智慧园区公共服务平台
总体规划方案

北京东正信科科技有限公司

二〇一六年十月

关于本文档

文档信息

项目名称	智慧园区公共服务平台顶层规划方案
作者	
说明	

修订历史					
版本	**范围**	**类型**	**时间**	**作者**	**备注**

目的与范围

本文档的目的仅用于项目实施使用，不得转载及提供他人使用，由此造成的法律责任完全由出让方承担。

适用的对象

本文档仅适用于甲方、相关领导及专家以及其他有关的参与者阅读。

目 录

一章 概述

1.1智慧园区介绍

智慧园区借助新一代的云计算、物联网、决策分析优化等信息技术，对现有互联网技术、传感器技术、智能信息处理等信息技术高度集成，通过监测、分析、整合以及智慧响应的方式，采取感知化、互联化、智能化的手段，将园区中分散的、各自为政的物理基础设施、信息基础设施、社会基础设施和商业基础设施连接起来，成为新一代的智慧化基础设施，从而提升为一个具有较好协同能力和调控能力的有机整体。

1.2智慧园区建设背景

在经济快速发展和政府政策的推动下，以产业聚焦为手段的园区经济发展迅速。各地园区经济呈现出覆盖区域不断扩大，产值越来越集中，GDP占比越来越大的趋势。

园区企业逐渐向高（高技术）、新（新领域）、专（专业性）行业发展。未来趋势，园区将是高新技术产业的集中研发地，高新企业群集的区域，高新产品孵化和生产的基地。

园区规划建设整体性越来越强，更加注重各种基础配套设施，以更好的服务促进高新产业的发展。尤其是注重产业园区的信息化建设，构建互联互通、资源共享的信息资源网络，以信息化带动产业化是加快产业园区发展的重要内容。

各类产业园区发展迅猛，规模扩张也越来越明显，高新企业纷纷入驻，企业对园区信息化要求越来越高，同时对园区服务和管理水平也提出了更高的要求。

第二章 指导思想及总体需求

2.1建设思想

1、统一领导，分级实施

加强组织领导，建立统一的顶层设计工作机制和制度规范，坚持统筹规划、试点先行、分级实施，逐步构建形成目标一致、方向统一、互联互通、层级衔接的智慧园区顶层设计实施体系。

2、统一建设，资源共享

坚持设施共建和资源共享，统筹利用已有园区基础设施和信息资源，统一设计建设智慧园区平台，实现基础设施和资源共享运用。

3、统一管理，保障安全

统一管理智慧园区规划、标准、制度和技术体系，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，全面提高安全保障能力。

4、统一服务，注重成效

顺应新技术发展趋势，探索运行管理服务新模式，加强智慧园区服务提供机构和服务队伍建设，建立统一的服务体系，全面提升服务能力，切实发挥智慧园区平台的成效。

2.2 建设原则

智慧园区的建设是一个系统工程，它涉及多个设计细节和执行环节，需要从园区整体的高度全盘考虑，并经历一个酝酿、启动、发展的过程。系统规划既要从时间上、发展上进行纵向的考虑，又要从各个部门协调运作的横向关系上考虑；既要考虑信息基础设施建设、软件系统的建设、安全保障系统的建设等建设项目的分步实施，又要考虑这些建设项目的协调发展，最终达到以园区各类应用和信息资源建设为基础，以公众、企业为核心，面向园区管理、园区文化建设、园区生活等多层次的信息化应用，提供综合的信息资源共享和业务协同服务，构建信息化环境。在建设的过程中的指导思想如下：

2.2.1 顶层设计的原则

站在园区全局角度，为园区人群及企业、园区管理者、经开区管理者提供一体化全生命周期服务，围绕不同服务对象重新梳理园区核心业务域的流程，实现园区各个核心业务域的管理一体化，以“全生命周期管理一体化”的思路重构园区的管理信息化建设。

