc5284535)

[4.5.2 标准规范研究与制定整体流程 199](#_Toc5284536)

[4.5.3 文档规范化的方法 199](#_Toc5284537)

[4.5.4 数据标准规范设计 200](#_Toc5284538)

[4.5.5 技术标准规范设计 200](#_Toc5284539)

[4.5.6 管理标准规范设计 201](#_Toc5284540)

[4.5.7 项目标准规范设计 202](#_Toc5284541)

# 项目概况

## 编制单位

编制单位：深圳市广通软件有限公司

## 项目背景

华为一直致力于为政府客户提供智慧城市整体解决方案，打造智慧城市神经系统，包括智慧城市中央神经系统与周围神经系统，构建智慧城市数字平台。基于标准化、模块化架构，协同业界伙伴构建智慧城市数字平台，是华为智慧城市解决方案的核心竞争力。

共享交换作为城市大脑IOC关键一环，消除政府客户烟囱化，实现各委办局源数据共享，同时提供厂家进行数据接入，数据归集，数据治理，从而汇入智慧大脑，实现城市的智慧化治理，因此，华为智慧城市团队计划通过发标，寻找在共享交换领域有成熟产品和专业服务能力的合作伙伴，并实现可销售，可复制，可交付目标。

深圳市广通软件有限公司是一家以软件开发、系统集成和技术服务为核心，提供行业应用软件、通用及个人软件、电子商务、网络应用集成、电信及有线电视系统集成和信息服务的国家高新技术企业。目前已在深圳、武汉、沈阳三地建立了研发中心，并在全国十几个主要城市设立了分公司及分子机构。

公司目前已具备计算机信息系统集成三级资质、ISO9000质量管理体系认证、ISO27001信息安全管理体系认证、涉及国家秘密的计算机信息系统集成乙级资质、CMMI3认证等多项资质。

公司已与华为达成战略合作伙伴关系，共同提出智慧城市联合解决方案，并长期与华为合作，就共享交换平台、基础库平台等一系列产品与华为进行了多个实际项目合作，且高质量的完成了产品和服务交付。依托实际项目经验及在数据共享交换平台的产品能力和服务能力，我司积极参与本次华为智慧城市运营中心（IOC）共享交换模块的产品及服务解决方案框招，给出具体的方案建议。

## 建设目标

按照《国务院办公厅关于印发政务信息系统整合共享实施方案的通知》（国办发〔2017〕39号）要求，要求实现与省政务信息系统进行共享，同时与各县（市）区留有接口。

1、要求实现国家《政务信息资源目录体系规范》和《政务信息资源交换体系规范》所描述的所有功能；

2、结合智慧城市公共信息资源的应用需求，提供并实现对《政务信息资源目录体系规范》扩展，提供不少于3类资源的元数据扩展及资源目录服务；

3、提供按照国标实现的资源发布工具（桥接中间件），该工具对平台上可编目的资源实现自动发布，包括扩展资源类型，提供产品登记证书及应用案例；

4、提供按照《政务信息资源交换体系规范》的体系架构要求建设交换平台，并实现所有功能，各功能模块的设定完全遵照国标实现；

5、遵照国家《政务信息资源目录体系规范》和《政务信息资源交换体系规范》定义的数据规范建设平台；

6、要求提供成熟的平台监控系统，可监控平台各节点及各节点环境、运行的应用系统的运行状态，及时通知、预警、报警平台的异常、错误状态信息；

7、要求提供基于国标《政务信息资源目录体系规范》和《政务信息资源交换体系规范》规范的安全认证、鉴证体系；

8、提供无障碍、无协助、无支持接入平台使用资源的便捷方法，业务系统接入平台的工作量不超过3人天。

## 建设内容

本项目包含以下建设内容：

1. 建设政务信息资源共享交换平台含目录子系统、交换子系统、质量工单管理系统、数据对账子系统、统一审计日志系统等；
2. 建设综合集成门户包含用户中心、单点登录、用户同步；
3. 建设运行管理平台含运维平台、监管平台、数学模型建模系统、定制化服务系统；
4. 建设信息与安全支撑平台；
5. 建设标准规范体系。

## 建设依据

1. 《关于印发〈国家电子政务总体框架〉的通知》（国信〔2006〕2号）
2. 《关于进一步加强政务部门信息共享建设管理的指导意见》（发改高技〔2013〕733号）
3. 《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）
4. 《国务院关于印发政务信息资源共享管理暂行办法的通知》（国发【2016】51号）
5. 《国务院办公厅关于印发政务信息系统整合共享实施方案的通知》（国办发〔2017〕39号）
6. 《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技〔2008〕2071号）
7. 《基于XML 的电子公文格式规范》；（GB/T 19667.2-2005）
8. 《政务信息资源目录体系国家标准》；（GBT\_21063.5-2007）
9. 《政务信息资源交换体系国家标准》；（GB/T21063.1-.4-2007)
10. 《电子文件归档与管理规范》(GB/T 18894-2002）
11. 《计算机信息系统安全保护等级划分准则》（GB 17859-1999〕
12. 《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008)
13. 《信息安全技术信息系统安全等级保护定级指南》（GB/T22240-2008）
14. 公安部、国家保密局、国家密码管理局、国务院信息工作办公室《信息安全等级保护管理办法》（公通字[2007]43 号）
15. 《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）
16. 《信息安全技术信息安全产品类别与代码》（GB/T 25066-2010）；
17. 《信息技术/安全技术/信息安全事件管理指南》（GB/Z 20985-2007）；
18. 《信息技术安全技术实体鉴别》（GB/T15843.2-2008）；
19. 《信息安全技术鉴别与授权基于角色的访问控制模型与管理规范》（GB/T 25062-2010）；
20. 《信息技术安全技术密钥管理》（GB/T17901.1-1999）；
21. 《信息安全技术信息系统灾难恢复规范》（GB/T 20988-2007）；

以上所有规程、规范以实施的最新版本为准。

## 建设原则

1. **总体规划，分步实施。**

严格按照相关标准和规范，紧跟信息技术发展趋势，结合政府电子政务信息化建设实际，科学规划公共信息平台项目，按照“规划引领，统筹推进”的建设思路，明确建设任务和要求，先易后难，分步实施，积极、稳妥、有序的推进整个项目建设。

1. **统筹协调，创新发展。**

统筹推进项目建设，加强政府各部门间的协作协调，形成发展合力。推动资源共享交换、大数据等新一代信息技术集成创新，结合不同部门要求推进管理、体制机制及应用创新，实现信息主导政务模式转变。

1. **统一建设，资源整合。**

统一建设要求，按照国家电子政务总体框架和政务信息资源目录体系与交换体系标准规范要求，搭建政务信息资源共享交换平台，为政府各部门数据共享交换提供技术支撑，实现资源共享，并通过中心库管理平台实现数据资源的高度整合，使用大数据平台进行数据存储和分析，为政府各类智慧应用提供数据和计算支撑。

1. **稳定可靠，安全运行。**

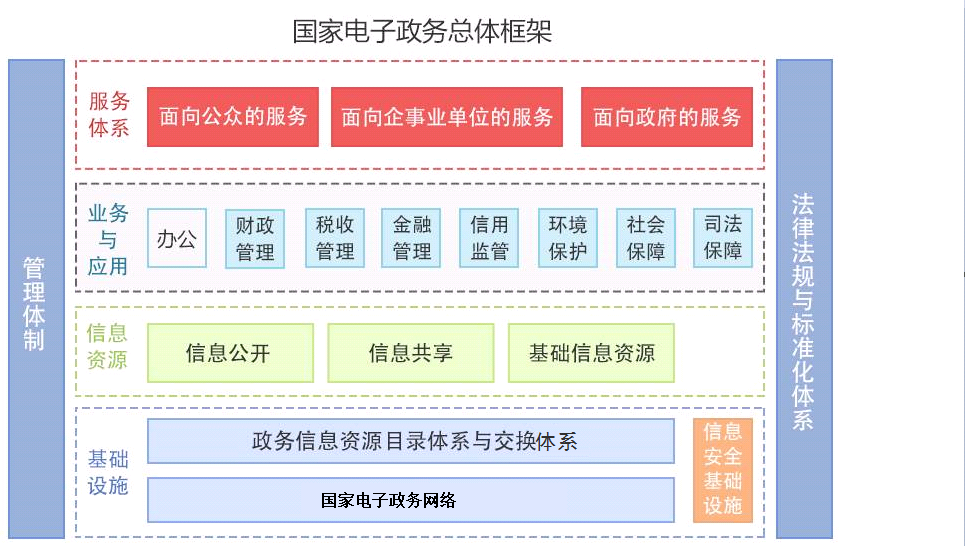
选择成熟实用的技术路线，适度采用符合技术发展方向、先进的IT技术，保证技术升级的连续性、稳定性、可靠性。采用安全可控的软硬件产品，综合运用信息安全技术，建立安全可靠的信息安全保障体系，提高故障监测预警技术水平，增强运维智能化和快速处置能力。

1. **面向服务，规范管理。**

在规范运行维护管理的基础上，探索服务新模式，建立以运营支撑平台为主要载体的运维服务体系，实现由技术保障型向资源服务型的转变，全面提升政府政府信息资源服务能力，提升系统的整体应用效能。

# 需求分析

## 政务信息资源共享交换平台需求分析

国家电子政务总体框架由服务与应用系统、信息资源、基础设施、法律法规与标准化体系、管理体制等部分组成。政务信息资源目录体系与交换体系是国家电子政务总体框架中的重要组成部分，是电子政务的基础设施之一。政务信息资源目录与交换体系在支持电子政务应用时是一个有机整体，都是以政务信息资源为基础，依托国家统一的电子政务网络，采用不同的技术架构分别实现不同的服务功能，提供目录服务和信息交换服务，实现部门间信息共享和业务协同的支撑，作为基础设施与电子政务的业务应用相对独立。

根据《[国家电子政务总体框架](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E6%80%BB%E4%BD%93%E6%A1%86%E6%9E%B6/14593108)》、《政务信息资源目录体系》、《政务信息资源交换体系》等国家标准规范的要求，为了实现政务信息资源的统一采集、梳理、质量治理、清洗、编目、合理共享、交换、管理、应用、分析，需要进行目录子系统和交换子系统等系统的建设，我们将核心和基础的目录子系统和交换子系统构成的有机整体，合称为政务信息资源共享交换平台。共享即各政务部门将信息资源统一整合后，将原则上可共享的信息资源目录和数据，共享在各部门的前置机共享信息库中，目录服务中心统一提取目录，提供资源的检索、定位功能，交换，即是指需要使用对应信息资源的政务部门，检索到对应资源后，提交审请，经审核通过授权后，由交换子系统，通过电子政务路由和网络，将提供方共享的对应信息资源，交换传输到申请使用方政务部门的前置机信息库中，以供使用方使用，最终实现通过资源共享和交换，所有参建政务部门获取所需共享的政务信息资源。

### 目录系统需求分析

目录系统需求分析内容主要有：

#### 资源管理

（1）提供结构化数据的数据库、表、字段等资源管理，能对数据对象进行新增、修改、删除操作；

（2）对应用系统资源进行登记、修改及删除的管理，形成单位的应用系统共享资源信息库。

（3）提供库表资源的自动采集功能。能够通过可视化配置，自动采集各数据库中的表、字段等信息，减少人工录入的工作量。

#### 编目管理

（1）提供资源目录的新增、修改、删除和发布；

（2）提供对资源目录的明细信息指标项管理（根据本部门的数据库资源的数据字段进行提取），单个资源目录内容可对应一个或多个信息指标项；指标项支持脚本转换；

（3）支持单个资源目录内容可设置一个或多个信息指标为主键功能，还可以撤消或调整当前主键；

（4）提供资源目录指定一个或多个指标项作为查询指标;

（5）提供非结构化数据编目功能，包括文件、服务、图片、视频等；

（6）提供资源目录的注册上报；

（7）提供人工编目、机辅编目等方式；

（8）编目系统支持中心系统集中编目，也可实现二级或多级汇总后传输到中心目录系统；

（9）提供目录形式审核功能，可实现漏填错填等问题的自动检测。漏填可自动检测。错填的判断规则复杂，由人工检测。

（10）提供前段码配置管理功能。要能跟按照2017新编目指南的要求，配置部门类、基础类、主题类的资源目录的前段码。

（11）部门信息资源编目必须满足2017年新编目指南的元数据要求。库表型资源必须包含名称、类型、长度等元数据。

#### 目录审核及发布

（1）根据目录内容提供目录审核功能，经审核后在资源目录中发布；

（2）提供图形化的审批流程定义和修改，并能监控流程环节状态；

（3）能够结合人工方式进行目录审核，包括审核数据和审核结果的导入导出。

（4）资源目录发起审批后，目录提供方可以修改目录信息，其他部门不能修改。

#### 目录检测

（1）配置定时任务，定时扫描比对资源目录的库表结构信息与资源管理中的库表结构信息是否发生了变化

（2）列表的方式展示定时扫描比对的结果

（3）变化提醒：信息中心、实施厂商、提供部门的用户登录系统，在消息栏看到消息提醒。

#### 目录变更

（1）提供目录修改变更功能，经审核通过后在资源目录中变更；

（2）提供目录变更的版本管理功能，包含自动检测和版本变更两种方式。

（3）手工发起变更：选择已发布的信息资源，发起变更申请

（4）自动发起变更：根据扫描比对结果，发起变更申请

（5）变更提醒：信息中心、实施厂商、提供部门的用户登录系统，在消息栏看到消息提醒。

（6）变更记录：在目录列表页面，点击“变更记录”按钮，查看信息资源的版本记录和变更比对情况

（7）变更完成，生产新的版本号。资源目录列表的每个目录显示最新版本。

#### 目录导出

（1）根据资源目录导出SQL建表脚本

（2）目录信息导出为文件，包含EXCEL、WORD、ZIP等格式。

#### 目录服务

（1）目录发布

a）分类导航；

b）单个检索词检索；

c）多个检索词的组合检索。

（2）目录查询

a)查询请求解析；

b)目录内容服务信息库查询；

c)查询结果封装返回。

（3）支持授权管理，用户只能查询权限范围内的资源信息；

（4）对非结构化文档（如文档），提供内容查询和直接下载功能；

（5）根据资源目录服务需求，生成各种固定导航目录。

#### 需求管理

（1）提供资源使用申请审批功能进行需求申请和备案；

（2）提供直观的资源需求的分类、汇总和统计功能；

（3）提供需求满足度的统计分析和评估功能，并为电子监察系统提供相应的统计和评估数据。

（4）提供依据资源目录提交使用申请的功能，可依据目录的信息项进行勾选。申请单内的字段信息必须全部来自于资源目录。

（5）提供对资源申请情况的统计分析功能。

#### 资源使用管理

（1）提供对需求申请的审批及授权；

（2）结合需求管理和服务使用情况，提供直观的资源使用情况分类、汇总、统计和日志报表等功能。

#### 目录部署

（1）支持集中编目；

（2）支持目录系统的分级部署（支持目录分中心）。

#### 目录元数据管理

用户可根据需求，在界面自定义编目等操作的元数据

#### 目录版本功能

支持目录版本，多个目录版本信息查看、比对、回滚等功能。

#### 工作流管理

用户可根据需求，自定义目录发布审核等操作的工作流。

#### 角色权限管理

需要提供用户的角色权限设置和管理、控制。

### 交换系统需求分析

交换系统的需求分析内容有：

#### 交换桥接子系统

(1）支持部门业务信息库与交换库之间的双向信息同步；

(2）支持各种主流数据库（Oracle/MySql/Postgres/SqlServer等）；

(3）支持结构化及非结构化文件的桥接，非结构化文件可桥接到交换库或是指定的文件目录；

(4）支持强大的逻辑运算适配，支持脚本语言；

(5）采用适配器组件访问桥接对像，实现数据的获取与存储；

(6）提供增量数据自动识别的功能，在不修改业务信息库结构的情况下，系统应能够自动的识别出需要交换的信息，包括新增、被修改或被删除的信息；

(7）提供部分数据、指标更新时的识别、同步功能；

(8）支持数据的实时同步、定时、增量同步；

(9）提供图形化的信息交换桥接配置及管理工具，提供桥接定义与桥接管理功能；

(10）应支持多个桥接任务或服务同时运行，应支持桥接服务的远程部署；

(11）提供单个数据源到多个目标、多个源到单个目标之间的定制功能；

(12）能对数据的抽取进行优化；

(13）对于大量数据的快速抽取；

(14）支持系统异地备份，并提供统一的管理界面；

(15）前置机系统的基础环境可快速恢复，并通过中心配置文件和备份数据进行远程恢复；

(16）提供详细的桥接日志、错误日志，具备异常的快速定位功能。

#### 前置交换子系统

(1）支持不同交换信息库之间的双向信息交换。前置交换子系统能够从交换信息库中提取数据交给交换传输子系统传递，也能够从交换传输子系统中获取数据存储到指定的信息库或其他数据库中；

(2）支持各种主流操作系统（Windows/Linux/Unix）；

(3）支持国内外主流数据库(Oracle/MySql/DB2/SqlServer等)；

(4）采用传输适配器接入到交换传输子系统；

(5）支持将现有服务和应用接入到交换传输子系统；

(6）支持用图形化向导的方式快捷生成服务；

(7）支持与服务与目录版本的同步和对应，记录服务版本变化情况，能对服务的生命周期进行管理；

(8）支持服务查询指标的优化，能为不同的查询条件订制化的服务；

(9）采用应用适配器访问交换信息库，实现对交换信息库中数据的获取与存储；

(10）提供图形化的服务定制工具，配置、测试、部署服务；

(11）支持多个服务并发运行；

(12）提供服务的监控功能，包括服务的使用者、调用时间、调用次数、响应时间、服务状态、运行时间、服务调用失败定位等，并能够对服务的使用情况进行查询统计；

(13）能远程启动和停止前置节点上的服务；

(14）支持配置文件异地备份与恢复，并提供统一的管理界面；

(15）提供服务安全性策略集中定义功能，能对服务进行统一的访问授权、审计、身份管理；

(16）支持服务远程部署功能，能将服务远程部署到一台或多台前置机上；

(17）支持服务的负载均衡；

(18）提供详细的错误日志，具备异常的快速定位功能

(19）提供管理与监控接口，支持远程管理功能。

#### 交换传输子系统

(1）消息传送应支持RFC2616；

(2）采用W3C的SOAP作为消息封装格式；

(3）采用W3C的WSDL作为交换服务描述规范；

(4）提供消息寻址功能，支持信息路由功能。

(5）支持多种传输协议，包括Http、Soap、MQ、JMS，可灵活选择其中的一种或多种协议进行通信；

(6）支持点对点、一点对多点和多点对多点的传输模式；

(7）提供消息确认和消息选择性重发机制以实现前置交换子系统之间安全的、可靠的信息传递功能；

(8）支持断点续传；

(9）提供对数据进行加解密、压缩及解压缩等功能；

(10）提供消息差错处理功能；

(11）提供信息转换功能，支持基于规则配置的格式转换与内容转换功能；

(12）提供大于2G以上文件传输功能，并支持分包机制进行传输。

#### 交换任务管理子系统

(1）任务创建：依据资源目录申请单配置共享交换任务，交换任务传输的字段信息必须全部来源于申请单。

(2）针对库表型共享交换任务，可动态配置源库表与目的库表之间的字段映射关系，并可配置字段与目录信息项之间的映射关系。

(3）任务审批：通过审批流驱动共享交换任务的审批过程。

(4）任务查询：可多条件查询共享交换任务信息，并可查看交换任务的详细信息。

(5）任务统计：提供交换任务的统计分析功能。

#### 交换管理子系统

(1）基于SOA框架，采用成熟的、具有成功案例的产品实现；

(2）支持跨平台的数据和消息传输；

(3）提供图形化的流程设计与配置工具配置信息交换流程；

(4）提供信息交换流程功能,通过灵活的服务组合配置，实现点对点、点对多点、多点对点、多点对多点的业务协同；

(5）支持流程版本管理能力，支持一个流程多个版本同时运行，并对版本的生命周期进行管理；

(6）业务流程支持人工参与流程和自动处理流程，通过直观的流程图标显示流程实例的执行路径；

(7）提供流程执行性能数据，生成各种流程的执行时间，流程节点执行性能指标的柱状图、饼图等展现方式；

(8）提供流程的调试功能；

(9）提供流程监控，对流程的错误进行精确定位，并能进行回溯；

(10）提供图形化的界面来配置进行业务流程的的整合与管理；

(11）支持流程的动态部署；

(12）支持WebService，提供在异构环境下对Web服务进行访问控制、策略定制等功能；

(13）支持服务集中注册，统一管理；

(14）提供应用之间数据格式转换功能；

(15）提供灵活的数据传输路由配置功能；

(16）提供数据的发布、订阅功能；

(17）与包括．NET、J2EE在内的各种平台进行集成；

(18）支持包括Soap、Http、Https通道在内的标准协议；

(19）提供负载均衡功能；

(20）提供统一的图形化管理工具，能对整个平台各个节点进行监控和管理及备份恢复；

(21）提供信息交换管理及日志查询的功能，实时监视信息交换的情况；

(22）提供强大的报表功能，支持自定义生成各类运维报表；

(23）支持对整个平台的运行情况进行审计，能够生成直方图等格式报表，并能将相应的审计信息导出为Word或Excel；

## 综合门户需求分析

### CA认证管理需求分析

（1）证书申请：用户填写证书申请表，向管理员提出CA证书申请。

（2）证书审批：查看证书申请记录，批准或拒绝CA证书申请。批准的CA证书申请则绑定CA证书并颁发CA证书给用户。

（3）证书管理：提供对CA证书的冻结、解冻、吊销的功能。

（4）证书吊销查询：展示已吊销的证书记录。

### LDAP认证需求分析

（1）VPN设备：管理的用户及组织信息进行统一身份认证。

（2）LDAP服务：LDAP实现组织身份信息的统一管理，并为各种软件提供一种统一的认证机制进行用户认证。

（3）LDAP服务：实现将用户中心的用户信息同步至LDAP服务器中，是LDAP实现身份认证的基础。

### 应用系统集成

（1）接入系统管理：对待接入应用系统的相关资料进行注册，资料核准无误后启用应用系统。

（2）接入系统同步管理：对接入的应用系统的用户、组织机构的同步范围进行设置。

（3）接入系统权限管理：设置可访问该接入的应用系统的用户或角色。

### 信息集成

（1）待办待阅任务对接：各接入系统调用待阅待阅任务对接接口上传待办、待阅、任务数据至综合门户，使综合门户能集中展示用户在各应用系统的待办、待阅和任务。

（2）日程对接：展示用户的所有日程安排。

（3）站内信息对接：展示和提醒用户接收的站内消息。

### 门户定制

（1）部件管理：注册和维护。

（2）模板管理：注册新模板，对所有可用模板进行维护。

（3）门户管理：门户授权给角色或具体人员。

### 内容管理

（1）Banner图维护：综合门户管理人员对综合门户、单点登录页面的LOGO、动态图片进行维护。

（2）通知公告管理：利用通知公告管理功能，系统管理员可以发布全网公告，所有用户都能接收到。

（3）友情链接管理：通过友情链接管理来维护它事务单位网站的外链，在综合门户上可展示所有的友情链接，点击链接可进入相应单位的网站。

（4）快捷办公管理：对用户经常使用功能，系统管理员可以通过快捷办公管理功能，将这些功能对应的应用系统的内部链接管理起来。

### 用户同步接口

（1）全量数据查询接口：已接入综合门户的业务系统，使用该接口读取用户中心的区划、单位、人员、单位人员的全量数据，并同步至业务系统的数据库中。

（2）增量数据查询接口：已接入综合门户的业务系统，使用该接口读取用户中心的区划、单位、人员、单位人员的增量数据，并同步至业务系统的数据库中。

（3）数据同步回执接口：已接入综合门户的业务系统调用全量数据查询接口、增量数据查询接口获取用户中心组织机构数据并更新到业务系统数据库后，需调用该接口反馈最终数据同步结果给用户中心。

### 门户部件渲染

（1）应用导航：集中展示当前用户在综合门户有权限使用的所有接入系统，点击对应的应用系统即可进入相应应用系统的界面，无需再次登录，实现统一入口。

（2）快捷办公：综合门户统一展示系统管理员定义的所有快捷办公链接，用户在综合门户上直接点击这些链接即可跳转进入应用系统的具体功能界面，实现快捷办公。

（3）通讯录：综合门户展示当前登录用户所在单位的全部人员信息，包括人员所在科室、联系电话，并提供即时通讯功能。

（4）通知公告：综合门户集中展示当前登录用户所在单位接收到的全部通知公告，包括公告内容、发出时间和发出人。

（5）待办：综合门户集中展示当前登录用户的所有待办信息，点击对应待办可进入对应应用系统的处理界面进行办理。

（6）待阅：综合门户集中展示当前登录用户的所有待阅信息，点击对应待阅可进入对应应用系统的处理界面进行办理。

（7）任务：综合门户集中展示当前登录用户的所有任务信息，点击对应任务可进入对应应用系统的处理界面进行办理。

（8）友情链接：综合门户上展示所有的友情链接，点击链接可进入对应单位的网站。

（8）日程管理：综合门户集中展示用户在各应用系统设置的日程，也可在日程管理部件中直接添加日程安排，实现日程提醒和任务催办的功能。

（10）个性化定制部件：直接将综合门户集成的业务系统的功能页面作为部件，在门户上进行渲染展示。用户不用进入具体的业务系统，也能实时地在综合门户首页上查看其关注的信息。