顶层设计思路，站在园区宏观视角为园区系统的面向不同的业务域做全局规划，为

不同对象，不同业务不同提供全方位的贴身、个性化、智能服务。体验信息化发展带来的便捷、小管理大服务感受。

整个解决方案不是一次性全部上齐，大而全的规划并不能很好的帮助园区解决现有的问题，而是根据园区真正的业务需求节点，有计划的设计整个方案，为园区贴身打造最适合园区建设步骤的解决方案，帮助园区解决现有的问题。

2.2.2 分步实施的原则

智慧园区建设的各个环节相互关联，在建设的过程中，有计划、有步骤地实施。智慧园区建设的规划根据园区各个部门的需求和业务流程的特点，制定合理的分步实施规划。

2.2.3 协调发展的原则

智慧园区建设的各个环节相互依赖，任何一个环节的建设都离不开其它环节。因此，智慧园区建设规划将根据信息基础设施建设、信息资源建设、公共基础平台、应用系统建设、支撑体系建设等内容内在的逻辑关系，制定合理的分步实施规划，以确保各项内容的协调发展。

2.2.4 完善基础的原则

智慧园区的建设应重视网络基础平台、公共数据平台、身份管理平台、协同门户平台等智慧园区基础平台的建设，这些平台建设完成后，符合一定信息标准和技术标准的应用系统可方便地实现与智慧园区的集成。

2.2.5 突出应用的原则

应用是智慧园区的灵魂，智慧园区的魅力只有在丰富多彩的应用中才能体现出来，因此，应用系统和服务的建设是智慧园区建设的核心内容。在制定智慧园区建设规划的过程中，可选择能在短期内实现的应用系统和服务作为试点工程，组织力量重点突破，争取早日见效并带动全局。

2.2.6 实用发展的原则

智慧园区的建设规划从园区的特点和需求出发，做到够用、能用即可，切不可一味地追求大而全，也不可一味地追求技术的先进性。与此同时，智慧园区建设的技术和应用都是不断发展的，具有一定的不确定性，所以，智慧园区的建设规划必须满足建设过程中的可扩展、可兼容和可转向。

2.3智慧园区功能需求

智慧园区主要功能包括：园区门户、园区办公、园区党建、园区招商、园区金融、园区物管、领导看板、智能监控、市政管线等。

第三章 智慧园区解决方案

3.1设计原则

稳定、成熟、可靠、灵活是系统架构设计的要求，为实现这些要求，系统架构设计遵循以下原则：

1、良好的开放性，业务平台必须满足开放的技术标准，保证架构内外现有的、可能增加的不同应用模型系统可以通过开放标准很容易的进行集成。

2、高安全性，信息安全是企业的重要要求，保证信息在各个阶段的安全和受控访问，要求从网络硬件、操作系统、中间件、应用开发等各个方面的统一考虑。

3、高可靠性，保障运行在其上的各应用系统不间断持续工作，是系统架构设计的重要要求。

4、高扩展性，考虑将来逐步增加新系统时，保证系统将来的可扩展性，确保分步实施时系统的完整性，避免重复建设和资源的浪费，并保证系统能够随着未来业务的变化而非常容易的作出改变。

5、高伸缩性，随着业务应用的增加，业务量的加大，应用用户的增加，系统可以通过服务器等硬件设备的添加实现，而无需对系统逻辑架构、系统应用或业务应用进行改动，保证了这种扩展是快速的、有效的。