### 门户设置

（1）应用设置：用户可以设置应用导航部件上的应用系统是否展示或隐藏。

（2）快捷办公设置：用户可以设置快捷办公部件上的快捷办公链接是否展示或隐藏。

（3）门户部件选择：对于用户个人办公空间上展示的部件，用户可以自行选择是否展示或隐藏。

（4）门户布局调整：用户可以对个人办公空间上的部件位置、顺序进行调整，满足个性化需求。

（5）个人信息管理：用户可以在综合门户上修改自己的个人信息，如手机号码、EMAIL等，实现用户信息的及时更新。用户也可对密码进行及时变更，保障个人账户的安全性。

（6）站内消息查看：在综合门户显示当前用户接收到的站内消息。

（7）办公门户：用户可以对行程进行安排和管理；用户可以查看站内消息和通讯录；提供各应用系统的统一入口；用户可以查看本单位接收到的通知公告等等。

（8）领导门户：根据领导的角色、权责范围以及个性化需求定义不同的界面布局、展现内容以及展现方式，从而让领导的日常办公操作更加人性化和便捷高效。

（9）部门门户：部门门户展示用户所在机构的相关信息。可作为各单位宣传教育、树立形象、传播文化的工具。

### 单点登陆系统服务端

（1）身份验证：支持不同的身份凭证注册及认证，如静态密码、动态密码、CA证书、指纹识别，实现不同安全等级的统一身份认证服务。

（2）应用访问安全控制：携带ticket并交由单点登录服务端进行验证，单点登录服务端进行ticket正确性、时效性等方面的验证，验证通过则跳转至功能页面，否则跳转至单点登录页面，要求用户重新登录。

（3）移动办公登录服务：提供登录验证、用户详情查询和密码修改等http服务供移动办公app使用。

（4）通知公告展示：在单点登陆系统的首页展示系统管理员发布的全网公告，用户不需要登录即可查看。

（5）资源下载：用户可通过该功能下载常用的资源、组件、应用。

### 单点登陆系统客户端

（1）访问控制过滤器：重定向到单点登录页面；获取Ticket；调用请求单点登陆系统服务端进行验证类，获取登录用户；调用业务系统初始化现类，完成应用系统的登录初始化。

（2）应用系统初始化：用户身份验证通过后，由访问控制过滤器调用该接口的实现类，对应用系统进行初始化，如选取登录用户的身份信息、权限等。

## 运行管理平台需求分析

### 基础环境监控

（1）监控配置-节点管理：注册新节点，建立节点档案，修改节点信息、启用和禁用节点。

（2）监控配置-数据库管理：注册新数据库，建立数据库档案，修改数据库信息、启用或禁用数据库。

（3）监控配置-应用服务器管理：注册新应用服务器，建立应用服务器档案，修改应用服务器信息、启动或停止应用服务器。

（4）监控配置-应用系统管理：注册新应用系统，建立应用系统档案，修改应用系统信息。

（5）监控配置-配置监控启用项及规则：根据配置的监控启用项和监控规则启动对应监控。

（6）监控配置-配置监控禁用项：根据配置的监控禁用项来决定是否启用某监控。

（7）连通性监控：资源的连通性监控。

（8）系统资源使用率监控：服务器的CPU、内存、磁盘空间、网络及磁盘IO使用情况的监控和预警。

（9）查看监控结果统计：查看具体节点的监控结果明细。

（10）查看监控结果明细：图表的形式展示所有监控项的结果。

### 智能监控

（1）自动巡检：巡检机器人对平台进行全方位的巡检。

（2）平台运行周报和日报：周报和日报机器人自动分析平台的运行情况产生周报和日报表发给运维人员和相关管理人员。

（3）服务接口自动巡检：服务接口巡检机器人对重新要的服务接口进行巡检，主动发现服务接口异常。

（4）异常事件和日志监控：感知机器人通过传感器监控平台异常，将异常预警信息发送给运维人员和相关人员。

### 基础环境运维

（1）数据运维-数据源管理：注册新数据库，建立数据库档案，修改数据库信息、启用或禁用数据库。

（2）数据运维-统一查询器：选择数据库，输入查询类的SQL语句并执行，界面会返回查询结果。

（3）数据运维-系统表运维：输入SQL脚本，选择要执行脚本的目标数据库，并输入执行脚本的备注说明等信息，建立系统表运维单，提交。

（4）业务运维：目录系统和交换平台的基础环境进行排查错误和测试，并展示排查结果。

（5）系统运维-节点管理：注册新节点，建立节点档案。修改节点信息、启用和禁用节点

（6）数据运维-运维控制台：在某个节点上打开一个运维指令控制台，在上面执行已经被授权的运维指令和操作系统命令，并实时查看指令执行的输出结果。。

（7）日常运维指令管理：预先录入一些常用的运维指令，并将它们授权给运维人员，或者将运维指令批量的发布到指令的节点上执行。

（8）指令分类管理：预先录入某些匹配规则，以便识别运维指令的类别，并此类别授权给运维人员。

（9）行为管理：查看各种运维日志。

（10）版本管理-应用版本管理：发布各种应用系统的版本。

（11）版本管理-补丁管理：发布各种应用系统的某个版本的补丁，以便可以通过部署在运行节点上的运维Shell进行补丁部署和升级。

（12）版本管理-配置管理：发布各种应用系统的项目配置文件，以便可以通过部署在运行节点上的运维Shell进行配置文件的部署和修改。

（13）版本管理-版本回滚：对应用版本、补丁和配置进行回滚操作，以便将最近一个升级更新操作回滚到上一个版本的状态下。

（14）版本管理-部署进度跟踪：实时查看版本、补丁、配置和回滚操作的状态和结果。

（15）版本管理-安装路径管理：配置各应用系统在各运行节点上的安装路径。

（16）版本管理-节点应用关联：控制关哪些节点上可以部署哪种类型的应用。

## 信息与安全支撑平台需求分析

### 平台配置管理需求分析

(1）用户管理：能够建立组织、用户、角色等管理要素，提供增加、修改、删除等管理功能。

(2） 权限/策略管理：提供权限定义和资源访问规则描述。根据资源描述的元数据，设定权限的访问控制策略，以描述权限对应具体的访问控制；

(3）授权管理：提供基于统一的用户库配置目录和交换服务的访问授权。授权粒度可以细化到角色到具体用户，也可以用户组进行管理。

(4）服务管理：服务的分类、部署方式、负载均衡和数据的转换、编码、加解密等特性的加载和解除管理。

(5）支持集中管理的配置文件和远程部署各种服务以及运行环境的软件升级。

(6）提供C/S和B/S的平台配置管理界面；

(7）可以授权牵头单位对特定的交换域组成单位进行分级授权。

### 监控管理需求分析

(1）支持网络拓扑发现；

(2）设备监控：监控设备的CPU、内存、磁盘、逻辑分区、交换分区、网络接口、进程使用情况；支持对数据库性能监控与管理，提供从应用使用情况、系统资源使用情况、性能指标等全面的监测管理；

(3）应用监控：对前置节点和交换中心部署的服务、组件运行情况进行监控，主要监控服务的使用率、异常及失败、服务消费能力、服务使用者情况；对信息交换整个业务流程进行监控；

(4）监控预警：支持对监控指标设立阀值，并能通过短信、邮件等多种方式进行预警，预警可以分等级，按照警报的不同等级选择不同的通知方式和通知人员；

(5）日志分析：采集来源于公共信息平台的交换资源日志、访问目录服务系统日志、使用基础（共享）库资源的日志、访问门户的日志，对这些日志信息进行统一展示和统计分析，为管理人员分析整个共享公共信息平台的运行和使用情况提供依据；

(6）数据库监控：支持对Oracle等数据库连接和性能监控，实现对数据库表空间使用情况的监控，支持对oracle等数据库管理，提供数据库服务的启动、停止功能，提供创建表空间、表、触发器、视图以及数据的备份和恢复功能；

(7）对中间件的监控：支持对OAS、BEA Weblogic Server、Websphere等中间件性能监控，能够帮助系统管理员监测系统性能、分析和确定系统的瓶颈。比如能监控应用服务器上页面/servlet的平均响应时间等性能指标。

### 安全管理需求分析

(1）统一认证：支持用户名/口令和数字证书两类技术电子身份认证，支持统一的认证网关和授权管理；结合内外网CA平台，实现资源访问的全程可控、可审计；

(2）传输安全：平台提供安全可靠的数据传输安全。支持VPN、数据加密、消息数据签名、摘要等管道套接方式对数据传输进行加密，防止越权访问机密信息或恶意篡改；

(3）支持HTTPS传输协议，通过SSL实现数据防篡改、数据加密等功能；

(4）支持对消息内容的数字签名、数字摘要和信息加密。

(5）提供多级冗余备份存储策略，提供安全可靠信息存储，保障系统安全运行；

### 流程建模需求分析

页面链接、新增流程、新增流程必填项验证、流程删除、流程信息修改、单个条件查询、多个条件组合查询、模糊查询、空值查询、重置按钮测试、删除流程、修改流程信息、流程发布、流程复制

### 权限管理需求分析

(1）菜单管理：添加系统菜单、菜单管理、系统名称进行模糊查询和全称查询

(2）角色管理：根据角色名称进行查询、角色授权

组织结构管理

(1）区划管理：新增、修改，查询，删除

(2）单位管理：新增、修改、删除、查询

(3）人员管理：新增、修改、删除、查询

### 服务管理需求分析

实现动静态两种服务。动静态服务：新增、修改、删除、查询。

### 参数配置需求分析

接入的应用系统需配置接入系统参数。字号配置、项目配置管理、参数配置、字典配置：新增、修改、删除、查询。

## 标准规范体系需求分析

本项目在标准规范方面需要重点考虑如下几点：

1.按如下顺序执行标准：国家标准规范、行业标准规范、国际标准规范、地方标准规范、企业标准规范。

2.按需求驱动原则，需要执行的标准先采用或制定；

3.先规范业务、数据指针。

另外，为实现部门资源发布的无缝集成，还需编制如下标准规范:

* 管理标准规范
* 技术标准规范
* 数据标准规范
* 业务标准规范
* 接口标准规范
* 文档标准规范

## 性能需求分析

### 总体需求

**1. 网络性能需求：**要求数据传输网络畅通、快捷、高带宽、安全、可靠、可扩展。

**2. 系统性能需求：**要求采用通用性好的计算机系统、安全可靠的操作系统以及大型数据库系统，吞吐能力强，保证系统良好的性能，数据库系统必须具有良好的垂直升级能力。

**3. 基础支撑平台性能需求：**应用支撑平台能为业务应用系统的开发和运行提供技术支撑，具备有异构系统和数据平台的信息交换能力，并具有灵活的可扩充性和高度的可配置管理性。

**4. 业务应用系统性能需求：**业务应用系统应满足用户的要求，稳定、可靠、高效。人机界面友好，输出、输入方便，图表生成灵活美观，检索、查询简单快捷。由于系统的数据量非常大，并且数据记录的增长速度非常快，对于关系数据库的查询能力和查询算法是一个挑战。必须设计出合理的数据库结构和查询算法，以保证查询的响应速度，并不随记录数的增长急速下降。

**5. 数据性能需求：**系统数据应完整、准确和及时。汇总统计、制表制图、分析计算、模型测算等功能比较齐全，保证计算结果准确。本系统不仅数据量大，而且数据类型多样，包括图像、文本等信息类型，因此，对处理系统的计算能力有比较高的要求，也要求对数据库记录数的增长没有限制，并且保证大容量数据库的可操作性。

### 具体需求

#### 系统稳定性指标

（1） 系统稳定性  
系统有效工作时间≥99％，系统故障平均间隔时间≥90天。

稳定性要求，支持10万次以上的连续请求处理无故障；

（2） 故障处理  
系统在设计时应充分考虑稳定性及对用户误操作的容错功能，保证在正常情况下系统能保持长时间无故障运行。对于不可预见的原因导致的系统故障，提供各种故障处理恢复机制使系统在尽可能短的时间内恢复运行，保证数据的安全性和完整性。

#### 系统应用性能指标

##### 基本性能

（1）在1000M局域网环境下进行增、删、改业务（不含大对象数据类型）响应时间在3秒以内。

（2）在1000M局域网环境下查询操作的响应时间要求在3秒以内。

（3）系统支持同时在线数大于200，并发用户数大于50。

##### 其他性能指标

（1）实时业务支持能力，对简单的实时交易，数据交换需在1秒内完成从接受请求到处理完成，基础库需同步支持以上能力；

（2）对实时或批量的数据交换业务请求给予响应，支持至少10个并发请求的响应，具备大并发量处理机制，支持实时与批量处理的均衡调度；

（3）对大数据包的处理，记录量在10万左右，能在10分钟以内完成交易从接受请求到处理完成。

#### 系统响应时间指标

从一个用户角度讲，一般性操作最长不超过 3秒；系统响应时间≤0.5 秒。

当用户做一些处理时间较长的操作时，能给出提示信息提醒用户。在返回数据量过大导致响应时间过长时，能提供部分响应，例如分页取数据等，减少操作人员等待的时间。

数据查询：

（1）查询基础数据（精确匹配）的响应时间不大于3秒。

（2）查询单个数据主题（百万级）的响应时间不大于3秒。

（3）目录检索的响应时间不大于2秒。

（4）查询统计报表（非实时统计）的响应时间不大于3秒。

#### 数据交换性能指标

##### 网内数据交换

（1）1000M内网环境下，数据库表与表之间的全量数据交换达到3000条/s以上。

（2）1000M内网环境下，数据库表与表之间的增量数据交换达到600条/s以上。

（3）1000M内网环境下，文件数据交换达到12M/秒以上。

##### 跨网数据交换

（1）100M带宽出口环境下，数据库表与表之间的全量数据交换达到3000条/s以上（记录大小10K左右）。

（2）100M带宽出口环境下，数据库表与表之间的全量数据交换达到600条/s以上（记录大小10K左右）。

（3）100M带宽出口环境下，文件交换全量数据交换达到5M/s以上。

数据交换任务量，支持2000以上的交换任务同时执行，交换性能可以根据交换服务器的扩展进行线性增加。

##### 实时数据交换

系统支持实时数据秒级交换能力

海量数据MPPDB高性能插入：

系统支持大量数据全量向MPPDB插入的性能达到10万条/秒

#### 数据质检性能指标

（1） 单节点支持质检支持20000条/s的质检速度

（2） 支持2000以上质检任务运行

（3） 质检性能可以根据质检服务器的扩展进行线性加

（4） 质检对象支持1亿以上的数据对象质检

#### 系统并发处理能力指标

系统能够支持同时从多个部门或地方并发使用，要求系统不能由于用户连接的增加明显降低系统的响应时间。支持同时在线用户数1000人；并发用户数100 人。

单个系统支持40+前置机数据接入、信息资源共享数量在1500+、数据指标项总数在45000+，支撑全市或者全国所有政务系统对共享数据的应用。

## 安全需求分析

### 物理安全需求

物理安全的威胁主要有地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识薄弱等。

### 网络安全需求

1、外部网络安全需求。

存在各种各样不可预知的风险，网络入侵者可以通过多种方式攻击内部网络。因此，有必要将对外信息发布服务器（Web, DNS, EMAIL等）部署在政务外网并和内部其它业务网络进行必要的隔离，避免网络信息外泄，使得攻击者无从下手，同时还要对网络通讯进行有效的过滤，使必要的服务请求到达主机，对不必要的访问请求加以拒绝。

2、内部网络安全需求。

需要对网络的运行状况实施有效监控，及时发现潜在的计算机病毒威胁，避免由于办公地点、人员、设备的变化，使得网络结构变化无法控制，同时需了解网络的漏洞和可能发生的攻击，建立对于己经或正在发生的攻击进行有效的追查方法。

#### 安全红线需求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 子项目 | 需求规格 |
| 1 | 管理通道安全 | 管理面与用户面隔离 | 对于支持带内管理模式且有独立管理面IP的系统，规格如下： 系统应提供有效的办法（如ACL、VLAN等机制）来保证带内管理面与用户面的隔离。 |
| 2 | Web系统安全 | 登录认证防暴力破解 | 登录认证模块提供防暴力破解机制；例如，验证码或者多次连续尝试登录失败后锁定帐号或IP。 |
| 会话管理 | 1、对于每一个需要授权访问的页面或servlet的请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作，以防止URL越权。 |
| 2、用户登陆认证通过后必须更换会话标识。 |
| 3、Web应用程序使用业界主流的web容器（Apache、Tomcat、jboss、weblogic、nginx、jetty、resin、websphere、IIS）的会话标识生成机制生成会话标识。如果没有使用业界主流的Web容器，自己生成会话标识,必须使用安全随机函数，如： 1）OpenSSL库的RAND\_bytes()； 2）JDK的java.security.SecureRandom()； 3）类Unix平台的/dev/random文件； 4）Windows平台的RtlGenRandom()。 |
| 登录口令保护 | 向服务器端传递用户名和口令（含应用层用户名/口令）时，需采用安全协议（如HTTPS、HTTP digest）或加密用户名/口令后再传输。只能本地访问的Web可不作要求。 |
| 认证管理 | 对用户的最终认证处理过程必须放到服务端进行。 |
| 输入校验 | 1、系统外部输入需在服务端进行最终校验。 |
| 2、产品的Web应用如果提供上传文件到Web内容目录的功能，必须在服务端对上传的文件类型进行限制（基于白名单机制对文件扩展名进行限制），仅允许上传业务允许的文件类型。（如提供此功能，为必须满足项，如不提供该功能，可不涉及） |
| 输出编码 | 对于不可信的数据，输出到客户端前必须先进行HTML编码。（如提供此功能，为必须满足项，如不提供该功能，可不涉及） |
| Web系统漏洞 | 使用Web安全扫描工具（如AppScan、WebInspect、Acunetix Web Vulnerability Scanner）扫描Web服务器和Web应用，测试应使用最新的漏洞库、配置所有漏洞相关插件，扫描报告中不得出现高风险级别的漏洞。 |
| 4 | 数据库安全 | 数据库生命周期 | 不得使用已经停止维护的数据库版本。 （如有需要，可填写要求的数据库具体版本） |
| 数据库加固 | 1、系统经业界主流漏洞扫描工具扫描（如NGSSQuirreL），扫描工具需使用最新的漏洞插件、配置所有漏洞相关插件，扫描报告中不得出现高风险级别的漏洞。 |
| 2、系统提供安全配置/加固指南和安全维护手册等文档。 |
| 数据库权限管理 | 1、数据库若存在多个默认帐号，须将不使用的帐号禁用或删除。 |
| 2、应使用非操作系统管理员账号运行数据库； |
| 3、数据库帐户只能具备执行其任务的最小权限。 |
| 4、数据库系统本身的文件及用户的数据文件需要严格控制访问权限，只有数据库进程运行帐户以及管理员帐户才具备读写权限； |
| 5、提供数据库口令复杂度检查功能，若口令不符合复杂度规则，可以禁止用户设置并进行警告。 |
| 物料对数据库安全补丁的兼容性测试 | 供应商应对数据库的安全补丁进行兼容性测试，定期发布数据库安全补丁列表。 |
| 数据库的安全补丁发布 | 提供数据库的安全预警以及安全补丁发布渠道。 |
| 5 | 产品开发、发布 | 禁止绕过系统安全机制的功能 | 1、禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：组合键、鼠标特殊敲击、连接特定接口，使用特定客户端、使用特殊URL等。 |
| 2、禁止不可管理的认证/访问方式：包括用户不可管理的帐号，人机接口以及可远程访问的机机接口的硬编码口令，不经认证直接访问系统的接口等。 |
| 3、除上述隐秘、不可管理的认证/访问方式外，不得含有其它任何形式的后门、木马、恶意广告、吸费陷阱、恶意消耗用户数据流量等恶意代码或未知功能。 |
| 4、所有帐户都必须被用户可见，禁止存在用户未知的帐户，在物料资料中提供所有帐号及管理操作说明。（仅用于物料内部通信，且外部无法访问的帐号，可以例外。） |
| 5、未文档化的命令/参数、端口等接入方式（包括但不限于物料的生产、调测、维护用途），提供资料进行说明。 |
| 禁止存在未文档化的命令/参数、端口等 | 1、不得存在客户资料(含通信矩阵)中没有公开的协议端口/服务； |
| 2、不得存在未文档化的命令、参数等（包括但不限于产品的生产、调测、维护用途）。 |
| 软件完整性 | 1、对于涉及软件包分发的物料应提供完整性校验机制（如：数字签名或者哈希值），并提供文档说明验证方法。注：CRC不能用于完整性校验。 |
| 2、涉及软件包分发的物料应经过业界至少两款知名杀毒软件扫描，不存在病毒、木马、恶意程序，并提供扫描报告结果。 |
| 安全编码 | 使用静态代码检查工具（如，Coverity，Fortify）对物料源代码进行扫描（可只扫描高风险模块），并对扫描的告警进行分析，确认告警的实际风险等级，对于实际风险为“高”的漏洞（CVSS 7分及以上），必须解决，提供扫描分析报告。 高风险模块识别参考标准： 1)物料对外提供的所有管理和控制接口相关的代码（如网管配置管理接口、Telnet/SSH、MML、路由协议、信令接口等） 2)对不可信来源的数据进行解析或处理的代码（如，用户面数据处理、网络或应用协议解析、文件解析等模块、计费策略或者逻辑处理） 3)安全相关类代码(如，认证、授权、接入控制、加解密、密钥管理、日志审计、软件完整性保护等模块) 4)集中处理个人数据或者敏感数据的代码（如，敏感数据匿名化） 5)WEB模块(如：HTTP协议头处理处理模块 、文件/图片上传处理模块 、SQL语句处理模块 、Response HTML输出模块 ) |
| 安全补丁发布 | 提供安全预警以及安全补丁发布渠道。 |
| 开源软件安全 | 1、供应商提供给华为的产品如含有开源软件，则须对其开源软件的漏洞进行及时检测，并对存在的安全漏洞进行修复或升级到无漏洞的新开源软件版本。 |
| 2、提供开源软件名称、版本号列表 |
| 6 | 协议与接口 | 通信矩阵 | 1、提供清单列举物料所有功能/特性所使用到的端口； |
| 2、未在通信矩阵中描述的端口应关闭。 |
| 协议安全 | 1、系统的管理平面和近端维护终端、网管维护终端间，支持使用合适的安全协议（如SSH v2/TLS1.1/IPSec/SFTP/SNMPv3等） |
| 端口接入认证 | 能对系统进行管理的物理/逻辑端口/协议，应提供接入认证机制，标准定义无认证机制的除外。 |
| 协议健壮性 | 对与终端用户有交互或者与非信任网络互联的容易受攻击的协议，使用工具（如，Codenomicon）进行畸形报文攻击测试，测试结果不得出现致命或严重级别的问题，提供测试结果。（如提供此功能，为必须满足项，如不提供该功能，可不涉及） 这些协议和版本包括但不限于（请去掉物料无关的协议、补充相关的协议）： BGP, Diameter, DNS, DVRMP, EAP, FTP, GRE, GTP, H.225, H.248, H.323, HTTP, ICMP, IMAP, IPSec, IPv4, IPv6, IS-IS, ISAKMP/IKE, LDAP, MGCP, MPLS/LDP, NTP, OSPF, PIM, POP3, RADIUS, RIP, RSVP, RTP, RTSP, SIGCOMP, SIP, SNMP, SMTP, SSH, SSL/TLS, TACACS, TR-069, XML/SOAP, WAP. |
| 7 | 敏感数据与加密 | 加密算法清单 | 提供物料所使用的加密算法清单，说明加密算法的应用场景。 |
| 私有密码算法 | 禁止使用私有算法实现加解密，包括但不限于： 1. 自行定义的通过变形/字符移位/替换等方式执行的数据转换算法； 2. 用编码的方式（如Base64编码）实现数据加密的目的的伪加密实现。 |
| 不安全密码算法 | 禁止使用业界已知不安全的加密算法,DES/3DES（除密钥K1≠K2≠K3外的场景）/SKIPJACK/RC2/RSA（1024位及以下）/MD2/MD4。。因标准协议定义且没有替代算法、需要与第三方系统对接、兼容老系统等情况需要使用不安全密码算法的，应在加密算法清单中说明。 |
| 敏感数据存储安全 | 认证凭据（如口令/私钥等）不允许明文存储在系统中，应该加密保护。对于认证凭据的安全存储，在不需要还原明文的场景，必须使用不可逆算法加密。对敏感数据的访问，需采取适当的安全机制（如认证、授权或加密等）。 |
| 敏感数据传输安全 | 在非信任网络之间进行敏感数据（包括口令，银行帐号，批量个人数据等）的传输须采用安全传输通道或者加密后传输，有标准协议规定除外。 |
| 密钥安全 | 用于敏感数据传输加密的密钥，不能硬编码在代码中，应提供密钥管理或密钥协商的机制。 |
| 8 | 隐私保护 | 个人数据转移 | 1、不得未经用户授权对外传送用户的个人数据，传送功能/特性应允许关闭； |
| 2、对外传送个人数据的类型、目的、实现和管理机制应在资料中公开。 |
| 9 | 口令安全 | 口令复杂度检查 | 物料涉及到操作维护类口令的，应默认检测口令复杂度，口令至少满足如下要求： 1、口令长度至少6个字符； 2、口令必须包含如下至少两种字符的组合:  －至少一个小写字母；  －至少一个大写字母；  －至少一个数字；  －至少一个特殊字符：`~!@#$%^&\*()-\_=+\|[{}];:'",<.>/? 和空格 3、口令不能和帐号一样； 若设置的口令不符合上述规则，必须进行警告。 缺省口令也应符合复杂度要求。 对于输入受限、符合业界惯例的场景，不强制要求口令复杂度。 |
| 用户锁定机制 | 支持设置口令出错锁定阈值，提供锁定用户的机制。当重复输入错误口令次数(如3次）超过阀值时采取合适保护措施。保护措施可参考： 1）锁定帐号； 2）锁定IP； 3）登录延迟； 4）验证码； 5）IP白名单。 |
| 口令加密存储 | 1、 口令需加密保护，不能够明文写入日志文件、配置文件以及cookie中； |
| 2、 口令文件必须设置访问控制，普通用户不能读取或拷贝加密的内容； |
| 3、 操作界面中的口令不能明文显示； |
| 4、 口令输入框内容禁止拷贝； |
| 口令安全传输 | 口令不能在网络中明文传输。 |
| 口令修改 | 1、用户修改自己口令时必须验证旧口令。 |
| 2、不允许修改除自身账号以外的账号的口令（管理员除外）。 |
| 账号口令清单 | 提供账号口令清单。 |
| 10 | 日志审计 | 管理面所有对系统产生影响的用户活动、操作指令必须记录日志 | 涉及以下用户活动和操作指令的需要记录日志： 用户活动包括： 1、登录和注销； 2、增加、删除用户和用户属性（帐号、口令等）的变更； 3、用户的锁定和解锁，禁用和恢复； 4、角色权限变更； 5、系统相关安全配置（如安全日志内容配置）的变更； 6、重要资源的变更，如某个重要文件的删除、修改等。 操作指令包括： 1、对系统配置参数的修改； 2、对系统进行启动、关闭、重启、暂停、恢复、倒换； 3、对业务的加载、卸载； 4、软件的升级操作，包括远程升级和本地升级； 5、对重要业务数据（特别是与财务相关的数据，包括：卡号、余额、话单、费率、费用、订单、出货、帐单等）的创建、删除、修改； 6、所有帐户的命令行非查询操作命令。 |
| 日志内容要能支撑事后的审计 | 日志内容要能支撑事后的审计，记录包括用户ID、时间、事件类型、被访问资源的名称、访问发起端地址或标识、访问结果等。 |
| 日志要有访问控制 | 1、日志要有访问控制； |
| 2、禁止日志模块提供修改日志记录的能力； |
| 3、日志如果允许删除，删除权限须控制在管理员或者系统。 |
| 12 | 安装和配置管理 | 软件安装 | 1、 安装软件过程中对用户权限有要求，以权限最小化原则进行软件安装，对于需要有管理员权限安装软件，需要说明原因。 |
| 2、 软件安装完成后，删除临时文件或备份文件，若要保留，需说明原因。 |
| 配置管理 | 1、物料对特定的文件系统以及系统中的功能软件等有依赖，所依赖特定版本的其他软件不能有严重漏洞。 |
| 2、根据最小权限原则，运行软件程序的帐号应该是一个分配最小权限（只分配了必须的权限）的操作系统帐号，而不应该是root等高权限帐号。 |
| 3、物料提供安全配置/加固指南和安全维护手册等文档。 |
| 13 | 用户管理 | 软件用户的隔离 | 软件的用户管理应保证不同用户的信息隔离以及权限分离，防止横向或纵向越权。 |

#### 网络安全标准

|  |  |
| --- | --- |
| **编号** | **网络安全标准详述** |
| 1 | 对于人机接口以及可远程访问的机机接口，不得存在用户无法修改的口令（含程序中的硬编码口令）。 |
| 2 | 对于出厂时缺省设置的帐号/口令或用于传输的加密密钥，产品必须提供客户修改机制，产品CPI资料中应提醒用户修改及定期更新，并提示风险。 |
| 3 | 如果采用解释性语言（如Shell/python/perl脚本、jsp、html等）实现，对于不满足“未公开接口”并需要清理的功能，必须彻底删除，严禁使用注释行等形式仅使功能失效。 |
| 4 | 认证凭据（如口令/私钥等）不允许明文存储在系统中，应该加密保护。 |
| 5 | 禁止使用私有密码算法实现加解密，包括： 1. 自行定义的通过变形/字符移位/替换等方式执行的数据转换算法； |
| 6 | 2. 用编码的方式（如Base64编码）实现数据加密的目的的伪加密实现。 |
| 7 | 用于敏感数据传输加密的密钥，不能硬编码在代码中，应提供密钥管理或密钥协商的机制。对于云服务产品，产品CPI资料中应提醒用户修改及定期更新，并提示风险。 |
| 8 | 日志记录需涵盖管理面上所有的用户活动，包括：  1、登录和注销； |
| 2、系统相关安全配置（如安全日志内容配置）的变更； |
| 3、重要资源的变更，如某个重要文件的删除、修改等。 |
| 9 | 日志记录需涵盖管理面上所有的操作指令，包括：  1、对系统配置参数的修改； |
| 2、对系统进行启动、关闭、重启、暂停、恢复、倒换； |
| 3、对业务的加载、卸载； |
| 4、软件的升级操作，包括远程升级和本地升级； |
| 5、对重要业务数据（特别是与财务相关的数据，包括：卡号、余额、话单、费率、费用、订单、出货、帐单等）的创建、删除、修改； |
| 6、所有帐户的命令行非查询操作命令。 |
| 10 | 管理面用户活动、操作指令的日志应支持回溯审计，至少包含下列内容： |
| a. 事件发生的时间； |
| b. 用户ID； |
| c. 访问发起端地址或标识(如关联终端、端口、网络地址或通信设备等）； |
| d. 事件类型； |
| e. 被访问的资源名称； |
| f. 事件的结果。 |
| 11 | 说明： 1）对于第三方OS/DB，如果不支持记录日志、记录内容不全或者启用记录存在严重性能影响，且风险可控，不强制要求。 |
| 2）如果系统是单用户或者没有用户的概念，可不涉及用户ID。 |
| 3）当目标设备是通过代理进行访问时，可以只记录代理的地址或标识。 |
| 12 | 产品对于每一个需要授权访问的请求都需核实用户的会话标识是否合法、用户是否被授权执行此操作。 |
| 说明： 1）请求是否需要鉴权，由产品根据具体业务需要以及安全风险确定。 |
| 2）对于图标、CSS文件、静态页面或JavaScript等，如果公开后没有安全风险，不强制认证鉴权。 |
| 13 | 对用户的最终认证处理过程必须在服务器端进行。 |
| 14 | 若输出到客户端或者解释器的数据来自不可信的数据源，则须对该数据进行相应的编码或转义。 |
| 说明：产品根据实际输出的目标位置，使用ESAPI或Web安全框架中提供的相应的编码接口对不可信数据进行编码。如自己实现，至少确保对&、<、>、"、'、(、)七种特殊字符进行编码。 |
| 15 | 用户登陆认证通过后必须更换会话标识，以防止会话固定（session fixation）漏洞。 |
| 说明：已经登录成功的用户，如果需要对重要操作进行二次认证，不强制要求更换会话标识（例如：锁定后解锁的场景、修改口令时验证旧口令的场景、涉及大金额或重要业务操作需要再次认证的场景）。 |
| 16 | 产品出厂使用的数据库口令不得使用数据库厂商的缺省口令，且设置的口令符合口令复杂度要求。 |
| 17 | 产品应缺省启用数据库口令复杂度检查功能，若口令不符合复杂度规则，必须禁止设置并进行警告。 |
| 19 | 如果产品支持关闭复杂度检查机制，对于云服务产品，应在CPI资料中提示风险。 |
| 说明：对于仅能本地访问的数据库，不强制满足口令复杂度要求。 |
| 20 | 数据库若存在多个默认帐号，必须将不使用的帐号禁用或删除。 |
| 21 | 使用操作系统的非管理员权限帐号来运行数据库。 |
| 22 | 数据库系统本身的文件（如$SYBASE、$ORACLE\_HOME等）及用户的数据文件需要严格控制访问权限，只有数据库进程运行帐户以及管理员帐户才具备读写权限； |
| 23 | 对数据库帐户授予的权限进行严格清晰的划分，所有数据库帐户只能具备执行其任务的最小权限。 |
| 1、禁止使用业界已知不安全的加密算法,DES/3DES（除密钥K1≠K2≠K3外的场景）/SKIPJACK/RC2/RSA（1024位及以下）/MD2/MD4。 |
| 说明： |
| 1）禁止MD5应用在参与生成“数字签名、口令加密保存”这两种场景（HMAC-MD5例外），禁止SHA1应用在参与生成“数字签名”的场景； |
| 2）SHA1算法可用于HMAC、PBKDF2、随机数发生器的场景； |
| 3）标准协议定义且没有替代算法的、或需要与第三方系统对接、或兼容老系统的除外。如需要与第三方系统对接或兼容老系统，产品支持使用不安全密码算法的情况，对于云服务产品，应在产品CPI资料或界面中提示风险。 |
| 2、推荐使用的密码算法：  1）分组密码算法：AES（密钥长度在128位及以上）  2）密钥交换算法：DH（2048位及以上)  3）非对称加密算法：RSA（密钥长度在2048位及以上)  4）流密码算法：AES（密钥长度在128位及以上）（OFB或CTR模式）  5）哈希算法：SHA2（256位及以上）  6）HMAC（基于哈希的消息验证码）算法：HMAC-SHA2 |
| 3、缺省使用安全的加密算法，如客户选择不安全的加密算法，应提示安全风险。 |
| 认证凭据不需要还原的场景（例如认证端保存的用户登录口令），必须使用PBKDF2或公司密码学专家组认可的更强的算法加密，对于性能极其敏感且安全性要求不高的场景允许使用HMAC（口令，盐值）（注：口令、盐值位置可以互换）。 |
| 24 | 密钥不允许明文存储在系统中，应该加密保护并提供访问控制。  说明： 1）硬编码密钥暂不要求。  2）对开源软件中密钥的加密保护不作强制要求。 |
| 25 | 在输入错误的用户名或密码时，不能出现类似于“密码错误”、“用户名不存在”之类的过于明确的原因提示信息，以防止攻击者用于猜解系统用户名/口令。 |
| 26 | 下列场景不违反本条红线要求： 1）因登录失败而提示帐号锁定的场景； |
| 2）不存在猜解口令的风险的场景，如Linux操作系统下以su方式登录时可以提示用户名无效。 |
| 27 | 对于系统自身操作维护类的口令： 1）图形界面缺省不能明文显示用户键入的所有口令； |
| 2）交互式命令行界面不能明文显示用户在登录过程中键入的登录口令； |
| 28 | 系统提供的口令输入框不支持口令拷出。 |
| 29 | 系统预置帐号的缺省口令（包括操作系统、数据库、业务系统），口令应符合复杂度的要求，如果不能满足口令复杂度则需要在用户首次登录时强制修改，客户明确定制的除外。 |
| 30 | 用户（包括管理员）修改自身口令前需再次验证旧口令。 |
| 31 | 管理员重置其他用户的口令，无需验证旧口令。 |
| 32 | 用户仅可以修改自身帐号的口令，管理员除外。 |
| 33 | 如系统支持文件访问控制，口令文件必须设置访问权限，普通用户不能读取或拷贝加密的内容。 |
| 34 | 系统的管理平面和近端维护终端（如LMT）、网管维护终端间，支持使用合适的安全协议（如SSHv2/TLS1.1/IPSec/SFTP/SNMPv3等）进行通信。建议缺省启用安全协议。 |
| 35 | 对于公司指定的不安全协议，支持关闭，建议缺省关闭。 |
| 36 | 公司指定的不安全协议有：FTP、Telnet和SSHv1.x。 |
| 37 | 修改自身口令的帐号只能从服务器端的会话信息中获取，而不能由客户端指定。 |
| 38 | 1、待修改口令的用户名或用户ID等禁止从请求报文里获取，应从服务器中的会话信息中获取。 |
| 39 | 对于管理面人机登录的场景（如近端维护终端、网管维护终端、网管登录Portal、系统维护工具等），在登录界面禁止提供“自动登录/记住我”功能 |
| 40 | 运行程序的帐号（OS帐号）不能拥有远程登录的权限 |
| 41 | 会话标识必须使用安全随机数算法生成，且有效长度不少于24个字符（或192bits） |
| 42 | 会话标识需要进行安全传输 |
| 43 | B/S 应用中，必须使用cookie 用于维持会话 |
| 44 | B/S 应用中，会话cookie的属性要设置为“HttpOnly”，“Secure”、域和路径 |
| 45 | 请求必须要使用token防止csrf攻击，必须使用会话Token对敏感或关键的操作进行校验，会话Token必须使用安全随机数算法生成、有效长度不少于24个字符（或192bits），且需要设置有效期 |
| 46 | 所有登录后才能访问的界面都必须提供主动退出选项，当用户退出时，服务器端必须清除该用户的会话信息 |
| 47 | 必须设置会话超时机制，在超时过后必须要清除该会话信息 |
| 48 | 禁止使用SSL2.0、SSL3.0协议，TLS1.0协议仅可遗留使用 |
| 1、禁止使用SSL2.0和SSL3.0协议。 |
| 2、TLS1.0仅在向下兼容、第三方对接等场景下可遗留使用。 |
| 49 | 密钥的生成、使用、更新、销毁等操作需记录详细的日志 |
| 50 | 在B/S系统中，如果提交的数据中包含个人数据，则禁止使用Get方式提交个人数据 |
| 51 | 禁止在URL、日志、错误消息、调试信息中暴露口令、密钥、银行账号、会话标识符等敏感信息 |
| 52 | 日志中禁止明文记录敏感数据 |
| 1、敏感数据（包括口令、对称密钥、预共享密钥、私钥、银行帐号、敏感个人数据、Session ID等）禁止明文记录在日志中。 |
| 2、口令禁止加密/哈希后以密文记录日志。 |
| 53 | 通过ICSL安全送检 |
| 54 | 安全风险响应，对产品Bug或设计等导致的安全漏洞和风险进行及时响应和处置。原则上修复时间不超过5个工作日。 |

### 系统安全需求

系统的安全需求是指整个系统网络操作系统和网络硬件平台对安全的需求。目前没有绝对安全的操作系统可以选择。需要根据不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置。同时也必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

### 应用安全需求

应用系统的安全与具体的应用有关。本系统是面向多用户、包括多种通用软件、行业专业软件的综合应用系统，随着应用系统的不断发展，其应用类型是不断增加的。因此应用系统的安全是动态的、不断变化的。在应用系统的安全性上，尽可能建立安全的系统平台，尽量选用国产设备和系统，而且通过专业的安全工具不断发现漏洞，修补漏洞，提高系统的安全性。

应用系统的安全性也涉及到信息的安全性，包括信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。因此需采用多层次的访问控制与权限控制手段，实现对数据的安全保护，保证网上传输的信息（包括管理员口令与账户、上传信息等）的安全性。

### 管理安全需求

管理是网络安全中最重要的部分。责权不明、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其它一些安全威胁时(如内部人员的违规操作等)，无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求必须对网络门户的访问活动进行多层次的记录，及时发现非法入侵行为。

# 总体设计方案

## 概述

根据《[国家电子政务总体框架](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E6%80%BB%E4%BD%93%E6%A1%86%E6%9E%B6/14593108)》、《政务信息资源目录体系》、《政务信息资源交换体系》等国家标准规范的要求，为了实现政务信息资源的统一采集、梳理、质量治理、清洗、编目、合理共享、交换、管理、应用、分析，需要进行目录子系统和交换子系统等系统的建设，我们将核心和基础的目录子系统和交换子系统构成的有机整体，合称为政务信息资源共享交换平台。共享即各政务部门将信息资源统一整合后，将原则上可共享的信息资源目录和数据，共享在各部门的前置机共享信息库中，目录服务中心统一提取目录，提供资源的检索、定位功能，交换，即是指需要使用对应信息资源的政务部门，检索到对应资源后，提交审请，经审核通过授权后，由交换子系统，通过电子政务路由和网络，将提供方共享的对应信息资源，交换传输到申请使用方政务部门的前置机信息库中，以供使用方使用，最终实现通过资源共享和交换，所有参建政务部门获取所需共享的政务信息资源。

## 总体框架

政务信息资源共享交换平台的构成主要包括：目录子系统、交换子系统、统一数据对账系统、数据质量工单管理系统、统一监控系统、统一运维系统等。



(政务信息资源共享交换平台总体框架图)

## 高性能设计

### 总体架构的高性能设计

 1、可采用2台商用的硬件（如F5）实现四层负载均衡，也可采用软件方式实现四层或七层负载均衡。但不管采用硬件或软件的，都要基于心跳机制实现主、备的负载均衡服务以防止单点故障。

2、关系数据库集群通常基于ORACLE RAC实现ORACLE数据库的集群，基于Mysql Cluster实现MySql数据库的集群,本项目支持使用华为Paas平台提供的关系数据库集群。

3、基于MapReduce原理实现并行计算框架构，基于Google GFS原理实现分布式文件系统。

4、构建多级缓存机制，在应用服务器端可缓存常用的、小容量数据，公用数据可缓存在集中服务器（主、备方式）由各应用服务器统一使用，当缓存的数据量非常大时可建立分布式缓存集群。

### 应用服务器的高性能设计

#### 应用服务器集群

使用2台Web服务器（主、备方式）做负载均衡，分发客户端访问请求至后端的应用服务器集群。

应用服务器集群需解决会话（SESSION）共享问题。可通过应用服务器本身提供的会话复制机制来实现会话共享问题，或是采用粘性（Sticky）会话模式,即同一个用户的访问请求都被派送到同一台服务器。另外一种方式是使用独立的服务器来存储所有访问涉及到的会话，应用服务器统一从这里读取会话数据。

#### 系统拆分

单个应用系统变得越来越来越庞大，业务越来越复杂，随着数据量和并发量的不断提升，最终会导致简单的使用集群也不能解决性能问题。因此需按照业务功能，将应用系统拆分成更小的应用系统，再将这些更小的应用系统在应用服务器集群中部署和运行。

### 数据库的高性能设计

#### 读写分离

让主数据库（写库）处理事务性增、删、改操作，而从库（读库）只处理查询操作，把事务性操作导致的变更从主数据库同步到从数据库中。对于读远远大于写操作的应用来说，采用读写分离，再结合缓存的模式，会大大提高应用性能的性能。

#### 数据库拆分

把一个数据库切分成多个部分放到不同的数据库，从而缓解单一数据库的性能问题。对于表多数据也多的业务型数据库可以采取垂直切分，将关系紧密的表的表切分出来放在一个数据库中。但如果是一些表少数据多的主题库或共享库，则可以采取水平切分，即把表的数据按某种规则（比如按日期或ID散列）切分到多个数据库。也可综合使用垂直和水平切分，从而将原有数据库切分成类似矩陈列一样可以无限扩充的数据库。

### 多级缓存与静态化

#### 多级缓存

将应用系统经常要使用的数据或对象缓存在内存中，但下次需要使用时，可以不必从数据库中读取数据或重新创建对象。减少系统开销，提高系统效率。

构建多级缓存机制，在应用服务器端可缓存常用的、小容量数据，公用数据可缓存在集中服务器（主、备方式）由各应用服务器统一使用，当缓存的数据量非常大时可建立分布式缓存集群。

 根据规则将缓存存储到不同的集群中。同一个集群中的每台缓存服务器数据保存同步，防止单点故障。

#### 动态页面静态化

效率最高、消耗最小的就是纯静态化的HTML页面，所以我们要采用技术手段使WEB应用的动态页面静态化。



## 关键技术路线

### B/S结构

B/S（Browser/Server）结构即浏览器和服务器结构。它是随着Internet 技术的兴起，对C/S 结构的一种变化或者改进的结构。在这种结构下，用户工作界面是通过WWW 浏览器来实现，极少部分事务逻辑在前端（Browser）实现，但是主要事务逻辑在服务器端（Server）实现，形成所谓三层3-tier 结构。这样就大大简化了客户端电脑载荷，减轻了系统维护与升级的成本和工作量，降低了用户的总体成本（TCO）。

以目前的技术看，局域网建立B/S 结构的网络应用，并通过Internet/Intranet 模式下数据库应用，相对易于把握、成本也是较低的。它是一次性到位的开发，能实现不同的人员，从不同的地点，以不同的接入方式（比如LAN,WAN,Internet/Intranet 等）访问和操作共同的数据库；它能有效地保护数据平台和管理访问权限，服务器数据库也很安全。特别是在JAVA 这样的跨平台语言出现之后，B/S 架构管理软件更是方便、快捷、高效。B/S 模式管理信息系统基本上克服了CS 模式管理信息系统的不足，其主要表现在：

1、系统开发、维护和升级的经济性对于大型的管理信息系统，软件开发、维护与升级的费用是非常高的，B/S 模式所具有的框架结构可以大大节省平台开发建设费用，同时，B/S 模式对前台客户机的要求并不高，可以避免盲目进行硬件升级造成的巨大浪费。

2、B/S 模式提供了一致的用户界面B/S 模式的应用软件都是基于Web 浏览器的，这些浏览器的界面都很相似。对于无用户交互功能的页面，用户接触的界面都是一致的，从而可以降低软件的培训费用。

3、B/S 模式具有很强的开放性，在B/S 模式下，外部的用户亦可通过通用的浏览器进行访问。

4、B/S 模式的结构易于扩展由于Web 的平台无关性，BS 模式结构可以任意扩展，可以从一台服务器、几个用户的工作组级扩展成为拥有成千上万用户的大型系统。

5、B/S 模式具有更强的信息系统集成性在B/S 模式下，集成了解决企事业单位各种问题的服务，而非零散的单一功能的多系统模式，因而它能提供更高的工作效率。B/S 模式提供灵活的信息交流和信息发布服务，B/S 模式借助Internet 强大的信息发布与信息传送能力可以有效地解决企业内部的大量不规则的信息交流。

B/S 模式整体架构图：



(图：B/S 模式整体架构图)

### 基于Hadoop的大数据平台框架

结合当前国内外主流大数据平台软件均能够满足海量存储、快速计算、可视化运维等通用性需求的现实情况，大数据服务支撑平台应满足两类需求：一是当前建设的综合性需求，即综合考虑平台的可替代性、与相关业务应用的适配性、规模化承载实践、平台安全支撑能力等因素，满足现阶段应用建设需求；二是长远发展的主流性需求，即要紧密结合当前大数据平台技术飞速发展、尚未形成平台标准的特点，尽可能地使所选择的大数据平台能够保持业界主流和引领地位，满足今后一个时期扩展建设的需求。

同时考虑到未来汇聚的公共数据信息量大、数据类型多种多样，从大规模数据、复杂关联查询、即席查询的需求考虑，基础支撑平台技术选型上要求采用有基于开源社区的Hadoop技术为基础进行搭建，以具备开放融合的数据采集、数据存储、数据分析的服务能力。支持并兼容业界主流的华为FunsionInsight平台

### 基于Java EE开发

基于目前主流的JavaEE 架构，采用三层架构的模式实现。Java EE 是SUN 公司提出的一套企业级JAVA 技术应用平台和规范，经过业界多年的使用验证，已经趋于成熟，是一套有效的实用的系统架构平台。三层架构的实现模式，就是把系统分为表示逻辑层、业务逻辑层、实体数据层三层表现方式，实现系统高内聚、低耦合的目标。使系统具有扩展性、健壮性、可维护性、可复用性等多种优点。集中表现在：

1. **可移植性：**

跨操作系统、跨数据库、跨应用服务器；开发人员可以开发运行在支持Java EE 平台的任何系统之上的产品。不需要额外的付出，其产品就可以运行在多种系统平台上；

1. **可扩展性：**

应用软件的可扩展性、应用系统的可扩展性、物理系统的可扩展性；可移植性组件技术使IT 应用独立于供应商，使IT 机构不再依赖某一个供应商；

1. **安全服务：**

权限认证、安全日志、数据加密； 采用 Java EE 平台可以保护政府的投资，因为它是一个工业标准，而不是某个供应商特有的结构；这个分布式计算的标准开发平台保证了所有开发的应用系统都是建立在成熟的平台之上；

1. **可重用性：**

Java EE 的组件技术使系统的可重用性大为提高；

1. **运行效率：**

高并发下的高效率、大数据量下的高效率、批量数据处理的高效率。

### 基于SOA架构思想的共享服务模式

采用面向服务架构（SOA，Service-Oriented Architecture），松耦合的设计分析方法，完成政务大数据平台的分析与设计，保证系统的灵活性、可扩展性和良好的维护性。所以系统整体设计需要灵活的适应各业务场景变化及新增需求快速响应及扩展、设计以业务角色驱动的系统模型、提供给不同工作岗位、相同岗位不同工作内容的人员的个性化服务需求。

### 采用XML格式作为消息传递标准

XML（extensible markup language 扩展标记语言）是由SGML（standard

generalized markup language）对应internet 的需求定义的一种通用文档语言，它的提出主要是解决那些在HTML 中无法完成的应用，主要包括以下四类：

* 需要WEB 客户在两个或多个异种数据库间操作的应用。
* 由WEB 客户分担相当比例的WEB 服务器处理任务的应用。
* 需要向WEB 客户呈现同一数据对不同用户的不同显示的应用。
* 智能WEB 代理试图使发现的信息和个人用户的需求相符合。

XML 主要有三个元素：DTD（document type definition）或XMLschema(XML

模式)、XSL（extensible stylesheet language 可扩展样式语言）和XLINK（extensible link language 可扩展链接语言）。DTD 和XML 模式规定了XML 文件的逻辑结构，定义了XML 文件中的元素、元素的属性以及元素和元素属性之间的关系；namespace(域名)实现统一的XML 文档数据表示以及数据的相互集成；

XSL 是用于规定XML 文档呈现样式的语言，它使得数据与其表现形式相互独立；

而XLINK 将进一步扩展WEB上已有的简单链接。

XML 实际上是一种元语言,可以用来创建其它语言,这些语言可以描述数据结构：以围绕它们的标记符及其属性描述的数据元素的层次结构。因为XML 数据有这种"自描述的"特性，它比传统的以行和列为格式的数据容易理解，因而比较容易开发、维护和共享。

XML 还提供在应用程序和系统之间传输结构化数据的方法。像客户信息、信息查询这类数据能够转换成XML 并在应用程序间共享，而无需改变原来遗留下来的系统。这个优点非常适合将来系统信息共享和综合利用的需求。

XML 词汇，也称数据格式，是标准的用于特殊的应用程序或工业的元素集合。该词汇是能够使应用程序和商业合作伙伴之间产生互操作性的公用语言。公用数据字典相当于XML 词汇的工作，为了对词汇进行统一管理，因此引入了数据字典的概念，数据字典是XML 词汇的数据库表示，XML 词汇是公用数据字典在WEB 中的具体表现。XSLT是XSL的一部分，是一种用来进行XML 文档间相互转换的语言，通过XSLT，可实现异构系统、异构数据库间的信息转换和沟通。

XML是一种可以对信息进行自我描述的语言。它允许定义一套符合自己需载体。标记用于界定内容。XML 语法允许自行定义任意复杂的标记结构。XML 使用普通的文本，而不是二进制的数据格式，因此具有跨系统的优点。

XML的优点在于：

规范、简单。XML文档有一套严谨而简洁的语法结构。这为XML解析器获取文档所含信息提供了前提。

可扩展性。应用者可以按照需求定义自己的标记，而不像html一样其标记都是预先定义的。

自描述性。自描述性使其非常适用于不同应用间的数据交换，而且这种交换是不以预先规定一组数据结构定义为前提，因此具备很强的开放性。

XML意义在于它可以把所有信息都存在于文档中，采用http 的方式传输；而远程的应用程序又可以从中提取需要的信息。因而，XML 为异构数据库系统在Web 方式下的应用提供了有利条件。XML 实质上是一种将多个数据库和数据库模型集成为一种统一的数据库视图的方法，它在分布的数据库和应用之间放置一个中间件层，该层与每一个后台的数据库用其自带的接口相连，并将分布的数据库映射为一种统一的虚拟数据库模型，而这种虚拟模型只在中间件中存在。各应用就可以使用该虚拟数据库去访问需要的信息。同时，该数据聚合软件也可以通过将相关数据映射和导入实体数据库，进行数据库更新。

这种基于XML的数据集成框架如下图所示：



(图：XML 数据集成层次示意图)

整个集成框架可以分为三个层次：其中最底层为信息抽取层，中间为中介层，最上层为用户接口层。

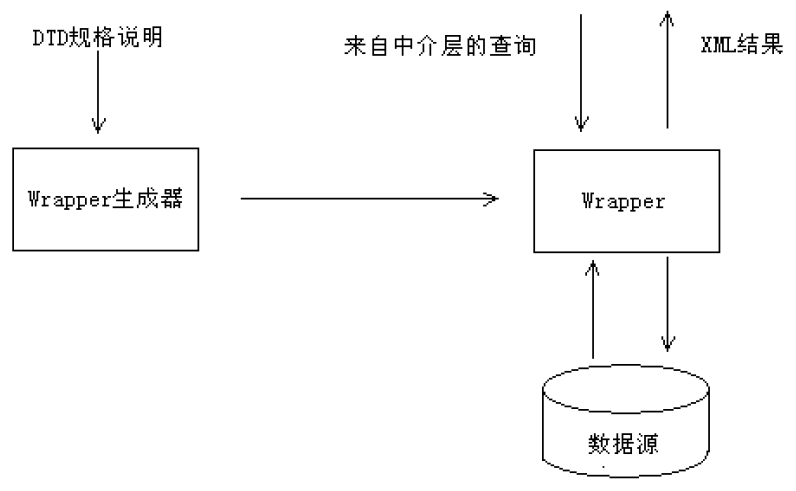
a) 信息抽取层

信息抽取层处于系统的最低层，是系统的数据提供者，主要功能是提取和集成分布在多个异构数据源(数据库，知识库及构件库)上的信息。这一层采用

Wrapper(包装器)技术实现将一个从中介层得到的查询，翻译成能在经过封装的数据源上执行的操作，将查询结果抽取并打包到一个XML 文档，最后将该文档返回给中介层。

信息抽取层的Wrapper 组件由两部分组成：Wrapper 生成器和Wrapper 实例(简称Wrapper)。如下图所示，一个Wrapper 位于中介层和一个数据源的中间，

它通常为中介层查询异构信息源集合提供一个公共接口。每个Wrapper 都要为某个特定的数据源制定相应的接口，这个功能是由Wrapper 生成器完成的。



(图：Wrapper 生成器和Wrapper)

Wrapper 生成器用于为查询某个确定的站点或站点集合构建Wrapper。

Wrapper 的输入是用一种Wrapper 规范语言书写的规格说明，包括关于将要为之生成的Wrapper 的数据源的元信息，该元信息描述了如何从一个数据源请求服务以及如何抽取和解释从数据源返回的信息。规格说明还必须能够表达以下内容：

数据源接口、数据模型、从用户到数据源本地操作的查询映射、数据源的查询能力。通常为一个数据源生成一个有效的Wrapper 所必须的信息是使用DTD 来描述的。Wrapper 生成器的输出是一个可以执行的 Wrapper，该Wrapper 能够接受由Wrapper 规范语言定义的查询。

b) 中介层

中介层(Mediation Layer)的主要功能有两方面：一方面对上接受用户通过

DOM 客户端API 向系统提交的或应用程序发出的查询，将其转换成对XML 的查询，并将查询结果返回给用户或应用程序；另一方面对下将XML 查询分发给各个包装器，并将查询结果通过DTD 说明再转换成XML 格式。

c) 用户接口层

用户接口层(User Interface Layer)在中介层之上，负责将用户的查询命令提交给中介层，获得并解释查询结果树，并将结果显示给用户。XML DOM(DocumentObject Model，文档对象模型)是为合法的格式良好的XML 文档设计的一套API(Application Programming Interface,应用程序接口)，它同时定义了这些文档的逻辑结构，访问及操作方法。由于数据显示与内容分开，XML 定义的数据允许指定不同的显示方式，使数据更合理的表现出来。本地的数据能够以客户配置，使用者选择或其他标准决定的方式动态的表现出来。CSS 和XSL 为数据的显示提供了公布的机制。在此设计中，XML 作为实现跨系统信息交换和提高异构系统之间的互操作性的最佳解决方案的提出，极大地促进了数据交换应用的发展。而基于XML 强大的可扩展性而提出的XML 安全服务标准，使我们可以在考虑XML 数据信息交换的安全控制问题上，完全采用基于XML 标准的体系结构，继承XML 的灵活性和可扩展性。而且，SOA 架构中业务请求和应答的描述标准均支持采用XML 的格式，如在Web 服务体系中的Web 服务描述语言（WSDL）、简单对象访问协议（SOAP）等协议标准，均是基于XML 数据格式的。因此在业务接口规范的选择上，我们根据国家《政务信息资源交换体系》标准采用XML 格式。

### 基于XML的信息交换

信息交换就是将各类信息进行统一的封装、传输、路由与交换的技术或标准。信息交换是应用支撑层的基础功能，在此基础上才能实现其它功能（如业务注册与发现、流程控制等）。由于本指南采用XML 信息表示方式，所以这里定义的信息交换实际上是指XML 信息交换。

信息交换作为一个协议层次（称为信息交换层）单独提出来，是有一定现实意义的。一方面，各种不同的应用系统需要进行数据交换，如果没有统一的报文封装格式，每个系统需要创建和维护多种报文格式以便与其它应用系统交流；另一方面，底层物理网络的多样性（Internet、GSM、PSTN 等），需要有一种统一的机制实现不同网络之间的数据交换，既能屏蔽物理网络协议，又能实现不同物理网络之间的信息融合。

信息交换主要解决下面几个问题：

* 信息的统一封装：只有统一了封装格式，才可能进行统一的交换。就像邮政信函业务，其前提条件是大家必须按规定格式填写信封。
* 统一编址问题：统一的地址编码是屏蔽物理网络的内在需求，也是进行统一信息交换的基础。如何设计一套统一的、简单易用、易扩展、易管理的地址编码体系，是实现信息交换的关键。
* 信息的可靠传输：信息交换层是为上层应用提供信息交换服务的，所以将信息可靠地传输到目的地址是基本要求。也就是说，信息交换层必须实现通信中间件（或消息中间件）的功能，而现有的IP/TCP/HTTP 协议并没有实现此功能。
* 信息路由问题：在一个大的信息交换网络中，可能会有许多信息交换节点，当某个信息需要通过多个节点到达目的地时，就出现了路由寻址的问题。
* 信息交换与传输的效率问题：信息交换关心的是信息的传输与交换，而不是信息本身的含义。为了实现高速的信息交换，需要将信息的表示与交换分开，同时采用专门的信息交换设备来提高性能。信息交换应该具有充分的灵活性，可根据实际需要组建多节点交换网络以提高总体交换性能。另外，信息在传输过程中需要通过压缩来提高传输速度。

信息交换的可管理性问题：提供日志、审计、会话管理、信息交换事务的一致性等。为了解决上面这些问题，XML 信息交换包由包头（信封）和包体（信体）组成，信息交换层只关心包头的内容。包头依照《电子政务信息资源交换体系国家标准》的消息寻址协议进行定义，用于交换传输子系统的寻址与定位，包体包含其他应用支撑层的信息或应用层各种与具体业务相关的数据。

基于云平台

### 基于REST架构

REST描述了一个架构样式的互联系统，如：Web应用程序。REST约束条件作为一个整体应用时，将生成一个简单、可扩展、有效、安全、可靠的架构。由于它简便、轻量级以及通过HTTP直接传输数据的特性，RESTful Web服务成为基于SOAP服务的一个最有前途的替代方案。用于web服务和应用程序的多层架构可以实现可重用性、简单性、可扩展性、和组件可响应性的清晰分离。开发人员可以轻松使用Ajax和RESTful Web服务一起创建丰富的界面。

### 基于云服务架构

云服务主要用于支撑显示层、也可以直接让用户调用，并主要有五种技术：

* **REST**:通过REST技术，能够非常方便和优雅的将中间层所支撑的部分服务提供给调用者。
* **多租户**：能让一个单独的应用实例可以为多个组织服务，而其保持良好的隔离性和安全性，并且通过这种技术，能有效地降低应用的购置和维护成本。
* **并行处理**：为了处理海量数据，需要利用庞大的集群进行规模巨大的并行处理，Hadoop中的MapReduce是这方面的代表。
* **应用服务器**：在原有的应用服务器基础上为云计算做了一定程度的优化，比如用Tomcat、Jetty应用服务器。
* **分布式缓存**：通过分布式缓存技术，不仅能有效的降低对后台服务器的压力，而其还能加快相应的反应速度，最著名的分布式缓存例子莫过于Memcached。
* **虚拟化**：可以理解为基础设施层的“多租户“，因为通过虚拟化技术，能够在一个物理服务器上生成多个虚拟机，并且能在这些虚拟机之间能实现全面的隔离，这样不仅能减低服务器的购置成本，而其还能同时降低服务器的运维成本，成熟的虚拟化技术有VMware的ESX和开源的Xen。

# 各子系统建设方案

## 政务信息资源共享交换平台

### 概述

国家电子政务总体框架由服务与应用系统、信息资源、基础设施、法律法规与标准化体系、管理体制等部分组成。政务信息资源目录体系与交换体系是国家电子政务总体框架中的重要组成部分，是电子政务的基础设施之一。政务信息资源目录与交换体系在支持电子政务应用时是一个有机整体，都是以政务信息资源为基础，依托国家统一的电子政务网络，采用不同的技术架构分别实现不同的服务功能，提供目录服务和信息交换服务，实现部门间信息共享和业务协同的支撑，作为基础设施与电子政务的业务应用相对独立。

### 建设内容

根据《[国家电子政务总体框架](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E7%94%B5%E5%AD%90%E6%94%BF%E5%8A%A1%E6%80%BB%E4%BD%93%E6%A1%86%E6%9E%B6/14593108)》及《政务信息资源目录体系》和《政务信息资源交换体系》等国家标准规范及规范涉及到的相关国家标准的要求，建设本地政府电子政务目录体系和交换体系相关的信息库系统和相关的服务支撑系统。为政务信息资源的统一梳理、编目、共享、交换、管理、应用、分析、和各部门的决策提供综合性的核心服务、支撑平台，即政务信息资源共享交换平台。

同时，在共享交换平台建设和运行的过程中，还需要建设相关的支撑和辅助平台，以确保政务信息资源的整合、共享和交换的高效实现和统一管理。还需要建设的相关支撑和辅助系统有：统一监控系统、统一运维系统等。

### 目录子系统

能方便地实现与资源目录对接，目录系统支持域管理，通过信息资源共享交换子系统的交换传输子系统与省资源目录系统对接。目录管理子系统通过系统配置管理实现基础信息配置、组织机构信息配置、权限角色管理等。业务流程管理提供工作流支撑，实现资源数据申请使用、审批的工作流支持。提供基于角色的权限管理，对目录资源的使用实现严格的权限管理。目录的服务统一通过目录访问接口实现。

#### 资源管理

**1、功能描述**

资源管理包括数据库资源管理、应用系统资源管理。主要包括如下功能：

* 提供结构化数据的数据库、表、字段等资源管理，如：数据库的新增、修改、删除，数据表的新增、修改、删除，数据表字段的新增、修改、删除；
* 数据表主键设置；
* 数据库、表、字段排序功能；
* 提供非结构化数据资源管理；
* 对应用系统资源进行登记、修改、删除及排序的管理，形成单位的应用系统共享资源信息库。

**2）运作流程**

**（1）资源生成：**

从各个部门业务信息资源中生成本部门用于共享的信息资源。资源分为：数据库资源和应用系统资源。

**（2）资源发布：**

提供以基于统一的电子政务网络为主的共享信息资源发布系统，发布共享信息资源。

**（3）资源访问：**

对资源进行权限控制以提供共享信息资源访问服务，用户可以浏览、查询、下载共享信息；并且基于统一的电子政务网络进行共享政务信息资源共享。

#### 目录编制

**1、功能描述**

目录编制是根据部门共享信息资源的内容，提取其基本特征，按照《电子政务信息资源目录体系国家标准》实现元数据赋值，形成目录内容。主要包括以下功能：

* + 提供资源目录的新增、修改、删除；
  + 提供对资源目录的明细信息指标项管理（根据本部门的数据库资源的数据字段进行提取），单个资源目录内容可对应一个或多个信息指标项；指标项支持脚本转换；
  + 支持单个资源目录内容可设置一个或多个信息指标为主键功能，还可以撤消或调整当前主键；
  + 提供资源目录指定一个或多个指标项作为查询指标；
  + 提供非结构化数据编目功能，包括文件、服务、图片、视频等；
  + 提供资源目录的注册上报；
  + 提供人工编目、机辅编目、自动编目等方式；
  + 编目系统支持中心系统集中编目，也可实现二级或多级汇总后传输到中心目录系统；
  + 提供目录形式审核功能，可实现漏填错填等问题的自动检测。
  + 提供视频资源的编目，建立视频资源库并统一管理（申请与授权），提供视频资源使用服务。

**2、运作流程**

**（1）编目类型控制：**部门编目人员根据需要对待编目资源进行编目方式的选择而对资源编目。

**（2）管理明细指标项控制：**提供对资源目录的明细信息指标项管理（根据本部门的数据库资源的数据字段进行提取），单个资源目录内容可对应一个或多个信息指标项；指标项支持脚本转换。

**（3）主键设置：**支持单个资源目录内容可设置一个或多个信息指标为主键功能，还可以撤消或调整当前主键。

**（4）目录审核：**提供目录形式审核功能，实现漏填错填等问题的自动检测。

**3、目录编制业务规则**

（1）编目对象是具体的共享政务信息资源，主要包括数据集、档案、法律法规、文件、报告、服务等，具体的形式可以是数据库、图片、文档、音频、视频、网页、服务等。具体粒度见附录。

（2）编目系统应支持自动、机辅方式完成元数据元素的赋值。

（3）提供唯一标识符管理功能。按照GB/T 21063.5—2007，支持唯一标识符的分配和赋值，包括支持后段码的自动生成管理。

#### 目录审核及发布

**1、功能描述**

目录审核及发布是指按照一定的规则对目录内容进行自动形式审核，按照标准进行发布，主要包括如下功能：

（1）根据目录内容提供目录审核功能，经审核后在资源目录中发布；

（2）提供图形化的审批流程定义和修改，并能监控流程环节状态；

（3）能够结合人工方式进行目录审核，包括审核数据和审核结果的导入导出。

**2、运作流程**

1. 部门资源编目:业务部门收集共享信息、发布到共享资源管理系统的资源库对其进行编目后向目录服务中心进行注册。
2. 目录内容审核：共享资源管理系统管理者按照GB/T 21063.3—2007、GB/T 21063.4—2007和GB/T 21063.5—2007对目录内容进行审核，未通过审核的目录内容，自动退回到相关部门，经形式修正后重新审核。

3） 目录自动发布：对于符合标准的目录内容自动进入目录内容服务信息库，按照标准要求自动发布以供用户访问。

#### 目录检测

1. 提供资源目录与库表结构在线比对，以列表形式展示，对差异化字段高亮显示。
2. 根据目录定义的提供数据不更新自动预警。
3. 提供待办待阅功能，用户登录目录系统，在待办待阅栏可看到待审核申请和阅知任务。

#### 目录变更

**1、功能描述**

目录变更提供对目录内容的维护管理，包括以下内容：

* 提供目录修改变更功能，经审核通过后在资源目录中变更；
* 提供目录变更的版本管理功能。

**2、运作流程**

* 目录变更需求：业务部门或管理者需要对目录进行变更，提出变更需求。
* 目录修改：管理者对于符合变更要求的目录按照相应规则进行修改,在修改的时候能够将要修改的内容与原内容进行对照。
* 目录审核：管理者对修改的目录内容进行自动新式审核，通过在发布，否则退回修改。
* 中心退回：对于不符合修改规定的变更需求，管理者退回给变更需求申请者，并说明原因。
* 发布：信息中心审核通过，发布后提供方才能看到变更后的目录内容。
* 同步：审核后的目录发布的同时进行目录同步。

#### 目录导出

**1、功能描述**

对已发布成功的目录，导出为文件的功能，支持导出全部资源目录和查询结果导出.

（1）根据资源目录导出SQL建表脚本;

（2）目录信息导出为文件，包含EXCEL等格式。

**3、流程描述**

1. 导出请求：使用者输入查询条件，向目录系统发出导出请求。
2. 获取导出信息：目录系统对导出条件进行解析。
3. 信息过滤：目录系统对导出请求结果过滤。
4. 封装并返回结果：对导出结果进行封装，并返回给使用者。
5. 获取下载内容：使用者得到所导出的信息结果。

#### 目录服务

目录服务是一种应用，其[存储](javascript:;)和组织关于网络用户和网络共享的信息。目录服务是基于目录内容服务信息库，向用户提供目录内容查询检索，目录导航和目录下载服务。

**目录查询**

用户基于浏览器等客户端查询目录服务中心目录内容的过程，通过目录查询可以定位共享信息，目录查询包括查询需求解析，目录内容服务信息查询，查询结果封装返回。

流程描述

（1）查询请求：使用者输入查询条件，向目录服务系统发出查询请求。

（2）获取查询请求：目录服务系统对查询条件进行解析。

（3）信息过滤：目录服务系统对查询请求结果过滤。

（4）查询结果封装返回：对查询的到结果进行封装，并返回给使用者。

（5）查询内容访问：使用者得到所查询信息结果，可对其内容进行访问。

用户只能查询权限范围内的资源信息。

#### 需求管理

需求管理是资源需求方向资源提供方提出共享需求申请，提供方对需求申请进行相应处理。

**1、需求申请**

通过需求申请，资源需求方向资源提供方提出共享需求。共享需求需引用的相关资源目录的数据指标，从而达到共享需求的功能需求。主要功能如下：

a) 提供资源使用申请审批功能进行需求申请和备案；

b) 提供直观的资源需求的分类、汇总和统计功能；

c) 提供需求满足度的统计分析和评估功能，并为电子监察系统提供相应的统计和评估数据。

**2、需求审核**

资源提供方对需求方提出的需求申请进行申请处理。

**流程描述:**

1）申请查看：

提供方查看申请到本部门的共享需求列表。

2）申请处理：

对需处理的申请，可做“已处理”或“不作处理”操作，“不作处理”表示提供方不认可该项申请。提供方只能对“未处理”的申请项进行操作。

3）处理情况通知：

资源提供方根据需求方提出的需求申请的实际情况，如需新编目则进行目录注册，如需对已注册发布的目录内容修改补充则进行目录变更，并在修改完成后通知需求方相应需求申请的处理情况。

#### 资源使用管理

**1、功能描述**

资源使用方建立本单位的某一系统对其他单位提供的共享资源目录信息及具体信息指标的使用需求申请，资源提供者、管理者对服务申请的审核和授权，同时根据服务申请和服务使用情况，提供直观的资源使用情况分类、汇总、统计和日志报表等功能。

**2、运作流程**

（1）服务申请：

资源使用方提出服务申请前，可先查看授权及可使用服务列表，如需要再提出服务申请，建立本单位的某一系统对其他单位提供的共享资源目录信息以及具体信息指标的使用需求的使用申请，包括增、改、删服务使用申请的管理。

（2）选服务提供部门：

提出服务申请时，选择本部门的应用系统后再选择服务提供部门。

（3）选资源目录及信息指标：

选择服务提供部门对应的资源目录和信息指标。

（4）备案：

进行服务申请时如果资源目录里面指标的共享类型都为强制共享类型时，则只进行备案及流转到管理者进行授权，不需提供方审核。

（5）部门审核：

当使用者申请使用的资源目录里面指标的共享类型包含条件共享类型时，申请将会流转到提供者进行审核，审核通过则流转到管理者进行服务授权。

（6）退回申请：

资源提供者对服务使用申请不予通过，做回退操作，状态变为“部门回退申请”。

（7）服务授权：

管理者查看使用者提出的服务申请列表，对申请使用的信息指标进行授权操作。如果使用者申请使用的资源目录里面指标的共享类型包含条件共享类型，则在管理者进行服务授权流程前需要经过资源提供者进行部门审核，部门审核通过才流转到管理者进行授权。

（8）定位使用：

使用者通过目录服务系统定位使用授权后的信息资源。

#### 目录部署

支持集中编目，支持目录系统的分级部署（支持目录分中心）。

**1、集中编目**

集中编目是经过系统授权的用户在市级或某一目录中心统一编目。

**2、分级编目**

分级编目支持市、区、街道办分级编目，在市、区、街道办分别建立目录中心，做目录管理时分别进行审核发布管理。

#### 目录元数据管理

用户可根据需求，在界面自定义编目等操作的元数据。

根据GB/T 21063.3—2007, 核心元数据中包含6个必选的元数据实体和元数据元素及6个可选的元数据实体和元数据元素，6个必选的元数据实体和元数据元素分别是：信息资源名称、信息资源摘要、资源资源提供方、信息资源分类、信息资源标识符、元数据标识符。

参照《政务信息资源目录编制指南（试行）》的代码结构规则，扩展信息资源代码，结构由前段码、后段码组成。前段码由“类”、“项”、“目”、“细目”组成，作为信息资源的分类码；后段码为信息资源的顺序码。

#### 目录版本功能

支持目录版本，目录初始版本为1.0，当目录发生变更后版本加1，在交换申请时只能申请最新版本目录。

目录版本变更后上一个版本提供的获取、比对服务继续能够继续访问，同时也可以申请使用新版本目录。

在资源管理中可以查看所有已发布目录版本，针对多个版本的目录，支持版本回退，可以回退到上一版本或取消发布该资源所有版本目录。

#### 工作流管理

用户可根据需求，自定义目录发布审核等操作的工作流。

支撑平台提供自主研发的工作流引擎，通过流程编排，统一调控各个业务流程，以确保工作在正确的时间被正确的人执行，达到优化整体业务过程的目的。BPM概念的贯彻执行，需要有标准化的流程定义语言来支撑，使用统一的语言遵循一致标准描述具体业务流程，这些流程定义描述由专有引擎去驱动执行。这个引擎就是工作流引擎，它作为BPM的核心发动机，为各个流程定义提供解析、执行、和编排，驱动流程“动”起来，让大家的工作“流”起来，为BPM的应用提供基本、核心的动力来源。

#### 角色权限管理

提供用户的角色权限设置和管理、控制。

角色是指具有某类相同行为的对象的集合，一个用户也可对应多个角色。一个角色可执行多项功能，一项功能也可由多个角色执行。角色按树进行维护，下级角色继承上级角色的操作权限。

系统中通过对角色的配置，再对角色进行权限，使该角色具有相应的功能。在系统管理中就可以对用户进行授予某一角色，使该用户具有该角色的相应功能和行为。用户登陆时，需要根据配置的角色功能和人员功能判断用户具有的功能菜单信息。对菜单内需要进行权限控制的组件进行管理，并与菜单页面进行关联，同时可以给角色授予权限。角色授权菜单页面之后，便可获取菜单与页面配置的菜单组件按钮权限。用户系统登录时系统会自动进行缓存权限，页面进行展示时会请求进行与缓存的权限组件判断，通过不同权限展示不同的菜单组件。

### 交换子系统

#### 概述

政务信息资源交换体系以国家统一电子政务网络为基础，通过构建覆盖中央、省、市县的多级政务信息资源交换体系技术总体架构，围绕跨部门的业务协同，以部门业务信息为基础，确定部门间交换信息指标及信息交换流程，实现不同部门间异构应用系统间松耦合的信息交换，形成部门间政务信息资源物理分散、逻辑集中的信息交换模式，提供部门间横向按需信息交换服务，提高各级政府行政管理效率和公共服务水平，满足各级政府履行职能的需要。

政务信息资源交换体系技术支撑环境由信息库系统和信息交换系统组成。信息库系统由若干交换信息库组成；信息交换系统由交换桥接、前置交换、交换传输、交换管理等子系统组成。

#### 系统组成

政务信息资源交换体系由信息库系统和信息交换系统组成。信息库系统由若干交换信息库组成；信息交换系统由交换桥接、前置交换、交换传输、交换管理等子系统组成。

通过交换桥接子系统将部门需要交换的信息交换到前置交换信息库，在交换管理子系统的流程控制下，通过交换传输子系统、前置交换子系统，把需要交换的信息定向传输到接收部门前置交换信息库。

#### 功能简介

##### 交换桥接子系统

###### 概述

交换桥接子系统实现部门业务信息库与前置信息库之间的信息交换。

交换桥接系统由桥接服务运行环境、桥接配置工具、桥接管理、应用适配器等部分组成。桥接服务运行环境是桥接服务的容器，桥接服务是利用桥接服务配置工具组装应用适配器组件以完成一个数据桥接流程的服务程序。桥接服务运行环境提供日志管理、安全管理、适配器管理等基本功能。桥接服务配置工具提供图形化的配置系统，通过配置业务信息库或共享信息库与交换信息库之间桥接内容映射规则生成桥接服务描述信息。

###### 系统功能

结构化数据桥接配置

结构化数据桥接主要包括实现各业务部门数据库桥接到前置共享信息库，同时也提供数据治理的功能，在共享信息库数据桥接到交换信息库的过程中，实现数据清洗、比对、查重、融合操作，将有效数据桥接到交换信息库，将问题数据桥接到问题库同时调用接口发送工单到工单系统，由工单系统实现问题工单的分派、追踪、整改与闭环操作。

关系型数据库之间数据桥接，在交换桥接管理系统配置数据桥接规则（如：数据源、目标资源、字段映射关系、数据同步周期等），发送数据桥接指定到桥接引擎，通过桥接引擎实现数据的搬运工作。

非结构化数据桥接配置

非结构化数据桥接支持ftp或sftp两种方式，在数据桥接管理系统配置文件桥接规则（如：源文件服务器、目标文件服务器、源文件目录表、文件同步周期等），发送文件桥接指定到桥接引擎，通过桥接引擎实现文件的搬运工作。

数据桥接执行引擎

数据桥接执行引擎主要实现结构化数据与非结构化数据实际执行者，通过接收桥接指定的方式执行结构化数据或者非结构化数据的搬运工作，主要采用restful的方式发布接口，供第三应用调用，桥接引擎提供的接口主要包括结构化数据桥接接口与非结构化数据桥接接口。

数据桥接管理

数据桥接管理包括各类数据库资源管理，数据源管理、作业管理、任务管理、任务调度管理、数据写入等说明。

1. 连接管理

归集连接是指向数据源的一个连接信息，其管理支持数据源的新增、修改、删除、连接测试等功能。

1. 任务管理

归集任务是指从各部门数据库采集数据并导入到目标数据库如：Oracle、MySQL、Postgresql、Hive、Hbase等数据库的过程。归集任务管理支持：

归集任务目录创建，分类管理归集任务。分类的方式从编目系统同步，即与编目系统保持相同的目录结构树，便于业务人员维护管理。任务管理子系统提供定时调用目录同步接口的能力，从而形成统一的目录呈现。

归集任务的创建分成：

1) 创建任务

2) 选择源数据库和表

3) 选择目的数据库和表

4) 设置清洗规则，支持以正则表达式的方式进行设置，同时也支持现成的简易规则，便于对数据进行初步处理。

5) 进行表字段映射，业务人员可以选择舍弃非关键字段，而保留业务关心的字段，减少数据冗余度，提高未来的数据

6) 输入抽取条件

7）保存任务

1. 作业管理

归集任务可以通过作业方式被调度，调度频率上支持T+0和T+1方式。

归集作业分类管理，支持按照编目系统的目录结构来呈现，在目录结构上形成统一的管理维度，便于业务人员维护管理作业。

1. 数据写入

数据写入通过Spark的扩展库sparkstreaming能力，调用大数据平台提供的分布式并行计算，完成海量数据高速处理。支持对文件、数据库记录等处理。

入库存储方式支持Oracle、MySQL、Postgresql、Hdfs、Hive、Spark、Hbase等。

数据桥接日志查询

桥接日志由数据桥接引擎产生，通过配置文件指定生成到指定数据库，数据桥接日志记录了执行任务状态信息、数据同步日志信息以及任务执行错误信息，可通过任务标示、任务名称、执行时间进行查询。

##### 前置交换子系统

###### 概述

前置交换环境由传输适配器、管理监控接口等部分组成，是交换服务的运行容器。安全加密服务提供基本的数据加密功能，保证信息传输过程中的安全。交换前置环境提供管理监控接口，交换管理监控子系统通过管理监控接口对交换前置环境进行管理。

前置交换子系统由交换前置服务器,交换信息库和交换适配器等组成.前置交换子系统与部门业务应用系统之间隔离,证保和部门业务信息库及业务应用系统的相互独立性。

###### 系统功能

前置交换环境由传输适配器、管理监控接口、安全加密、应用适配器等部分组成。前置交换子系统提供的主要功能如下：

1、支持不同交换信息库之间的双向信息交换。前置交换子系统能够从交换信息库中提取数据交给交换传输子系统传递，也能够从交换传输子系统中获取数据存储到指定的信息库或其他数据库中；

2、支持各种主流操作系统（Windows/Linux/Unix）；

3、支持国内外主流数据库(Oracle/MySql/DB2/SqlServer等)；

4、采用传输适配器接入到交换传输子系统；

5、支持将现有服务和应用接入到交换传输子系统；

6、支持用图形化向导的方式快捷生成服务；

7、支持与服务与目录版本的同步和对应，记录服务版本变化情况，能对服务的生命周期进行管理；

8、支持服务查询指标的优化，能为不同的查询条件订制化的服务；

9、传输适配器支持RFC2616；

10、采用应用适配器访问交换信息库，实现对交换信息库中数据的获取与存储；

11、提供图形化的服务定制工具，配置、测试、部署服务；

12、支持多个服务并发运行；

13、提供服务的监控功能，包括服务的使用者、调用时间、调用次数、响应时间、服务状态、运行时间、服务调用失败定位等，并能够对服务的使用情况进行查询统计；

14、能远程启动和停止前置节点上的服务；

15、支持配置文件异地备份与恢复，并提供统一的管理界面；

16、提供服务安全性策略集中定义功能，能对服务进行统一的访问授权、审计、身份管理；

17、支持服务远程部署功能，能将服务远程部署到一台或多台前置机上；

18、支持服务的负载均衡；

19、提供详细的错误日志，具备异常的快速定位功能

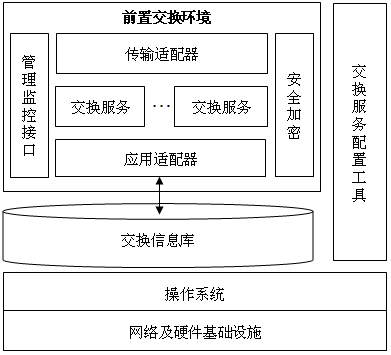
20、提供管理与监控接口，支持远程管理功能。

21、提供资源使用的数据接口。

22、提供安全的动态链路实现数据传输。

23、提供结构化、非结构化共享资源的安全存储和增量同步。

前置交换子系统的逻辑结构由网络通信系统、操作系统、交换信息库、前置交换环境、提供交换服务配置工具等组成。前置交换子系统的基本结构如下图所示。



图：前置交换子系统基本结构示意图

前置交换子系统是交换域的边界，实现交换域与部门业务系统的隔离。前置交换环境由传输适配器、管理监控接口、安全加密模块等部分组成，是交换服务的运行容器。安全加密服务提供基本的数据加密功能，保证信息传输过程中的安全。交换前置环境提供管理监控接口，交换管理监控子系统通过管理监控接口对交换前置环境进行监控。

前置交换子系统用来完成交换信息库与交换传输子系统间的双向信息交换。交换传输子系统能够从交换信息库中提取数据交给交换传输子系统传递，也能够从交换传输子系统中获取数据存储到交换信息库。

前置交换子系统和交换信息库之间的数据采集、发送通过应用适配器完成，该应用适配器的功能和结构与交换桥接子系统中的应用适配器一致，用来解决跨部门、跨系统的业务数据协同。前置交换子系统的数据传送分两个方向：

1. 交换信息库至交换传输系统

当应用适配器取得交换信息库中待传输的交换信息数据后，将该信息进行转换为传输XML数据格式，并对其进行加密、存储、完全验证，对传输的XML格式进行验证，然后查找接收方路由，并将XML数据投递给传输适配器，由传输适配器发送到交换传输系统中进行投递。

1. 交换传输系统至交换信息库

当前置交换系统的传输适配器从传输交换系统接收到交换信息后，查找信息接收方的路由，对传输信息的格式和接收方进行验证，对接收方的权限进行安全验证、存储转发、解密，然后将传输信息转换为交换信息，由应用适配器将交换信息存入交换信息库中。



双向信息传输功能

支持不同前置交换信息库之间的双向信息交换。在资源申请和审核、传输的整个过程中，部门A通过交换管理子系统向部门B申请相关共享信息资源审核通过后，交换传输子系统，在部门A的前置机A上，通过交换前置子系统A验证通过后，能够从前置交换信息库A中提取数据，将交换数据打包、分包、并加密处理后，然后传输子系统进行传输，部门B的前置机B，作为资源的申请使用部门，交换传输子系统在收到全部加密分包数据后，组包、解密处理，通过与前置交子系统B的交互和验证通过后，将数据在前置机B上，将申请获得的交换数据，入库到部门B的前置交换信息库B中，部门B申请、获得需要的共享、交换数据资源后，进行使用。

数据打包、分包及加密

前置交换子系统为资源请求方提供数据，对传输的数据包有加密功能，提高数据安全，在接受资源的前置子系统提供数据解密服务。

同时为了保证大数据量的传输，需要提供对数据分包，打包功能，实现数据的稳定传输。

前置数据交换

获取

前置机的数据获取流程包括二个接口，响应业务系统请求的接口，响应交换传输的接口。

**功能点**

1．检测资源请求是否合法

2．对业务系统请求的负责对象进行解析

3．封装资源请求的消息体Envelope对象

4．资源请求对象Envelope消息体的序列化

5．解析返回的数据包

6．判断返回的资源的类型：结构化数据，包含非结构化数据

7．结构化数据对象BusinessData的抽取

8. 非结构化数据下载

2）提供数据接口：IReceive

**接口描述：**

主要负责响应交换传输请求，在接收到数据请求时，分析Envelope对象，判断请求的数据源，包括数据库类型，服务型，文件型的数据源。在指定的数据源中提取数据，数据过滤。封装数据对象，封装Envelope对象，返回资源。

订阅

在资源编目后提交审核通过后，目录中心将会构建建表指令，由交换传输系统将指令传递到资源提供方前置，资源提供方前置接收到指令后在交换信息库中建表；

政务部门如果需要订阅其它部门所发布的资源，需登录到目录中心，通过检索订阅资源后，作资源订阅申请，申请信息中包括该部门的哪个应用系统要订阅哪个资源哪些指标项，当发布该资源的政务部门登录到目录中心后，可对这些订阅申请作授权操作，授予这些应用系统订阅本部门发布资源的权限。

订阅审核通过以后，首先将在资源的订阅方前置交换信息库中建立接收订阅数据表，目录中心构造建表指令，由交换传输系统将指令传递到订阅方前置，订阅方前置接收到指令后在交换信息库中建表；其次目录中心需将订阅相关信息同步到交换管理系统，订阅信息包括订阅方的部门信息、应用系统标识、订阅的资源标识、订阅周期等，交换管理系统根据同步过来的订阅信息，在订阅条件满足时触发订阅，执行订阅流程。

Destination存放的指令的目标地址；

CommandId标明了指令的类型；

Parameters存放的是具体的建表指令；

指令中存放只有一条或多条SQL语句；

前置指令接收接口接收到该指令后，解析并执行该指令。并将执行结果返回给调用方。

比对

数据比对流程包括二个接口，数据比对发起方访问前置机的接口和权威数据提供方接口数据比对的接口

1. **前置机接收到业务系统数据比对接口**

描述：数据比对发起方前置机接收到请求，分析请求对象合法性，如果对象符合要求对对象分析拆装，重新组装成Envelope对象，请求交换传输。

接收到交换传输返回的Envelope对象后分析对象。提取数据集返回给业务系统。

订阅消息握手

一个订阅发送任务涉及到的各个子项目的执行完全分散，相互之间的关联关系是单向关联，所以整个任务执行流程是一个单向的不可逆的。为了解决这一问题，现在订阅发送引入握手机制，在订阅方与提供方之间加一个握手机制，但要考虑到加入的握手机制本身不能太过影响现有的任务执行效率，所以只进行2次握手，一次在订阅方接收到订阅任务并入库成功，第二次在订阅数据成功或失败后进行第二次握手（前提是订阅发送任务也要和订阅接收任务一样，是会长久的保存，但现在有的机制是只要发送任务发送成功，如果这个订阅重新触发）。

消息补发策略

前置子系统提供消息确认和消息选择性重发机制,实现前置系统间可靠的信息传递功能，通过配置消息传输策略，可是使传输成功或失败后按照既定的策略进行处理，如果配置了传输消息确认，则传输成功后会向消息的原始发送方返回一个传输成功的消息确认，如果消息传输由于某种原因永久失败(即已经超过最大重发次数)，则向消息的原始发送方返回一个传输失败的消息确认。根据消息传输策略，传输子系统可以在消息传输过程中对消息的传输方式进行控制，如设置消息的重发次数、重发时间间隔、重发超时时间、错误码响应流程等，对传输进行灵活的配置。

数据订阅的快速传输

针对结构化数据的传输，采用消息队列对象传输的方式，减少数据序列化和落地磁盘的次数，加快数据传输速度。

订阅容错处理

共享交换平台作为地区数据共享交换统一的出入口，承载着大量应用的请求，随着业务流量的规模增长，系统要有较强的容错能力和扩展能力，系统应具备一定的容错和自动恢复能力，较强的容错能力是系统稳定性的重要保障。

**重试机制**

重试机制是最容易也最简单的容错方式，实现简单。通过重试机制，可以有效地解决网络不稳定之类的因素造成的偶发异常。

**设置超时时间**

超时时间设置过短，会将很多本来处理成功的请求，当做服务超时处理掉，进而引起服务成功率下降。将全部业务服务，以一刀切的方式设置一个超时时间，是比较不可取的。优化的方法，我们分为两个方向。

**为服务和存储设置合理的超时时间**

根据实际的业务维度，区分对待地给各个业务服务配置不同的超时时间，同时，最好也将它们的部署服务也分离出来。

**快慢分离**

根据实际的业务维度，区分对待地给各个业务服务配置不同的超时时间，同时，最好也将它们的部署服务也分离出来。

**解决同步阻塞等待**

“快慢分离”可以改善系统的同步等待问题，但是对于某些耗时本来就比较长的服务而言，系统的进程/线程资源仍然在同步等待过程中，无法响应其他新的请求，只能阻塞等待，它的资源仍然是被占据，通过异步处理,当进程遇到I/O网络阻塞时，就保留现场，立刻切换去处理下一个业务请求，进程不会因为某个网络等待而停止处理业务，进而系统吞吐率即使遇到网络等待时间过长的场景，通常都能保持在比较高的水平。

**消息的时序与一致性设计**

共享交换平台中，由很多业务场景都需要考虑消息投递的时序，例如：

1. 订阅触发，保证前置接收的任务顺序与平台一致；
2. 点对点，保证发送方发送顺序与接收方任务顺序一致，保证每个任务中数据包任务一致；
3. 一对多，保证所有接收方展现顺序一致，保证每个任务中数据包任务一致。

##### 交换传输子系统

###### 概述

交换传输子系统根据交换体系部署的交换流程,实现部门前置交换信息库之间处理和稳定可靠的信息传递。交换传输子系统作为前置交换子系统之间的信息交换通道，实现交换信息的打包、转换、加密、传递、路由、解包等功能。

###### 系统功能

交换传输子系统作为前置交换子系统的信息交换通道，实现交换信息的打包、转换、传递、路由、解包等功能。

交换传输子系统提供的主要功能如下：

* 消息传送应支持RFC2616；
* 采用W3C的SOAP作为消息封装格式；
* 采用W3C的WSDL作为交换服务描述规范；
* 提供消息寻址功能，支持信息路由功能。
* 支持多种传输协议，包括Http、Soap、MQ、JMS，可灵活选择其中的一种或多种协议进行通信；
* 支持点对点、一点对多点和多点对多点的传输模式；
* 提供消息确认和消息选择性重发机制以实现前置交换子系统之间安全的、可靠的信息传递功能；
* 支持断点续传；
* 提供对数据进行加解密、压缩及解压缩等功能；
* 提供消息差错处理功能；
* 提供信息转换功能，支持基于规则配置的格式转换与内容转换功能；
* 提供大于2G以上文件传输功能，并支持分包机制进行传输。

交换传输子系统是用来构建前置交换子系统之间安全、可靠、稳定、高效的信息交换通道，实现信息的打包、转换、传递、路由、解包等功能。以下是交换传输子系统的架构图。

交换传输子系统由核心交换服务器和接口服务器组成，核心交换服务器处理信息资源中转交换；接口服务器由一系列的服务器组成，它完成交换前置子系统与核心交换服务器的通讯，所以称之为接口服务器，由于鄂尔多斯市党政机关在数量上可能存在上百个政务信息资源网络与接口服务器相连，所以提供接口服务器群来响应来自不同政务信息资源网络的连接，每个接口服务器上运行环境以及服务完全是一样。根据性能的要求，可以增加接口服务器的数量来达到负载均衡。一个接口服务器服务与1至N个资源网络，后台提供接口服务器与资源网络的匹配设置，匹配设置后，对于一个资源网络都有一个接口服务器来进行接收、发送响应；



编目、订阅建表

将路由服务,鉴权服务全部串联后形成一个通用的同步获取服务,调用通用的同步获取服务后,先调路由服务填充路由地址,然后 判断是否在本中心，若不是则请求到下一个中心，若是则判断建表类型，订阅在订阅提供方记录订阅交换记录，并调用申请方前置建表。

获取、比对

将路由服务,鉴权服务全部串联后形成一个通用的同步获取服务,调用通用的同步获取服务后,先调路由服务填充路由地址,然后 判断是否在本中心，若不是则请求到下一个中心，若是则走鉴权服务，鉴权通过后将请求发送到动态路由服务,动态路由服务将解开目标地址,然后调用相关的提供方前置服务，提供方前置上的对服务类型判断，如果是比对服务,则用前置库上的数据进行比对，如果是获取数据,最后前置将数据封装成标准的交换XML,最后返回给请求方。

业务规则

交换传输子系统作为前置交换子系统的信息交换通道，实现交换信息的打包、转换、传递、路由、解包等功能。

消息路由寻址功能

在交换传输子系统中，提供消息寻址和定位功能，是在整个传输子系统中的基础功能，其它所有功能应该是基于消息寻址的机制之上，交换传输子系统可以支持基于消息头以及基于内容的信息路由功能。

消息传送策略配置

交换传输子系统提供消息确认和消息选择性重发机制以实现前置交换子系统之间可靠的信息传递功能，通过配置交换传输子系统的消息传输策略，可是使传输成功或失败后按照既定的策略进行处理，如果配置了传输消息确认，则传输成功后会向消息的原始发送方返回一个传输成功的消息确认，如果消息传输由于某种原因永久失败(即已经超过最大重发次数)，则向消息的原始发送方返回一个传输失败的消息确认。根据消息传输策略，交换传输子系统可以在消息传输过程中对消息的传输方式进行控制，如设置消息的重发次数、重发时间间隔、重发超时时间、错误码响应流程等，对交换传输策略上进行灵活的配置。

消息转换功能

在传输子系统应支持基于对信息体的元数据映射或规则的数据转换的配置，并能作数据转换。

大文件及大数据量的传输

交换传输子系统提供结构化数据传输和非结构化数据传输。

根据数据的使用和提供方式不同，我们根据交换业务规则把数据分为同步数据和异步数据。同步数据交换指，当数据的消费方提出请求后数据的接收方必须立即，或者在没有人工参与的情况下返回数据。异步数据是指当数据的消费方提出数据请求后，接收方不必立即返回，或者需要人工干预下才能返回数据。

交换传输子系统应支持大数据量的高效传输，同时又应考虑到核心负载压力和业务保密需求，交换传输子系统对大数据量的高效的传输应支持点对点的数据传输服务，即前置服务器与前置服务器之间能过交换传输通道直接传输数据。在传输之前，提供方先分配会话ID，服务请求方凭借提供方的会话ID来作身份确认，并通过交换传输子系统来传输大数据，从而保证大数据量的快速安全的传输。

交换传输子系统可以支持大文件的传输（2G以上的文件传输），支持对大文件的分包/组包转输机制,同时也支持消息传递的可持续化，支持大文件的断点续传，支持消息中间件的数据传输机制。交换传输子系统应该提供数据的分解组合的可靠性及安全性，使得前置交换子系统在接收端能安全可靠的将数据组合成最终文件成为可能。

点对点传输模式

交换传输子系统支持两个前置子系统之间点对点的通信，交换传输子系统可以为前置交换子系统请求作消息路由，并为两个交换前置子系统直接建立起安全，可靠的连接，使得两个前置交换子系统之间能作快速，安全可靠的数据交换。

批量数据交换

由于不同业务要求的时效不同、传输数据量不同，在交换的方式中，分成异步消息交换以及同步消息交换。异步消息交换完成大数据量、时效要求低的交换，例如业务信息批量交换、公关信息批量更新等。同步消息交换完成时效要求高、传输数据量小的数据交换，例如查询业务信息、配置交换系统参数等。

访问安全

1. 保证平台能够确定访问来源。
2. 保证平台能够确定被传送的数据没有被篡改。

订阅握手策略

现在交换传输没有握手机制，整个任务执行流程是一个单向的不可逆的，所以可在使用方与提供方之间加一个握手机制，但要考虑到加入的握手机制本身不能太过影响现有的任务执行效率，所以只进行2次握手，一次在订阅方接收到订阅任务并入库成功，第二次在订阅数据成功或失败后进行第二次握手（前提是订阅发送任务也要和订阅接收任务一样，是会长久的保存，但现在有的机制是只要发送任务发送成功，如果这个订阅重新触发）。

##### 交换管理子系统

###### 概述

交换管理子系统实现对整个信息交换过程的流程配置\部署\执行和整个信息交换系统运行进行监控\管理。

交换管理子系统支持对整个交换过程的综合管理监控，包括交换流程的配置、部署与管理以及对交换系统运行情况的监控与管理两个方面。

###### 系统功能



节点管理

节点管理只有管理员拥有权限，每新增一个单位接入时，需要在此进行节点配置，包括分配节点编号，这个节点编号需要与前置子系统的配置节点编号一样，管理员可对节点进行增删改查。

订阅管理

每条订阅申请都显示订阅的订阅标题、请求的资源名称、申请单位和资源提供单位、订阅状态。点击每条记录，下方“编辑信息”中显示该记录的详细信息。其中“订阅开始时间”和“订阅结束时间”表示的是申请单位在目录平台提交申请时填写的订阅开始时间和结束时间，订阅会在开始时间和结束时间内执行，在结束时间以后就会自动结束；“订阅间隔时间”表示交换平台在每个时间间隔向提供方前置发送一次指标，“最后执行时间”表示交换平台最后一次向提供方前置发送指令的时间。

订阅状态有两种：可订阅、不可订阅。“可订阅”表示当前的订阅申请为有效，如果提供方的资源表数据有所改动，则会正常送到请求方。“不可订阅”表示当前的订阅申请为无效，申请方已没有权限订阅提供方的数据，无论提供方的资源表数据作何改动，都不会送到申请方。

订阅状态由“可订阅”变为“不可订阅”有四种情况：

当前时间已经过了结束时间；

提供方表不存在；

人为把订阅状态由“可订阅”改为“不可订阅”；

提供方和申请方不在同一个目录中心，一般不允许跨目录中心访问数据库；所以申请方交换平台看到的订阅状态即为“不可订阅”，但提供方仍可看到“可订阅”。

交换中心路由管理

对整个交换平台而言，所有的中心节点间在交换传输的路由关系是以树的形式体现出来，它们都有且仅有一个共同的根节点，当某次数据交换需要跨中心交换时，这时，交换路由是根据这棵树中所定义的中心节点之间关系来生成的。

实时监控图

实时监控平台数据的交换量，可快捷进行按天、周、月、进行统计查阅，也可以按任意时间段进行数据统计查阅，对提供方数据和申请方数据，都可进行分类查询统计。

节点状态监控图

监控节点状态可分为四种情况：

1. 正常：物理机和应用网络均处于正常状态。
2. 预警：物理机正常运行，应用网络中断。
3. 中断：物理机与应用网络均中断。
4. 停止监控：已停止节点状态监控。

数据排名（前十）：

对资源提供、资源共享、资源使用进行排名统计。

### 质量工单管理系统

#### 概述

质量工单管理系统为共享交换交换平台进行数据共享交换提供数据质量保障，对共享过程中出现问题的数据，及时形成资源提供方待解决工单并自动发送给资源提供方，质量工单管理系统可及时通知资源提供单位进行修改、重新提交审核，并最终提交资源。从而保证共享数据的正确性和可靠性。质量工单管理系统，为数据质量管理系统形成事务工单，方便各部门之间进行事务协作、问题处理和交互。

#### 功能简介

##### 数据提供

###### 工单管理

本单位工单处理数量走势统计分析

按月对各单位数据资源的提供工单、问题工单的处理数量，进行统计展示，用于对数据资源的使用总体需求和各单位对资源共享的贡献情况，进行统计和度量。

待处理工单

数据提供用户进入待处理工单菜单，用户查询本单位待处理工单数据，待处理工单状态有：已分派，同意挂起、上级决策再处理、上级决策决绝驳回、上级决策同意挂起、上级决策拒绝挂起，查询条件有工单编号，工单标题，共享目录表名，工单发起单位，工单处理单位，问题来源，工单状态，解决时限，发起时间。在查询结果中，选择一条工单记录，在工单处理界面，用户可以查看当前工单详情和关联的问题单详情，并填写处理结果和处理意见后完成工单处理操作，已处理的工单不能重复处理。

已处理工单

待处理工单经过处理后，处理流程变更为已处理，数据提供方用户可在已处理工单菜单查询已处理的工单，已处理工单状态有：已处理、申请驳回、申请挂起、已完成、确认不通过、同意驳回、决绝驳回、上级决策同意驳回、上级决策、已完成。对查询结果进行工单详情信息查看，查询条件有工单编号，工单标题，共享目录表名，工单发起单位，工单处理单位，问题来源，工单状态，解决时限，发起时间。

已办结工单

数据共享提供方将工单处理之后，工单流程转为由数据使用方对处理后的工单进行再确认处理，之后，工单转为以办结状态。已办结工单状态有：已完成、同意驳回、上级决策同意驳回、上级决策已完成。数据提供方用户可对已办结工单进行查询，查询条件有工单编号，工单标题，共享目录表名，工单发起单位，工单处理单位，问题来源，工单状态，解决时限，发起时间。

首页

首页功能主要展示当前用户所属单所有待处理工单处于不同处理状态的工单处理情况。提示用户对单位需处理工单进行处理。

##### 数据使用

###### 问题单管理

暂存问题单

对数据资源共享过程中，对于提供方提供的数据资源，如果存在质量问题的，产生暂存问题单，在此暂存问题单管理中，每个单位可以查阅本单位提供的数据资源，在质量上存在问题的工单，使用方可在此进行查看，并将期望提供方进行修正的数据，在此人为干预，转工单给提供方，进而进行针对性的处理和再次提交审核。对于不需要转工单，使用方可人工确认的问题单，在此可进行人工干预，直接将问题单状态关闭为办结。

已转工单的问题单

对使用方已转工单的数据质量问题单，在此进行统一的查阅、统计。

已办结工单的问题单

对于存在问题的数据问题单，如使用方可直接确认，标记为已办结的问题单，可在此进行详情查阅和统计参考。

###### 工单管理

首页功能

对共享数据资源的使用方，对于已形成系统内的所有相关工单，在首页中根据工单的处理状态，进行了分类统计展示，从而对使用方本单位和相关单位对整个数据共享资源的贡献，进行量化统计和考察、考核。工单和问题单的处理状态如：已缓存、已分派、已处理、申请驳回、申请挂起、已完成、确认不通过、同意驳回、拒绝驳回、同意挂起等。

发起工单

对于使用方而言，发起工单功能，主要对使用方问题单转工单后的处理情况在此进行查询。同时，作为使用方，对共享数据资源在使用中存在的问题，如果不属于系统自动生成问题单的情况，使用方在此还可以人工添加发起一个工单给某个提供方，在工单中可以对具体存在的问题，进行具体的规范化描述，从而方便提供方查验问题，并最终反馈一个预期期望的处理结果，给使用方。

待处理工单

对使用方而言，提交给提供方处理的工单，如数据方已进行了处理，工单状态发生了变更，则使用方在流程上需要对工单进行进一步确认处理操作和工单状态的进一步更新，确保工单处理的流程完备性和规范性。

已处理工单

对于使用方已处理的工单，在此进行统一状态查阅，统计和管理。对于已处理的工单，在此可标记更新工单状态为已办结或其它暂结状态。

已办结工单

对于使用方已办结的工单，在此进行统一查询和详细查阅及统计。

本单位工单状态统计

使用方单位工单各种状态的量化统计，有助于本单位作为使用方，对相关工作的处理，进行综合分析和决策。

##### 数据管理

在整个数据资源的共享交换系统中，某个具体的单位，同时行使两个职能角色，为了更好的推动和促进数据资源共享交换系统的建设、发展、完善和使用，同时通过设定指标及对所有单位对系统的综合贡献情况进行量化、可视化的实时和科学的统计分析，使工作落后的单位，能够在工作的及时性和正确性等方面，努力与先进工作单位看齐，努力高质量完成本单位的所有工作项，完成相关指标考核，从而推动资源共享交换系统的健康、良性、快速的建设和发展。相关综合统计分析的功能模块展示如下：

###### 本单位工单处理率

PC可视化统计展示了本单位工单处理率，并对工单按待处理、已处理的状态和工单总数统计展示出具体的数量和占总百分比。

###### 所有单位工单处理率

PC可视化统计展示了所有单位工单处理率对比情况，对每个单位，分别按资源的使用方和提供方2个不同的角色，进行统计。

###### 所有单位工单状态统计

PC可视化统计展示了所有单位工单处理状态对比情况，状态如：已暂存、已分派、已处理等。

### 数据对账子系统

#### 概述

数据对账子系统，用来保证资源提供方和使用方两方数据交换的一致性，同时建立有效的数据交换异常处理机制，针对数据交换过程中可能出现的异常进行定时监控，对账，产生详细日志，并提供快速排查问题的功能（如握手异常查询，异常信息查询功能等），供系统管理和运维人员分析故障和原因。

对账系统主要功能包括：资源数据监控、数据同步监控、应用系统配置等。

#### 功能简介

##### 结构化资源对账

统计共享交换平台中结构化数据的提供和使用情况数据并进行对账，让操作员在平台上可以直观的看到资源目录每日交换数据量变化情况和订阅运行情况和对账情况。

###### 资源提供情况

用户可通过该页面可查看本单位发布的每个资源上传的数据量，和每日数据变化量情况；

可以比对实际表结构是否与平台记录的表结构一致，如不一致记录有什么不同；

可查看每个资源被哪些单位订阅了和订阅异常与否的具体情况；

可对上述三种情况进行即时的统计；

提供同步数据功能，对使用方和提供方交换数据不一致的数据，用提供方对应数据，同步使用方对应数据；

提供分页浏览功能；

提供资源提供情况查询、查阅并导出为Excel报表功能。

###### 资源使用情况

用户可通过该功能查看本单位订阅其它单位结构化资源的数据订阅情况，检查是否订阅正常，还可查看每日的订阅情况；

支持自动排障分析功能，及时发现并处理数据交换过程中的异常情况；

支持按所选资源即时统计，表结构比对监控，比较数据库中表结构与在交换平台中登记的结构是否相同；

提供握手信息快捷查询功能、订阅发送任务快捷查询功能、订阅接收任务快捷查询功能、修改字段长度快捷查询功能、详细信息查阅功能；

支持资源使用情况导出为Excel 报表功能。

###### 订阅排障情况

将前置节点和数据库异常的订阅纳入排障管理，如该异常不能马上解决的，人工标记为排障中，排障中的订阅任务将暂停数据统计，订阅会暂时关闭，以减少系统资源消耗，当节点异常情况解决后,订阅标记修改为正常后恢复订阅功能，同时恢复订阅任务。支持资源下载排障情况的查询统计功能；查看排障具体情况等功能。

##### 非结构化资源对账

统计共享交换平台中非结构化数据的提供和使用情况，让操作员在平台上可以直观的看到非结构化数据资源目录每日交换数据量变化情况和订阅运行情况。

###### 提供方非结构化

支持查询并展示非结构化资源文件个数、订阅单位数量、状态等基础信息；

支持按所选资源即时统计，支持同步数据、分页浏览功能；

支持资源提供情况导出为Excel报表功能。

###### 非结构化订阅

用户可通过该页面查看本单位订阅其它单位非结构化资源的数据订阅情况，查看是否订阅正常，可快捷查询每日的订阅情况；

支持使用方非结构化资源订阅情况查询、统计功能；

支持按所选资源的即时统计对账功能；

支持资源下载排障情况的查询统计功能；

支持排障情况查阅功能；

支持所选数据即时比对功能；

支持订阅发送任务功能；

支持订阅接收任务功能；

支持非结构化资源订阅情况导出为Excel详情报表功能。

###### 非结构化订阅排障

对发现订阅异常不能马上解决的信息，可标记为排障中，暂停订阅，从而节省系统资源，标记为排障中的订阅会暂时关闭同步和统计功能，异常解决后把订阅标记为正常恢复订阅和统计。

提供非结构化资源订阅排障情况查询统计功能；

提供即时排障等功能。

##### 对账管理

###### 应用配置

把资源按应用场景或应用系统进行关联，在查看资源提供和使用情况时，可以分类的应用场景和系统进行检索，可以更加高效的对这些订阅进行监控。

提供了接入对账系统的各政务部门应用系统的登记功能及登记信息的维护功能。

###### 异常信息

提供了对账系统在定时或即时运行数据对账过程中，出现异常情况的查询、浏览功能，以备运维人员能够及时参考并对系统本身或各节点的故障，进行及时的修复和故障排除。

###### 握手异常

提供了对账系统在进行定时或即时运行数据对账过程中，出现节点间握手异常情况的查询、浏览功能，以备运维人员能够及时参考，并处理情恢复相关节点间通信的故障。

###### 统一查询

提供了按所有对账系统相关数据库（如：前置数据库、存储库、平台数据库等）进行综合执行查询命令的功能。

###### 系统配置

* 服务端基础运行数据配置

提供了基础运行数据配置信息的增加、修改和删除、查阅功能；

配置重点信息为所属单位、配置项、配置内容、配置解析说明等信息。

* 前置端基础运行数据配置

提供了按单位进行信息重置和按所有单位进行信息重置的功能；

配置项如：IP地址及端口、MQ地址、最大统计线程数等诸多项的配置。

### 统一审计日志系统

#### 概述

统一审计日志系统将各支撑应用系统产生的日志通过多种方式收集并存储，最终实现日志的分类、查询、统计、分析的功能。

统一审计日志系统采集的日志记录不能被修改。以保证审计日志的真实性和完整性。

#### 功能简介

##### 应用系统日志接入管理

基于日志数据存储平台的日志接入管理，管理日志的用户、日志接入申请、日志分类、日志目录、日志权限管理、日志展示、监控告警、日志搜索等功能。

##### 日志目录编辑以及接入申请

普通用户通过日志接入申请，需填写日志所属单位、系统名称、应用系统IP或域名、该系统是否关联上级系统或平级系统、关联系统名称、日志类型，并且进行日志目录编辑，提交并且管理员用户进行审核。

##### 日志分类

接入日志可分为：应用系统运行日志（log4j等）、应用系统内部审计日志、应用系统性能日志。

##### 日志权限管理

管理员用户可以对日志权限进行分配管理，日志权限分为接入权限、查看权限、下载权限等权限进行管理。

用户分为管理员用户（admin）、普通用户（user）:

管理员用户是账户的创建人以及所有人，具有账户的最高管理权限，其中包括添加其他用户和更改其他用户权限的权利。

普通用户进行日志的接入申请、日志的目录编辑、日志展示查看、进行日志搜索。

##### 监控告警

管理员预先设置告警的日志类型，告警关键字，告警内容，告警负责人，当预先设置的告警条件满足时，系统自动产生告警通知事件，同时通过告警的输出模块（短信、邮件等）将信息通知相关人员。

##### 日志检索

检索条件多样性：

可根据日志类型、日志产生时间、日志源等进行复合条件查询：

对更精细查询可以用组合条件查询完成；

对查询显示的日志字段可以根据管理员查询的侧重角度进行选择性配置。

##### 日志展示

* 表格视图

使用表格视图将搜索字段简化展示，只显示用户选择所关注的关键字段。表格视图通过应用管理中对应的字段选择配置，被选中显示的字段将在表格面板中展示。日志时间为默认显示字段。

* 审计日志统计视图

每次统计，系统都会生成可视化的操作日志的时间序列趋势图，同时生成搜索时间范围内所有日志事件接入的直方图，所有操作日志类别统计的饼状图。

##### 审计日志传感器功能

审计日志传感器负责采集业务系统中的独立日志，将分散的日志信息通过指定的消息队列传输到对应的日志服务器，最终处理并存储在大数据平台信息库中。

###### 审计日志采集

所有相关支撑平台每天都会产生大量的日志数据，日志采集系统客户端将收集相关的日志数据，供离线或在线的分析系统使用。高可用性和可扩展性是日志采集系统必须具备的特征。日志采集系统客户端部署在每台服务器上，负责对每台服务器的日志收集，然后将日志传输到消息队列中暂存，再由日志采集系统服务端将日志数据入库到大数据平台对应的信息库中。为了保证审计日志系统的高可用及高性能，建立MQ集群并提供负载均衡。日志采集系统客户端到MQ使用负载均衡策略，使用VIP(虚拟IP)技术，基于Keepalived实现主、备负载均衡，避免单点故障。

###### 审计日志传输

日志客户端采集到数据后，需采用TCP协议，建立安全的传输方式。把日志信息传输到审计日志系统。

采用分布式存储计算基础软件中的kafka作为消息队列进行审计日志传输工作。Kafka 是一个高吞吐量的分布式发布订阅日志服务，具有高可用、高性能、分布式、高扩展、持久性等特性。

###### 审计日志数据存储

通过日志数据存储平台整合各基础平台日志信息，使日志数据存储平台和各基础平台日志实现无缝结合，达到数据资源整合，实现统一管理的目的。日志数据存储平台为各基础平台日志提供海量数据的实时检索和信息推送功能。

实现目标：

1、日志数据存储平台根据各基础平台的实际业务类型进行划分，真正从业务的角度考虑日志数据存储平台如何高效并且友好的为各平台提供数据信息支撑。

2、根据不同业务场景对数据进行针对性分析，并提供相应的可视化结论，以更为友好的方式展示相应的数据信息，减少人工干预。

3、日志数据存储平台针对各基础平台日志进行分析，为各基础平台提供不同状态和条件下的日志进行收集，并提供相应的消息推送功能，达到日志数据存储平台和各基础平台有效且高效的协同处理任务。

###### 审计日志行为跟踪

提供相关日志统计分析功能，能知晓业务平台的运行状况、性能指标等。如提供指定事件或错误的出现频率与趋势、服务执行时间等统计分析。

###### 系统运行日志分级

* 日志记录器的管理

系统通过保持多个日志记录器(Logger)对象的方式来进行日志记录的分类。每一个Logger对象代表一类日志分类。

* 日志分级

按照日志目的不同，将日志的级别由低到高分成五个级别，分别为：

* Debug：表示输出的日志为一个调试信息
* Info：表示输出的日志是一个系统提示
* WARN：表示输出的日志是一个警告信息
* ERROR：表示输出的日志是一个系统错误
* FATAL：表示输出的日志是一个导致系统崩溃严重错误

记录信息的同时会对日志信息赋予基本属性，这样为后续的按照级别不同进行输出工作奠定了基础。

* 日志信息的获取

日志对象上包含了一条日志所具备的所有信息。通常这些信息包括：输出日志的时间、Java类、类成员方法、所在行号、日志体、日志级别等等，获取日志信息时可以对日志信息进行格式化操作。

* 日志文件输出

文件输出器内部定义了一个线程安全的高速缓冲，所有通过日志记录部分分派到文件输出器的日志被直接放置到该高速缓冲当中。同时在文件输出器内部定义一个工作线程，负责定期将高速缓冲中的内容保存到文件，在保存的过程中同时可以进行日志文件的备份等工作。

* 日志数据库输出

数据库输出需要现在数据库创建好相应的日志表，然后将系统日志输出到数据库中保存，使用数据库保存的最大好处是便于对日志进行统计分析。

* 日志控制台输出

直接将日志输出到控制台，主要在现场调试时使用。

#### 审计日志规范

在智慧城市政务系统应用中，审计的作用日益突出，在以“一数一源，谁的数据谁负责;根据职责和履职需要使用共享资源”为主题的今天，完善和推行审计日记制度尤为必要。

不同时期实施的各个系统都有独立的日志系统，这么多零散的审计日志，使得信息分散，需要登录不通的系统才能查看到对应的审计日志，将会给审计工作带来不便，降低办事效率。

统一审计日志系统的建设中保证数据的需要客观性、相关性、充分性和合法性。

##### 日志归一化

将形式各异的日志统一成专有日志格式，归一化后利于审计数据的收集和程序处理。

日志数据多种多样，每种日志都有它独特的作用，要保证将每种日志都归一化太难，这就需要我们的规范体系技能保证格式的统一，有能允许有自定义类型的日志出现。

##### 归一化日志规范

将整个审计日志定义为xml格式，第一次为日志id、日志类型、基础日志和详细日志。

基础日志包括日志记录的时间、发生的时间、事件类型、服务器ip地址、服务器主机名、应用容器类型和访问的客户端Ip地址。

详细日志记录日志的详细信息(主要是错误堆栈信息)、如果是应用报错则提供线程名称、源程序路径、访问信息和数据库信息。

记录的访问信息主要针对系统间交互、人机交互时产生的信息。包括访问的主机端口、访问的路径、访问时的协议、访问的方法、访问的域名、服务端的过滤动作及服务端返回的http状态码。

数据库信息主要是针对服务端执行数据库操作时的审计记录，它是运行时的日志记录，并不只是在错误发生时记录。主要包括：操作的数据库URL、数据库用户名、执行的sql、以及执行的操作结果。

##### 个性化日志规范

为接纳不同的业务系统审计日志，统一日志审计平台提供以下格式的自定义日志记录方式，日志上报的方式需保证与统一审计日志系统上注册的日志格式一致。

## 综合集成门户建设

### 建设目标

综合门户是信息一体化平台所有业务系统的统一入口及信息集中展示平台，是政务办公人员之间的沟通纽带，是内部办公、管理、辅助决策、宣传教育、树立形象、传播文化的工具。

### 平台功能

#### 应用系统集成

待接入系统方管理员提供应用系统的相关资料给综合门户管理员，由综合门户管理员对将要接入综合门户的应用系统进行注册、审核和启用。启用的应用系统可以从用户中心同步组织机构和人员信息，并在综合门户中集中展示，实现统一入口。

##### 业务流程



待接入应用系统管理员提供应用系统的相关资料给综合门户管理员，包括应用中文名称、访问地址、LOGO、组织机构和人员的同步策略（全量或指定），由综合门户管理员对将要接入综合门户的应用系统进行注册、审核和启用。

##### 接入应用系统管理

对待接入应用系统的相关资料进行注册，包括应用中文名称、访问地址、LOGO、组织机构和人员的同步策略（全量或指定），资料核准无误后启用应用系统。

#### 单点登录

在多应用系统环境下，为提高用户的使用方便性，提高办公效率，需要实现用户对多系统的单点登录能力，减少用户的操作复杂度，确保“一点登录、多点漫游”，真正提高办公的高效性、快捷性。

##### 登录流程

通过单点登录统一认证，实现单点登录功能。当用户登录综合门户系统之后，不用再输入账号信息就可以直接访问已授权使用的其它应用系统。

如果用户直接访问各种业务系统时，则检测是否用户是否已单点登陆。没登录则重定向到单点登录服务器后进行登录；如果他已经访问过其他系统，认证中心会自动记住当前用户的身份，自动判断当前用户是否拥有足够的权限访问目标应用系统，从而避免了重复输入账户信息，在提供方便性的同时保证系统的安全性。

##### 单点登录客户端

单点登陆客户端集成在需要单点登录的业务系统，与业务系统部署在一起。对于应用系统每个需要访问控制的请求，单点登陆客户端会分析该请求中是否包含授权码，如果没有则说明访问用户未登录，并将请求重定向到指定的登录地址，同时传送需要访问的目标地址，以便登录成功后转向该地址。

单点登陆客户端需提供接口供业务系统初始化数据，如用户、组织机构、权限等信息。

##### 认证服务

提供集中身份认证服务，实现用户访问各应用资源的认证入口集中化和统一化。引入可靠的认证体系来对用户进行安全管理，通过为各个用户分配安全的身份凭证，确保各个应用系统登录的安全性。支持不同的身份凭证注册及认证，如静态密码、动态密码、CA证书、指纹识别，实现不同安全等级的统一身份认证服务。

**静态密码**

用户登录时，系统提示用户输入用户名和口令。系统采用加密方式或明文方式将用户名和口令传送到认证中心。并和认证中心保存的用户信息进行比对。如果验证通过，系统允许该用户进行随后的访问操作，否则拒绝用户的下一步的访问操作。

静态密码的优点是简单且成本低，但是如果用户不去修改它，那么这个密码就是固定不变的、长期有效的，因此这种认证信息的静态性，导致传统密码在很多情况下都有着发生密码泄密的危险。在整体安全认证中，对于浏览非重要资源的用户可以采用该方法。

**动态密码**

用户每次访问系统资源时产生不同的密码，即动态密码，解决静态密码认证服务发生密码泄密的危险。如用户登录时，将动态产生的密码已短信的方式发送到用户的手机上。用户输入动态密码后，系统将用户名和动态密码传送到认证中心，并和认证中心保存的用户信息进行比对。

**CA证书**

数字证书是目前最常用一种比较安全的身份认证技术。数字证书技术是在PKI体系基础上实现的，用户不但可以通过数字证书完成身份认证，还可以进一步进行安全加密，数字签名等操作。

数字证书的存储方式非常灵活，数字证书可被直接存储在计算机中，也可存储在智能卡或USB Key中。

**指纹识别**

生物识别是利用用户所特有的、可测量的生理和行为特征进行身份认证的一种技术。生物识别主要包括指纹、虹膜、人脸识别。

最常见的生物识别是指纹识别，指纹识别通常是先采集用户指纹图像，系统会对指纹图像进行预处理，去除指纹图像中的噪声，使图像画面清晰，然后再提取指纹特征，存入指纹库，当用户输入指纹信息时，系统将新输入指纹的特征信息与指纹库中所存指纹的细节特值进行对比，找出最相似的指纹作为识别的输出结果。

**OAuth2认证**

OAuth（开放授权）是一个开放标准，允许用户授权第三方网站访问他们存储在另外的服务提供者上的信息，而不需要将用户名和密码提供给第三方网站或分享他们数据的所有内容。Atuth2是OAuth协议的延续版本，要么通过组织在资源拥有者和HTTP服务商之间的被批准的交互作代表用户，要么允许第三方应用代表用户获得访问的权限。同时为Web应用、桌面应用和收集、起居室设备提供专门的认证流程。

##### 在线用户管理

系统管理员可以查看当前在线用户列表，提供强制用户下线功能。

##### 用户日志收集

业务系统所有的访问请求都需经单点登陆认证服务器认证，因此用户日志通过单点登陆认证服务器收集。需详细记录用户访问的应用系统、模块、功能，便于日后审计和统计分析。

#### 信息集成

聚集各应用系统的信息和资源。集中待办、待阅、任务、日程、站内容消息，实现统一待办；集成日程安排，实现日程集中管理；集成站内消息，实现站内消息的集中展示和提醒。

##### 待办待阅任务对接

各应用系统同步待办、待阅、任务数据至综合门户。综合门户集中展示用户在各应用系统的待办、待阅和任务。办公人员不需一一进入各应用系统，即可办理日常业务，实现统一待办。

##### 日程对接

各应用系统将用户的日程安排信息同步至综合门户，综合门户集中展示用户的所有日程安排，实现日程集中管理。

##### 站内信息对接

各应用系统将用户的站内消息同步至综合门户。综合门户集中展示和提醒用户接收的站内消息。办公人员不需一一进入各应用系统查看消息，提高办公效率。

#### 门户定制

可通过界面定制功能定制不同维度的多级门户，如基于角色可定义领导门户；基于组织机构可定义不同的部门门户。

同时普通用户也可以根据自己的实际需求将自己关心的内容和功能组织起来形成自己的个人门户。

界面定制功能主要包括门户组件管理、页面布局模板定制、页面风格定制以及内容定制。

##### 部件管理

部件是指在综合门户上展示的栏目、图表等粗粒度界面元素。这些部件是由综合门户管理员是在部件管理功能中进行注册和维护。常用的部件有应用导航、快捷办公、通讯录、通知公告、待办、待阅、任务、友情链接、日程管理、统计报表（由数学模型动态产生）。可根据需要定制部件并利用部件管理进行注册，注册后的部件就可以在定制门户时使用。

##### 模板管理

模板用来定义某类门户的整体结构，如采用上中下、左中右结构、左右结构，各个结构部分的高度和宽度。综合门户管理人员利用模板管理功能注册新模板，对所有可用模板进行维护。综合门户预先定义了适用于普通办公人员、领导、系统管理员办公门户的3种模板。

##### 门户管理

综合门户管理员负责维护所有门户，包括个人办公门户、领导门户。提供门户布局设计器，采用所见即所得的方式，选择适用的模板，选择需要的部件拖入设计器，调整部件的位置和顺序。将门户授权给角色或具体人员，这类角色或该人员登录后，所看到的就是授权的门户页面风格、组件和内容。

#### 内容管理

维护和发布门户空间各展示区域的数据，如通知公告、快捷办公、友情链接、通讯录、新闻等。

##### 通知公告管理

利用通知公告管理功能，系统管理员可以发布全网公告，所有用户都能接收到。单位管理员也可以发通知公告给其它单位，单位的人员登录综合门户后能接收到发给本单位的所有通知公告。

##### 友情链接管理

通过友情链接管理来维护它事务单位网站的外链，在综合门户上可展示所有的友情链接，点击链接可进入相应单位的网站。

##### 快捷办公管理

对用户经常使用功能，系统管理员可以通过快捷办公管理功能，将这些功能对应的应用系统的内部链接管理起来。在综合门户的快捷办公部件中统一展示，用户在综合门户上直接点击这些链接即可跳转进入应用系统的具体功能界面。

##### 通讯录管理

建立统一的通讯录，数据来源是各单位办公室统一维护的单位人员信息库；在统一通信录的基础上可以轻松地建立部门和个人通讯录。根据管理权限，每个工作人员只能见到能访问通讯信息。综合办公门户展示用户通信录，以便用户可以方便地进行联络沟通，并提供通信录维护功能。详情请参考用户中心的单位人员管理功能。

##### 互动交流

管理员在互动交流版块可以管理用户在门户上的提问，对不当的提问进行删除操作，对正常的提问进行回复。

##### 新闻管理

管理员可以通过新闻管理功能管理门户上的新闻内容，可对新闻进行增加、修改、删除、发布操作，新闻内容必须经过发布操作才会在门户上进行展示。

##### 渲染门户空间

用户登录成功后，立即展示的界面是管理员其定制好的门户空间。门户空间是基于管理员定制门户空间的模板、部件及其布局来渲染的。门户空间不负责具体内容的展示，而是由部件负责内容的加载和刷新。常用的部件有应用导航、快捷办公、通讯录、通知公告、待办、待阅、任务、友情链接、日程管理、统计报表，也可在部件管理功能中添加新的部件。

##### 站内消息查看

在综合门户显示当前用户接收到的站内消息。

##### 个人信息管理

用户可以在综合门户上修改自己的个人信息，如手机号码、EMAIL等，实现用户信息的及时更新。用户也可对密码进行及时变更，保障个人账户的安全性。

##### 部件定制

对于用户个人办公空间上展示的部件，用户可以自行选择是否展示或隐藏。

##### 界面布局调整

用户可以对个人办公空间上的部件位置、顺序进行调整，满足个性化需求。

##### 应用设置

用户可以设置应用导航部件上的应用系统是否展示或隐藏。

##### 快捷办公设置

用户可以设置快捷办公部件上的快捷办公链接是否展示或隐藏。

#### 领导指挥舱

领导桌面是专门针对各级领导个性化定制的个人门户，是领导办公业务的统一入口及信息集中展示平台。可根据领导的角色、权责范围以及个性化需求定义不同的界面布局、展现内容以及展现方式，从而让领导的日常办公操作更加人性化和便捷高效。

除此之外，领导桌面还可以整合展示来源于外部的各类信息资源，以大数据服务应用支撑为基础，结合中心资料库，通过海量数据挖掘、多维度分析、智能知识库加载、结构/非结构化数据融合等技术进行数据分析，辅助领导决策。

##### 领导桌面部件管理

部件是指在领导桌面上展示的栏目、图表等粗粒度界面元素。这些部件是由领导桌面管理员是在部件管理功能中进行注册和维护。常用的部件有工业经济、宏观经济、商事主体等统计报表（由数学模型动态产生）。可根据需要定制部件并利用部件管理进行注册，注册后的部件就可以在领导桌面管理时使用。

##### 领导桌面模板管理

模板用来定义某领导桌面的整体结构，如采用上中下、左中右结构、左右结构，各个结构部分的高度和宽度。领导桌面管理人员利用模板管理功能注册新模板，对所有可用模板进行维护。领导桌面预先定义了普通领导桌面模板。

##### 领导桌面设计及管理

领导桌面管理员负责维护所有领导桌面。通过门户布局设计器，采用所见即所得的方式设计领导桌面，可选择适用的模板，将需要的部件拖入设计器，并可调整部件的位置和顺序。将领导桌面授权给角色或具体领导，这类角色或该领导登录后，所看到的就是授权的领导桌面页面风格、组件和内容。

##### 领导桌面渲染

领导登录成功后，立即展示的界面是管理员其定制好的领导桌面。领导桌面是基于管理员定制的模板、部件及其布局来渲染的。领导桌面不负责具体内容的展示，而是由部件负责内容的加载和刷新。常用的部件有大气环境状况、水环境状况、声环境状况等统计报表，也可在部件管理功能中添加新的部件。

##### 领导桌面个人定制

领导可对桌面上展示的部件选择是否展示或隐藏，对桌面上的部件位置、顺序进行调整，满足个性化需求。

## 运行管理平台建设

运营支撑平台目的是为了建立政务信息资源共享交换平台运行管理系统，实现平台的全面运行环境监测、安全化以及智能化运维、数据定制化服务，为整个信息资源共享交换平台的稳定运行监管提供技术和服务支撑。

### 监控平台

#### 建设目标

监控系统实现对IT系统基础环境及各项业务系统的运行情况进行监控，建立集中的告警分析处理和故障预警机制，有效帮助运维人员快速定位故障，提高运维效率。包括服务器、存储、网络、系统软件、中间件（包含应用服务器、数据库等）、应用系统的运行状态的监控和预警。

提供智能化的监控服务，包括自动巡检、服务接口自动巡检、平台运行日报和周报、异常事件日志监控等。

能实时了解IT资源的使用情况，根据需要从整体角度考虑资源的配置、调剂和使用，提高资源的有效利用率。包括服务器的CPU、内存、磁盘空间、网络及磁盘IO使用情况的监控和预警。

#### 平台功能

##### 监控管理

实现对IT系统的全面监控，对IT信息环境及各项业务系统的运行情况进行监控，建立 集中的告警分析处理和故障预警机制，有效帮助运维人员快速定位故障，提高运维效率。包括服务器、存储、网络、系统软件、中间件（包含应用服务器、数据库等）、应用系统的运行状态和系统资源利用率的监控。

###### 节点管理

运维管理人员可以注册新节点，建立节点档案。可以修改节点信息、启用和禁用节点。

###### 数据源管理

运维管理人员可以注册新数据库，建立数据库档案，可以修改数据库信息、启用或禁用数据库。数据库档案包括包括IP地址、数据库实例名、用户名、密码、端口、所属节点IP等连接属性，作为后续的监控及数据运维的对象。

###### 网络设备管理

运维管理人员可以注册交换机、路由器档案，对其进行管理。网络设备档案包括IP、snmp端口、snmp版本等信息，作为后续的网络设备监控的基础信息。

###### 应用服务器管理

运维管理人员可以注册新应用服务器，建立应用服务器档案，修改应用服务器信息。应用服务器档案信息包括访问地址、访问端口、所属节点IP地址等属性信息，作为后续的监控及系统运维的对象。

###### 应用系统管理

运维管理人员可以注册新应用系统，建立应用系统档案，可以修改应用系统信息。应用系统档案包括所属应用服务器、应用访问上下文等属性，作为后续监控的基础信息。

###### 监控项启用管理

监控项是指服务器、数据库、应用服务器、应用系统和CPU、磁盘、内存等监控类型，监控规则是指监控项适用的节点、监控方式和参数信息。监控平台定时器需根据配置的监控启用项和监控规则启动对应监控。

###### 监控项禁用管理

对于不需要启用的某种监控项或节点、数据库、应用系统，可配置为监控禁用项。监控平台定时器需根据配置的监控禁用项来决定是否启用某监控。

###### 通知地址管理

对通知地址进行管理，支持邮件、短信和系统通知3种类型的地址注册。邮件对应的是邮箱地址，短信对应的电话号码，系统通知对应的是webservice或rest api的地址。

###### 通知发送列表

展示监控系统相关通知的发送详情，包含通知方式，通知内容的标题以及通知创建时间，点击具体记录可以查询通知的详细内容并提供下载附件功能。

##### 应用环境监控

实现对IT系统的全面监控，对IT信息环境及各项业务系统的运行情况进行监控，建立 集中的告警分析处理和故障预警机制，有效帮助运维人员快速定位故障，提高运维效率。包括服务器、存储、网络、系统软件、中间件（包含应用服务器、数据库等）、应用系统的运行状态和系统资源利用率的监控。

###### 监控看板

基于拓朴图、以节点为组织，展示平台所有节点及节点上的服务的运行状态，节点状态包括所有服务正常、部分服务异常、服务器网络中断3种状态，可查看具体节点的服务运行状态明细。

能实时查看各监控对象的预警信息和各监控对象分类的监控统计信息。

###### 连通状态详情

定时器需根据配置的监控项和监控规则驱动对应监控的数据采集，收集监控状态并过滤分类后产生监控结果。

支持服务器、存储、网络、系统软件、中间件（包含应用服务器、数据库等）、应用系统等资源的连通性监控。能展示以下连通状态详情:

###### 系统资源使用情况

图表化展示绑定服务器的CPU使用率、内存使用率、磁盘空间使用状态、MQ磁盘使用状态、DB磁盘适用状态的监控结果，状态分为正常、次要、紧急三种，并且以不同颜色标注，使运维人员能通过观图表迅速得出系统资源使用状态紧急的情况从而采取相应处理措施。

###### 前置订阅关系状态

通过图形展示与表格展示两种展示方式展示平台中存在订阅关系的单位前置机的互联互通情况。

###### 网络设备状态

图表化展示网络设备包括交换机、路由器的连通和预警状态。

###### 数据库性能

图表化展示数据库的连通和预警状态、数据库的连接情况。

###### 应用服务器性能

图表化展示应用服务器的连通和预警状态、进程和内存使用情况。

### 运维平台

#### 建设目标

运维系统主要用于整个统一业务应用系统平台的日常运维和管理，保障平台的高效和稳定运行。

#### 平台功能

##### 数据运维

###### 数据源管理

运维人员可以注册新数据库，建立数据库档案，可以修改数据库信息、启用或禁用数据库。数据库档案包括包括IP地址、数据库实例名、用户名、密码、端口、所属节点IP等连接属性，作为后续的监控及数据运维的对象。

###### 数据查询

运维人员选择数据库连接成功后可查询具体数据库的相关信息，

###### 数据更新

运维人员输入SQL脚本，选择要执行脚本的目标数据库，并输入执行脚本的备注说明等信息，建立系统表运维单，提交，由运维经理审核后开始真正执行。脚本执行结果在运维单的详情中展示。

###### 备份策略管理

提供要备份的数据源及备份策略的新增/修改/删除操作，并可进行备份的启动、停止操作。

###### 备份管理

查看备份的执行日志及产生的备份文件，并可选定备份文件进行数据库的恢复。

###### 恢复记录

查看数据库恢复的执行日志。列表信息包含：恢复数据源、恢复数据源IP、数据库类型、恢复文件名、备份文件大小、（恢复）状态、创建人、创建时间。

##### 系统运维

###### 节点管理

运维人员可以注册新节点，建立节点档案。可以修改节点信息、启用和禁用节点。节点档案包括节点IP地址、所属单位、中文命名等属性信息，作为后续运维的基础信息。

###### 远程控制台

运维人员可以在某个节点上打开一个运维指令控制台，在上面执行已经被授权的运维指令和操作系统命令，并实时查看指令执行的输出结果，这样就不需要使用SSH工具远程登陆到节点上操作，以方便节点的运维管理和权限控制、日志审计。

###### 日常运维指令管理

运维经理可以在这里预先录入一些常用的运维指令，并将它们授权给运维人员，或者将运维指令批量的发布到指令的节点上执行。

###### 指令分类

运维经理可以在这里对指令分类进行查询/新增/修改/删除操作。新增时主要是预先录入某些匹配规则，以便识别运维指令的类别。

###### 指令运行跟踪

运维人员和运维经理都可以在这里实时查看指令执行的输出和执行状态。

###### 运维指令授权

运维经理可以在这里根据实际需求将不同的指令类别/具体指令根据实际业务需要授权给不同的角色，具体的用户则通过绑定指定角色获取运维指令类别/具体指令，从而达到权限控制的目的。

##### 版本管理

###### 应用版本管理

运维人员可以在这里发布各种应用系统的版本，以便可以通过部署在各运行节点上的运维Shell进行部署、升级。新增后的版本包需进行发布操作后才能部署到服务器上。

###### 补丁管理

运维人员可以在这里发布各种应用系统的某个版本的补丁，以便可以通过部署在运行节点上的运维Shell进行补丁部署和升级。新增后的补丁包需进行发布操作后才能部署到服务器上。

###### 配置管理

运维人员可以在这里发布各种应用系统的项目配置文件，以便可以通过部署在运行节点上的运维Shell进行配置文件的部署和修改。

###### 版本回滚

运维人员可以在这里对应用版本、补丁和配置进行回滚操作，以便将最近一个升级更新操作回滚到上一个版本的状态下。

###### 部署进度跟踪

运维人员可以在这里实时查看版本、补丁、配置和回滚操作的状态和结果。

###### 安装路径配置

这里是版本管理的基础配置，需要配置各应用系统在各运行节点上的安装路径，以便向运维Shell发送版本管理指令时，运维Shell可以正确地将版本、补丁、配置部署到对应的路径上并重启对应的应用和服务。

###### 节点应用关联

运维经理/人员可以在改页面控制关联哪些节点上可以部署哪种类型的应用，以便简化运维人员发布版本管理的操作。

##### 运维工单

###### 运维工单管理

工作人员可以在这里提交工单至上级审核，上级审核通过之后将任务分配给运维人员，运维人员接单之后可以对任务进行跟踪直至处理结束。运维工单处理结束后经过归档操作则会纳入运维知识库。

###### 运维知识库

运维知识库包含2种来源，一种为手动新增，另一种为运维工单处理完成后的归档。该页面可提供运维知识库的查询/新增/修改/删除操作。

###### 运维知识库分类

提供运维知识库知识类别的管理，可以对知识类别进行增删查改操作。

##### 行为管理

###### 系统操作日志

展示用户操作日志、系统表运维日志、指令跟踪日志三种运维日志，这些日志记录了具体时间、IP、操作、内容、结果等信息，从而可以找出系统运维过程出现问题的具体原因。

### 数学模型建模系统

#### 建设目标

数学模型建模系统通过知识库、机器人连接指定基础环境，机器人通过调度任务执行各种数学模型，数学模型连接础环境进行分析计算,从而得出各种分析统计结果，并可作为后续自动化智能化决策或解决方案的依据。

#### 平台功能

##### 知识库管理

###### 规则模型库管理

规则模型是数学模型输入参数的匹配处理规则，可以让数学模型接收任意类型任意格式的数据，并通过规则模型匹配处理得出数学模型所需要的参数。

###### 标准模型库管理

标准模型库管理是数学模型输出参数的格式化处理标准，可以让数学模型输出指定标准格式的数据。

###### 数学模型管理

数学模型是智能运维的核心，它以机器人语言的形式描述了机器人任务的处理流程、操作定义、调用规则、执行内容、输入输出等处理逻辑，由机器人在指定调度时间里调用数学模型解释器，数学模型解释器加载数学模型、分析数学模型、处理执行数学模型、并输出数学模型的计算结果，机器人最后将输出结果保存。

数学模型中可以调用平台服务、调用外部服务、发送运维指令、收集事件异常等等。数学模型是一个解决方案的定义，由XML语言描述，有各种语法和主义，并由数学模型解释器相应的组件来执行处理。由数学模型库、规则模型库、标准模型库、页面组件库、事件异常分类组成的知识库可以实现自动化、智能化运维。

数学模型有建模工具和调试器来编写，可以在友好的可视化界面上完成建模和调试工作。

###### 页面组件管理

页面组件是数学模型输出展示的一种表达，可以是一种页面html、javascript脚本、静态文本等形式。从而实现多样的数学模型输出格式。

###### 事件异常分类

事件异常分类定义了机器人处理系统事件、系统异常时的匹配规则，并将匹配的事件、异常交由指定的数学模型进行处理。

##### 机器人与任务

###### 机器人管理

运维人员可以在这里新增、修改、删除机器人的定义，机器人有2种类型：任务机器人、监控机器人。可以启动、停止、废弃机器人。

###### 任务定义

机器人任务定义是由数学模型来作为任务的执行分析处理逻辑，任务描述来说明目的。任务最后会分配给机器人调度执行。

###### 机器人任务分配

运维人员可以在这里给机器人分配不同的任务，指定任务的调度规则。

###### 挂起管理

数学模型在分析处理过程中，可能会在某些指定的条件达成后挂起，并生成挂起记录，挂起同时会产生邮件、短信或界面方式的通知。由操作人员手工决定是否让挂起恢复执行。

###### 通知发送列表

这是机器人对数学模型输出结果的记录，将以邮件、短信的方式生成通知。运维人员可以在这里查看各种通知信息和通知发送状态。

###### 通知地址管理

通知地址的管理页面，可以对通知地址进行增删改查操作。

##### 接口服务管理

###### 服务管理与发布

这里可以管理向外提供服务的数学模型接口，可以进行增、删、改、查，启用、禁用、和发布。数学模型服务接口有3种类型：http接口、webservice接口和socket接口。分别对应于不同应用系统接入需求。

###### 应用系统接入

管理第三方应用系统的接入管理，并为应用系统分配一个app key，这样应用系统每次调用发布了的数学模型服务接口时，必须提供此app key为作鉴权。 这里可以进行增、删、改、查、启用、禁用、重新生成app key、设置appkey有效期、给应用系统分配数学模型服务接口。

###### 服务检索

用户通过页面搜索功能可以快速定位到具体的接口服务，同时可以查看每个对外提供服务的接口详细说明信息（可以理解为服务接口说明文档）。

### 定制化服务系统

#### 建设目标

定制化服务系统通过数据可视化功能提供BI（Business Intelligent）方案，可以快速生成商业分析用的各种图表和交互元素,协助决策人员进行业务数据分析和挖掘。同时对外提供接口服务，可将数据报表以及BI方案生成的图表交互页面通过接口形式发布给外部系统使用。

#### 平台功能

##### 数据可视化

###### 数据源管理

数据源是连接第三方数据库的各种参数设置信息。工作人员可以在这里管理维护各种需要进行报表分析的数据源信息。同时该功能模块提供通过Excel导入的方式创建数据源，以便适应于不能直连第三方数据库的情景。

###### 数据集管理

数据集是数据源中某一个表或一个查询语句返回的行列数据集。数据集将会是后续仪表板中图表的绑定对象，绑定成功之后便可在图表上展示数据。数据集定义了图表所需要的维度、量度的信息。数据集可以进行关联，从而得到业务所需要的数据。

###### 工作表管理

工作表是对数据集的进一步处理，比如过滤列，加入复杂的查询条件等。

页面列表展示已经整理好的数据集，点击修改可以对数据集进行修改操作，可选择对不同维度的排序整理，也可以根据需要针对不同的字段进行增加过滤条件，同时操作界面提供预览功能，可查看整理好的工作表效果。

###### 仪表板管理

仪表板管理是将各种图表、界面交互元素以相应的布局组合而成的报表看板，这里将提供仪表板的图形化建模工具，可以方便快捷地通过拖放图表和交互元素来生成仪表板。

###### 我的仪表板

页面展示已经创建好的所有仪表板效果图并提供查询功能。在此页面上用户可以直接预览全部已经创建完成的仪表板。

###### 领导驾驶舱

通过汇集各类基础数据、平台数据、主题库数据、业务数据，集中化、实时化、图形化展示各类业务数据、投放到大屏墙上显示，以辅助领导做决策和分析。提供丰富多彩的各类统计图表、地图图表，布局样式、界面元素，以便生成可以满足各种大屏定制场景需求的效果。

##### 接口服务管理

###### 服务管理与发布

管理向外提供服务的定制化（包含数据处理和可视化图表）接口，可以对接口服务进行增、删、改、查，启用、禁用、和发布操作。服务接口有3种类型：http接口、webservice接口和socket接口，可以灵活满足不同应用系统的接入需求。

###### 应用系统接入

管理第三方应用系统的接入管理，并为应用系统分配一个app key，这样应用系统每次调用发布了的定制化服务接口时，必须提供此app key为作鉴权。 这里可以进行增、删、改、查、启用、禁用、重新生成app key、设置appkey有效期、给应用系统分配数学模型服务接口。

###### 服务检索

用户通过页面搜索功能可以快速定位到具体的接口服务，同时可以查看每个对外提供服务的接口详细说明信息（可以理解为服务接口说明文档）。

## 信息安全与支撑平台建设

### 信息安全

信息安全为硬件、软件、物理环境及基础设施保驾护航，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常的运行，信息服务不中断，最终实现业务连续性。

#### 信息安全设计

##### 物理安全

物理安全风险主要是指网络周边的环境和物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力。例如：

* 机房缺乏控制，人员随意出入带来的风险；
* 网络设备被盗、被毁坏；
* 线路老化或是有意、无意的破坏线路；
* 设备在非预测情况下发生故障、停电等；
* 自然灾害如地震、水灾、火灾、雷击等；
* 电磁干扰等。

为满足物理安全相关技术要求，系统部署机房、办公场地要具备一定程度防震、防火、防风、防雷、防水、防潮、防静电、防雷击、防盗窃、防破坏的能力；同时加强机房场所的管理，要有专人值守和规范化的机房进出申请、审批、登记制度，来访人员有专人全程陪同，并限制和监控其活动范围；以及要有温湿度控制、电力供应保障、电磁防护等防护措施。

##### 网络安全

网络的安全根据应用的安全级别有不同的安全性措施，在将来可能的应用中，网络安全性级别由高到低的顺序依次为：市政府内网、市政府公众网、市政府外网。

网络结构的安全主要指，网络拓扑结构是否合理；线路是否有冗余；路由是否冗余，防止单点失败等。

根据国家对网络安全性要求，在市政府内网与市政府外网之间、市政府内网与市政府公众网门户之间都有相应的规定，必须遵守这些规章制度。特别是外网与内网之间必须在物理上隔离。

在考虑内网系统的安全性时，需要重点考虑以下问题：

数据链路层及网络层的信道加密；

网络防火墙、访问代理、攻击检测；

系统监控、日志分析等。

##### 设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；设备冗余备份；通过严格管理及提高员工的整体安全意识来实现。

主机设备主要指数据库服务器、应用服务器、邮件服务器、文件传输服务器等，这些设备的安全性主要由主机本身来保证。

对于工作站、输入/输出设备等设备来说，可根据应用安全性要求，采取不同的安全性措施（这里包括管理措施），特别是对于核心应用而言，建议采用设备证书方式加强其安全性。

设备证书是平台设备的身份证书，可信WEB服务平台使用多证书实体密码鉴别器作为设备证书。多证书实体鉴别密码器是信息安全平台的终端产品系列之一和用户终端PKI安全服务调用的支持设备，是密钥材料、密码运算的载体,是实现基于PKI架构的“一人一证”，“一机一证”的强身份管理的关键设备，为分布式计算环境中终端实体（包括用户个人和终端设备）提供唯一性身份标识，多证书实体鉴别密码器同样是为上层应用提供各种PKI服务支持以及用户敏感信息的存储管理的设备。

##### 系统安全

###### 操作系统安全

对于操作系统的安全防范可以采取如下策略：尽量采用安全性较高的网络操作系统并进行必要的安全配置、关闭一些起不常用却存在安全隐患的应用、对一些保存有用户信息及其口令的关键文件（如Windows NT下的LMHOST、SAM等）使用权限进行严格限制；加强口令字的使用（增加口令复杂程度、不要使用与用户身份有关的、容易猜测的信息作为口令），并及时给系统打补丁、系统内部的相互调用不对外公开。

通过配备操作系统安全扫描系统对操作系统进行安全性扫描，发现其中存在的安全漏洞，并有针对性地进行对网络设备重新配置或升级。

###### 应用系统安全

在应用系统安全上，应用服务器尽量不要开放一些没有经常用的协议及协议端口号。如文件服务、电子邮件服务器等应用系统，可以关闭服务器上如HTTP、FTP、TELNET、RLOGIN等服务。还有就是加强登录身份认证。确保用户使用的合法性；并严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。充分利用操作系统和应用系统本身的日志功能，对用户所访问的信息做记录，为事后审查提供依据。

###### 隔离与访问控制

(1)严格的管理制度

可制定的制度有：《用户授权实施细则》、《口令字及账户管理规范》、《权限管理制度》、《安全责任制度》等。

(2)配备防火墙

防火墙是实现网络安全最基本、最经济、最有效的安全措施之一。防火墙通过制定严格的安全策略实现内外网络或内部网络不同信任域之间的隔离与访问控制。并且防火墙可以实现单向或双向控制，对一些高层协议实现较细粒的访问控制。

###### 入侵检测

利用防火墙并经过严格配置，可以阻止各种不安全访问通过防火墙，从而降低安全风险。但是，网络安全不可能完全依靠防火墙单一产品来实现，网络安全是个整体的，必须配相应的安全产品，作为防火墙的必要补充。入侵检测系统就是最好的安全产品，入侵检测系统是根据已有的、最新的攻击手段的信息代码对进出网段的所有操作行为进行实时监控、记录，并按制定的策略实行响应（阻断、报警、发送E-mail）。从而防止针对网络的攻击与犯罪行为。入侵检测系统一般包括控制台和探测器（网络引擎）。控制台用作制定及管理所有探测器（网络引擎）。探测器（网络引擎）用作监听进出网络的访问行为，根据控制台的指令执行相应行为。由于探测器采取的是监听不是过滤数据包，因此，入侵检测系统的应用不会对网络系统性能造成多大影响。

###### 病毒防护

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力。我们都知道，网络系统中使用的操作系统一般均为WINDOWS系统，比较容易感染病毒。因此计算机病毒的防范也是网络安全建设中应该考虑的重要的环节之一。反病毒技术包括预防病毒、检测病毒和杀毒三种技术。

##### 应用安全

###### 资源共享

严格控制内部员工对网络共享资源的使用。在内部子网中一般不要轻易开放共享目录，否则较容易因为疏忽而在与员工间交换信息时泄漏重要信息。对有经常交换信息需求的用户，在共享时也必须加上必要的口令认证机制，即只有通过口令的认证才允许访问数据。虽然说用户名加口令的机制不是很安全，但对一般用户而言，还是起到一定的安全防护，即使有刻意破解者，只要口令设得复杂些，也得花费相当长的时间。

###### 信息存储

对有涉及秘密信息的用户主机，使用者在应用过程中应该做到尽量少开放一些不常用的网络服务。对数据服务器中的数据库必须做安全备份。通过网络备份系统，可以对数据库进行远程备份存储。

##### 信息安全保障体系

安全保障是综合的、相互关联的，不仅仅是技术问题，而是人、管理和技术三大要素的结合，构成动态的信息与网络安全保障体系框架WPDRR模型，实现系统的安全保障。WPDRR是指：预警（Warning）、保护（Protection）、检测（Detection）、反应（Reaction）、恢复（Recovery），五个环节具有时间关系和动态闭环反馈关系。



**信息安全体系基本框架示意图**

预警：利用远程安全评估系统提供的模拟攻击技术来检查系统存在的、可能被利用的脆弱环节，收集和测试网络与信息的安全风险所在，并以直观的方式进行报告，提供解决方案的建议，在经过分析后，了解网络的风险变化趋势和严重风险点，从而有效降低网络的总体风险，保护关键业务和数据。

保护：保护通常是通过采用成熟的信息安全技术及方法来实现网络与信息的安全，主要有防火墙、授权、加密、认证等。

检测：通过检测和监控网络以及系统，来发现新的威胁和弱点，强制执行安全策略。在这个过程中采用入侵检测、恶意代码过滤等等这样一些技术，形成动态检测的制度，建立报告协调机制，提高检测的实时性。

反应：在检测到安全漏洞和安全事件之后必须及时做出正确的响应，从而把系统调整到安全状态。为此需要相应的报警、跟踪、处理系统，其中处理包括封堵、隔离、报告等子系统。

恢复：灾难恢复系统是当网络、数据、服务受到黑客攻击并遭到破坏或影响后，通过必要的技术手段（如容错、冗余、备份、替换、修复等），在尽可能短的时间内使系统恢复正常。

###### 安全区域策略

根据安全区域的划分，主管部门应制定针对性的安全策略。

1、定期对关键区域进行审计评估，建立安全风险基线

2、对于关键区域安装分布式入侵检测系统；

3、部署防病毒系统防止恶意脚本、木马和病毒

4、建立备份和灾难恢复的系统；

5、建立单点登录系统，进行统一的授权、认证；

6、配置网络设备防预拒绝服务攻击；

7、定期对关键区域进行安全漏洞扫描和网络审计，并针对扫描结果进行系统加固。

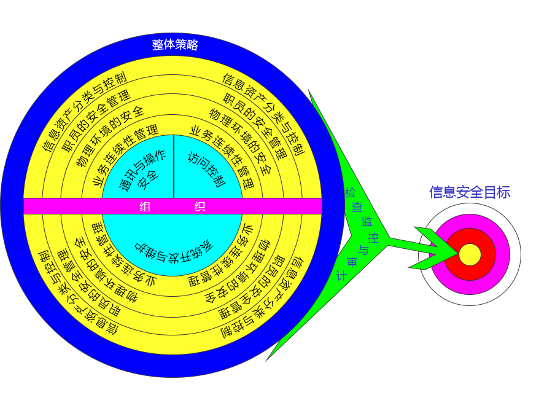
###### 网络安全管理

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠地运行，将起到十分有效的作用。

安全体系建设中，安全管理是一个非常重要的部分。任何的安全技术保障措施，最终要落实到具体的管理规章制度以及具体的管理人员职责上，并通过管理人员的工作得到实现。

安全管理遵循国际标准ISO17799，它强调管理体系的有效性、经济性、全面性、普遍性和开放性，目的是为希望达到一定管理效果的组织提供一种高质量、高实用性的参照。各单位以此为参照建立自己的信息安全管理体系，可以在别人经验的基础上根据自己的实际情况进行设计、取舍，以达到对信息进行良好管理的目的。信息安全不仅仅是一个技术问题，更重要的是一个管理问题。对一种资产进行保护的最好方法就是为它建立一个完整的、科学的管理体系。建立和实施信息安全管理体系（ISMS）是保障企事业单位、政府机构信息安全的重要措施。目前世界上包括中国在内的绝大多数政府签署协议支持并认可ISO17799标准。

其组成部分如图所示，各模块的作用如下：



**管理体制图**

1）总体策略

确定安全的总体目标，所遵循的原则。

2）组织

确定安全策略之后，必须明确责任部门，落实具体的实施部门。

3）信息资产分类与控制、职员的安全、物理环境的安全、业务连续性管理

有了目标和责任单位，紧接着要求我们必须仔细考虑流程，从信息资产、人、物理环境、业务可用性等方面考虑安全的具体内容。

4）通信与操作安全、访问控制、系统开发与维护

这三方面属于解决安全的技术问题，即解决如何做的问题？如何通过技术支撑安全目标、安全策略和安全内容的实施。

5）检查监控与审计

用于检查安全措施的效果，评估安全措施执行的情况和实施效果。

###### 安全运行组织

安全运行管理组织体系主要由主管领导、信息中心和业务应用相关部门组成，其中领导是核心，信息中心是系统运行管理体系的实体化组织，业务应用相关部门是系统支撑平台的直接使用者。

确定系统内部的管理职能部门，明确责任部门，也就是要组织安全运行管理团队，由该部门负责运行的安全维护问题。

###### 安全管理制度

面对网络安全的脆弱性，除在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须建立网络的安全管理。明确安全职责，制定安全管理制度，实施安全管理的原则为：多人负责原则、任期有限原则、职责分离原则。

###### 应急响应机制

筹建管理人员和技术人员共同参与的内部组织，提出应急响应的计划和程序，提供计算机系统和网络安全事件的提供技术支持和指导；提供安全漏洞或隐患信息的通告、分析；事件统计分析报告；提供安全事件处理相关的培训。

##### 信息安全病毒防御

###### 网络入侵防御

网络入侵检测系统基于网络和系统的实时安全监控，对来自内部和外部的非法入侵行为做到及时响应、告警和记录日志，具体功能描述如下：

1. 支持统一的管理平台，实现集中式的安全监控管理；
2. 自动识别攻击类型；
3. 支持按行为特征的入侵检测；
4. 能够在检测到入侵事件时，自动执行预定义的动作，包括切断服务、记录入侵过程、邮件报警等方式；
5. 支持集中的攻击特征和攻击取证数据库管理；
6. 支持攻击特征信息的集中式发布和攻击取证信息的分布式上载；
7. 提供对监视引擎和检测特征的定期更新服务，更新方式有多种，包括厂家的直接服务和联网更新操作；
8. 支持内置的风险评估工具（扫描器）；
9. 具有内置的网络使用状况监控工具和网络监听工具；
10. 支持纳入网络信任域进行可信管理。

###### 漏洞扫描与系统加固

目前，本项目可能存在以下漏洞:

1. 系统设置配置不当使得普通用户权限过高；
2. 管理员由于操作不当使得系统被安装了后门程序；
3. 系统本身或应用程序存在可被利用的漏洞。

网络漏洞扫描系统主要扫描以下内容：

1. Web服务；
2. FTP服务；
3. 守护进程；
4. 电子邮件服务；
5. CGI-BIN；
6. 浏览器设置；
7. RPC攻击；
8. 特定的强力攻击选项；
9. 拒绝服务攻击检测；
10. 安全市检测；
11. 用户策略。

网络漏洞扫描系统必须能够动态地分析目标系统的安全脆弱性，并实现以下功能：

1. 根据不同的对象类型，自动寻找匹配的扫描策略进行下一步的分析扫描。
2. 远程在线升级远程下载升级模块，自动完成升级过程。
3. 灵活的策略配置可按照特定的需求配置多种扫描策略和扫描参数，实现不同内容、不同级别、不同程度、不同层次的扫描。
4. 多种形式的报表全面详细的分析报告能力，可根据用户的不同需求提供不同层次的报告，并提供安全补丁供应商的热连接，快速及时的修补漏洞。
5. 实用的模拟攻击工具系统提供用于测试的模拟攻击，较好反映了黑客实际攻击的必经之路，同时对被测试系统的测试力度可控，不会为系统带来危害。
6. 合理的结构化设计、模块的继承性，使得系统具有很大的可扩展空间。

###### 信息防篡改

Web信息防篡改系统是网络安全防御体系的重要组成部分,它监控Web服务器和应用服务器上的文件目录,并通过可信部署进行合法更新。

系统中使用的Web信息防篡改系统必须符合以下功能：

必须能够支持多种服务器操作系统，例如：Windows系列、UNIX系列、Linux系列等；

1. 必须具有非常高效的信息扫描速率，同时，还不影响服务器的工作效率；
2. 具有集成发布与监控功能，使系统能够区分合法更新与非法篡改；
3. 实时发布与备份；
4. 自动监控；
5. 自动恢复；
6. 自动报警；
7. 日志管理；
8. 扫描策略管理；
9. 更新管理。

### 支撑平台

集成管理支撑平台(PowerEIMS)在长期的开发使用中，已经积累了很多成熟的可复用的模块，使用这些模块可以极大地缩短开发周期，提高开发质量。在公司开发的产品和项目中，可以完全复用或以很小的改动重用PowerEIMS的功能模块。支撑平台主要由数据管理、认证服务、组织机构管理、日志管理、表单建模、流程引擎、通信服务、平台组件、接口管理、服务管理、权限体系等功能组成。

#### 建设目标

使用PowerEIMS作为开发基础平台可以直接满足政务信息资源共享交换平台的支撑需求，实现以下建设目标：

* 实现认证、授权等基础功能的统一管理，为各部门提供基础功能服务；
* 为跨部门应用系统建设提供技术支撑环境和服务；
* 在新的信息交换与共享平台上开发新应用，实现信息资源的最大增值。

#### 平台功能

##### 数据同步

基于细粒度授权的需求，各业务系统必须有组织机构和人员信息的支撑，来实现业务系统内部的细粒度授权。各业务系统必须从用户中心同步组织人员的基本信息。

首先在用户中心注册业务系统的接入信息，指定其组织结构和用户信息同步策略，用户中心管理员对业务系统接入信息进行核准和授权。提供以下数据同步服务接口：

1）组织机构信息全量同步接口；

2）组织机构信息增量同步接口；

3）人员信息全量同步接口；

4）人员信息增量同步接口。

提供API，支持各类同构与异构系统的接入， 提供至少2种主流开发语言的SDK包。

##### 认证服务

提供全市集中身份认证服务，实现用户访问各应用资源的认证入口集中化和统一化。对于重要的应用系统或功能模块，为加强安全性，需引入可靠的认证体系来对用户进行安全管理，通过为各个用户分配安全的身份凭证，确保各个应用系统登录的安全性。同时，由于各应用系统自身的安全等级不同，统一用户及授权管理系统应能根据应用资源的不同安全等级支持不同的身份凭证注册及认证，如静态密码、动态密码、CA证书、指纹识别，实现不同安全等级的统一身份认证服务。

###### 静态密码

静态密码是最传统且最普遍的身份认证方法，通常采用如下形式：当用户需要访问系统资源时，系统提示用户输入用户名和口令。系统采用加密方式或明文方式将用户名和口令传送到认证中心。并和认证中心保存的用户信息进行比对。如果验证通过，系统允许该用户进行随后的访问操作，否则拒绝用户的下一步的访问操作。

###### 动态密码

用户每次访问系统资源时产生不同的密码，即动态密码，解决静态密码认证服务发生密码泄密的危险。如用户登录时，将动态产生的密码以短信的方式发送到用户的手机上。用户输入动态密码后，系统将用户名和动态密码传送到认证中心，并和认证中心保存的用户信息进行比对。

###### CA证书

数字证书是目前最常用一种比较安全的身份认证技术。数字证书技术是在PKI体系基础上实现的，用户不但可以通过数字证书完成身份认证，还可以进一步进行安全加密，数字签名等操作。

CA中心的服务结构将根据各CA中心的具体功能和服务对象而定，典型的服务结构主要包括：证书签发服务、CRL发布服务、证书状态查询服务、证书存储服务、控制台及受理审核服务等。

各证书审核注册中心RA是数字证书申请受理及审核单位，是证书认证系统不可缺少的功能模块，由CA中心授权运作。RA负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书，由能够承担这些责任的部门担任。

证书审核注册中心RA下设业务受理点，作为RA的派出单位，业务受理点负责对申请证书的机构、实体进行初步身份审核，并代理RA进行数字证书的发放。

安全服务为项目中的各种应用提供所需的各种安全服务功能。

###### 指纹识别

生物识别是利用用户所特有的、可测量的生理和行为特征进行身份认证的一种技术。生物识别主要包括指纹、虹膜、人脸识别。

##### 组织机构管理

根据业务需求，平台提供组织机构管理功能，范围包含党政机关所有的组织对象，功能包括：区划管理、单位管理、人员管理、职能管理等。

###### 区划管理

区划管理的元素包含：区划编码、区划名称、上级区划编码、上级区划名称、行政区划级别、排序号、状态等。操作功能包括：区划新增、区划修改、区划删除、区划查询等。

###### 单位管理

单位管理的元素包含：单位名称、单位编号、区划名称、机构类型、排序号、状态等。操作功能包括：单位新增、单位修改、单位删除、单位查询、下属人员的查看、单位信息导出等。

###### 人员管理

人员管理的元素包含：用户名、人员名称、手机号码、排序号、状态等，操作功能包括：人员新增、人员修改、人员删除、人员查询、人员禁用、人员启用、人员信息导出、添加已有人员等。

###### 职能管理

职能管理的元素包含：职能名称、职能编号、所属部门、描述等，操作功能包括：职能新增、职能修改、职能删除、职能查询等。

###### 用户组管理

用户组管理的元素包含：用户组名称、用户组编号、状态等，操作功能包括：用户组新增、用户组修改、用户组删除、用户组查询、用户组成员的添加等。

##### 日志管理

日志跟踪记录登录者的行为信息包含：组织机构管理日志、权限管理日志、个人中心操作日志、流程审批日志等，日志内容包括用户名称、部门、IP地址、操作时间、操作等，并提供日志详情查看功能。

##### 表单建模

通过表单定制模块开发人员可以不需要编写代码，只需要通过表单定制引擎中的表单数据定制、表单数据解析、表单数据操作功能来完成对业务表的数据维护操作。以及在定制表数据维护操作页面添加一系列的扩展功能。

* **表单配制引擎**

表单配制引擎包括数据表结构定义、数据展示模板定义、数据操作模板定义，还包括一些界面控件，界面布局控件。

* **表单解析引擎**

表单解析引擎会解析开发人员配制的表单配制信息，通过解析信息展现此表单，包括表单的数据显示区域与数据编辑区域。

* **数据操作引擎**

数据操作引擎会根据对定制出的表单数据进行数据操作。包括日常数据维护以及用户配置的一些高级操作。

##### 流程引擎

支撑平台提供自主研发的工作流引擎，通过流程编排，统一调控各个业务流程，以确保工作在正确的时间被正确的人执行，达到优化整体业务过程的目的。BPM概念的贯彻执行，需要有标准化的流程定义语言来支撑，使用统一的语言遵循一致标准描述具体业务流程，这些流程定义描述由专有引擎去驱动执行。这个引擎就是工作流引擎，它作为BPM的核心发动机，为各个流程定义提供解析、执行、和编排，驱动流程“动”起来，让大家的工作“流”起来，为BPM的应用提供基本、核心的动力来源。

##### 通信服务

###### 邮件管理

根据业务需求，将用户注册管理与内部邮件实行统一管理，提高内部员工的沟通速度。邮件管理功能实现记录邮件的发送记录管理和邮件模板管理。

###### 短信管理

根据业务需求，实现平台短信的统一管理、统一发送。手机短信息服务器用来实现手机短信息的接收、存储、转发、重发，短信息的优先级、短信息设定，实时、定时发送，群发，状态监控、配置和管理等，提供开放的接口，方便将短消息系统与各种计算机应用系统结合在一起，平台提供统一的短信接口。

##### 平台组件

集成管理平台(PowerEIMS)在长期的开发使用中，已经积累了很多成熟的可复用的模块，使用这些模块可以极大地缩短开发周期，提高开发质量。在公司开的产品和项目中，可以完全复用或以很小的改动重用PowerEIMS的数据交换中心模块、数据管理模块、企业级搜索平台等模块，完全实现组件化、架构化。使用PowerEIMS作为开发基础平台可以直接满足各应用平台的技术要求。

提供内容：

1.实现认证、授权等基础功能的统一管理，为各部门提供基础功能服务；

2.为跨部门应用系统建设提供技术支撑环境和服务；

3.在新的平台上开发新应用，提供前端一系列的组件。

##### 接口管理

根据业务需求，系统之间业务交互越来越频繁，接口调用也越来越多，提供与其他应用系统的数据交换接口管理功能，方便接口的统一管理、统一维护。接口管理主要分三大部分：

* 接口配置
* 接口日志
* 接口监控

##### 服务管理

通过集成管理平台提供的授权管理服务机能，就能建立用户的各层次的访问控制机能，从用户认证和授权、数据库对象的访问控制、用户操作权限控制到系统操作的记录和稽核，确保系统运行的安全性。

通过支撑平台提供的服务组件，用户可以实现应用级的操作日志和审计功能，即记录操作员进入和退出的时间，记录每项重要的操作。提供对各类操作痕迹的审计追踪功能，确保用户的每个行为都能产生必要的操作痕迹，并能以防抵赖的方式提供事后的审计验证支持。

对外具体开放性、可扩展性，可提供API等接口服务方式与外部系统进行无缝集成对接。

##### 权限体系

###### 统一授权管理

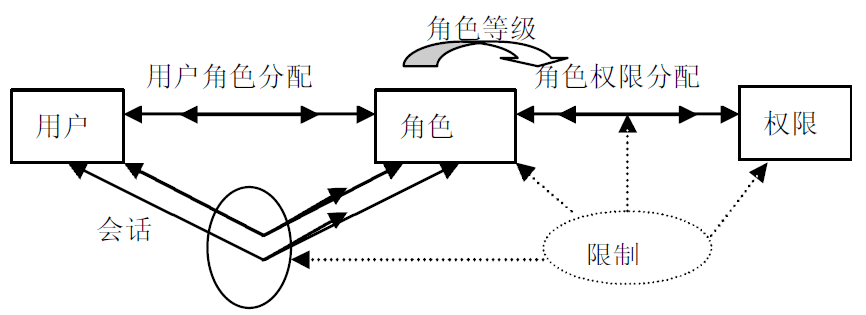
用户的角色多种多样，在不同的业务系统中具有不同的角色，在不同的岗位具有不同的权限，如何保障多身份下合理的授权，保障业务资源的安全访问，就需要在统一身份用户管理的基础上，实现对所有用户的统一授权管理，构建分布式管理模式，提供灵活的粗细粒度的多种授权模式，包括应用系统级粗粒度访问控制授权、系统功能调用级细粒度访问控制授权以及基于工作流的授权信息审批，从而提供责权分明的资源保护机制，真正实现“各职其责，杜绝越权”。

统一授权管理主要是管理员通过用户中心，实现对全市所有用户的授权。授权主要分为应用系统级的和系统功能调用级两种授权模式。

统一权限管理是按照基于角色的访问控制模型，提供应用、角色、功能、被授权对象和服务范围的管理，采用基于角色的访问控制，用户所能访问的权限就由该用户所拥有的所有角色的功能集合的并集决定。

平台内的所有应用，遵循统一授权管理规范，使用统一的授权接口进行。

统一权限基于SOA架构向应用提供Web Service服务用于权限信息查询和维护等服务。



图：基于角色的访问控制模型图

###### 机构管理员设定

平台可以按组织机构指定管理员,应用系统内部的模块操作级(如增删改查等)细粒度的授权由应用系统自身的授权管理功能来完成。

###### 机构角色授权

机构管理员可以在机构内增加角色，并对角色授权,机构根据权限配置的需要，任意设置具有不同权限的角色；为用户赋予不同角色来控制用户使用系统和信息的权限，为方便不同用户的不同需求以及特殊的权限管理，每个用户都可以同时拥有多个角色，例如控制给用户显示的应用菜单和按钮。通过权限管理，用户只能浏览属于其职责范围内的信息、使用属于其权限范围内的系统功能。系统提供角色维护，角色功能管理，角色岗位管理，网站权限管理等功能。

###### 设置多个系统管理员

平台可以设置多个系统管理员,机构根据权限配置的需要，任意设置具体管理员角色，为多个用户赋予管理员的控制权限。也可以根据业务需要，配置不同管理角色，分别给不同管理员设置不同的管理权力。

###### 批量授权

平台实现批量授权，方便管理员针对大批量的用户进行批量授权、批量管理。系统管理员根据权限配置的需要，任意设置单个用户授权或者多用户批量授权。

## 标准规范体系建设

### 符合国家相关标准和技术要求

1. 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》(国发﹝2012﹞23号)
2. 《全国企业基础信息共享和应用建设实施要求》（国信办[2005]10号）
3. 《电子政务信息共享互联互通平台总体框架技术指南》（国办秘函[2004]79号）
4. 《政务信息交换体系》（GB/T 21062-2007）
5. 《国家电子政务总体框架》（国信办[2006]2号）
6. 《中共中央办公厅国务院办公厅关于转发〈国家信息化领导小组关于我国电子政务建设指导意见〉的通知》 （中办发〔2002〕17 号）
7. 《中共中央办公厅国务院办公厅关于加强信息资源开发利用工作的若干意见》（中办发〔2004〕34 号）
8. 《关于印发〈国家电子政务总体框架〉的通知》（国信发〔2006〕2 号）
9. 《[信息安全等级保护](http://baike.baidu.com/view/3636116.htm)管理办法》[信息安全等级保护管理办法（公通字[2007]43号）](http://www.mps.gov.cn/n16/n1282/n3493/n3793/n494630/494907.html)
10. 《关于加快推进国家电子政务外网建设工作的通知》（发改高技[2009]988号）
11. 《国家电子政务“十二五”规划》（工信部规(2011) 567 号）
12. 《关于印发“十二五”国家政务信息化工程建设规划”的通知》（发改高技[2012]1202号）

### 标准规范研究与制定整体流程

本项目平台标准规范制定过程要经过规划、研制、试用验证、培训与宣贯、应用示范、完善与实施等六个阶段，而每个阶段的工作都需要在统一的标准规范工作平台上完成。

### 文档规范化的方法

在信息资源交换过程中包括文档等非结构化数据的交换，因此进行文档规范化非常必要。文档规范化阶段是根据业务建模阶段产生的业务模型，并根据数据规范化阶段产生的标准数据元目录和信息表示和信息分类目录，基于相关的文档格式管理法规和基于XML的电子文档格式设计指南，在业务专家、XML文档设计专家及XML文档设计工具，进行电子文档的设计，最终产生用于各类信息资源间信息交换和信息共享的各类电子文档和电子文档模型库，以实现各类信息资源间的信息共享。文档规范化阶段是数据规范化成果实际应用的关键，是实现离散数据有效合成的重要途径。该阶段是业务领域专家和电子文档设计专家对各类电子文档格式进行规范化设计和管理的过程，并形成一批电子文档格式规范。各类电子文档规范化必须依赖于数据规范化阶段成果，各类电子文档处理系统也要依赖于数据规范化阶段成果才能实现对各类规范电子文档的有效处理。标准数据元素是构造完整信息的基本单元，而各类电子文档则是传递各类业务信息的有效载体，并是粘合标准数据元素的粘合剂。因此，文档规范化阶段是数据规范化成果及信息共享的关键应用，是将各信息系统及各应用间的孤立信息集成并达到共享的有效途径。

### 数据标准规范设计

数据标准规范设计主要实现对共享数据与交换数据标准的编码框架（信息分类编码）、业务类指标分类编码与数据结构、标准制订主要过程、标准实施过程与办法、标准管理维护过程与办法的详细设计。对数据中心的数据标准规范进行初步的设计，将来在充分调研的基础上，加以改进调整。

### 技术标准规范设计

技术标准规范主要为数据交换与接口，以及业务系统设计提出可参照的标准规范。技术标准规范的制定主要依据《电子政务信息资源目录体系国家标准》和《电子政务信息资源交换体系国家标准》，结合信息资源现状以及我们在数据交换平台建设方面的技术与经验进行制定。

### 管理标准规范设计

#### 标准管理

标准管理是为做好标准宣贯、执行、版本、变更机制等工作而制定的，对标准的管理提供具体方法。

* 标准宣贯方法要点

标准的培训与宣贯是在标准化过程中，尤其是标准的制定过程中，需要不断地试用并验证标准的正确性和可用性。

* 标准执行监督管理

监督标准执行实施的主要工作是：

* 制定推广应用、全程监控的技术方案与组织方案
* 建立实施的质量控制体系，坚持标准符合性测试与认证
* 在共性、关键性工程项目上重点实施相关标准
* 对实施结果进行综合评估
* 标准版本管理工作

标准版本管理工作主要有：

* 设立专人负责标准的版本管理工作
* 标准的版本管理包括文档的管理与系统标准版本管理
* 解决数据中心与各业务系统标准版本的一致性问题
* 由标准审核小组确定版本的更新原则
* 标准变更机制
* 标准的变更机制参照数据标准的更新维护方法流程。

### 项目标准规范设计

本项目在设计和建设过程中，将采用并遵照以下标准：

* **技术标准**

**Web服务标准-UDDI,WSDL和SOAP：**该标准的使用可以实现跨不同系统环境的应用之间的通信；

**XML技术标准：**采用XML技术标准，实现系统的异构；

**WFMC标准：**在工作流平台中，我们采用WFMC（工作流管理组织）的规范，实现流程定义与其他流程管理平台的接口；

**MVC开发规范：**MVC开发模式是一种先进的技术构架，有助于软件构件化的实现，提高系统的复用性和可维护性。

开发标准

**CMM规范：**在需求、设计、开发、测试、实施等阶段严格遵守CMM规范；

**软件工程规范：**在设计采用Rational Rose可视化建模工具统一建模。采用RUP进行需求、设计、编码、测试等软件开发过程的统一管理；

**文档规范：**严格遵循CMM规范中的要求，对技术文档和管理文档进行管理。

**数据交换标准：**采用基于XML的数据交换标准

* **业务数据标准**

在业务数据编码上将参照国家和上海市有关数据标准进行规范化定义，在通用编码上将参照国家标准进行规范化定义，比如地区编码、行业编码、人员基本信息等；

* **安全标准**

BG4943-1995信息技术设备（包括电气事务设备）的安全（IEC950）

BG9361-88计算机场地安全要求

GB/T9387.2-1995信息处理系统开放系统互连基本参考模型第2部分安全体系结构（ISO7498-2:1989）等国家标准。