6、良好的管理性和可维护性，系统对不同性质用户、系统运行状态、数据资源等应具有良好的可管理性和可维护性。

7、友好性，系统界面的友好性将直接影响用户使用系统的效率。要尽可能地满足用户已有的使用习惯。

8、容错性，系统应具有很强的容错性。由于数据传输、子系统宕机等各种原因使系统无法正常处理时，系统应给出提示，但不能影响系统的正常运行。

9、可扩展性，保证系统的性能指标，系统的设计和开发不仅要满足现有用户的数量、数据存储量和响应时间的要求，而且还要为未来的发展的提供必要的扩充空间设计。

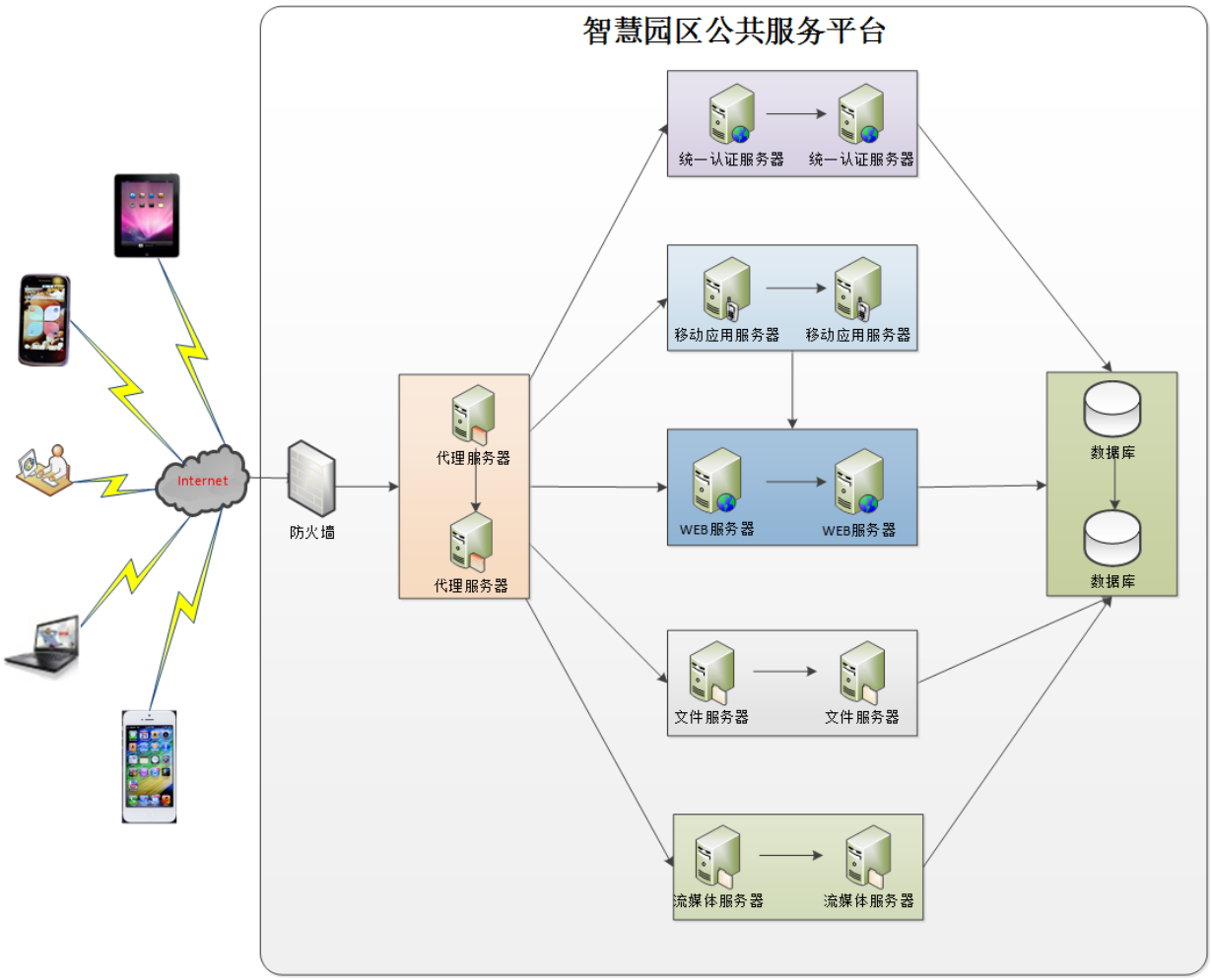
3.2 方案综述

智慧园区公共服务平台是为经开区、园区及园区的企业提供的统一的智慧化服务平台，为经开区及园区各部门提供业务和数据系统的技术承载环境、技术支撑服务、运维保障服务和安全保障服务等。

基于云服务平台，统筹使用已有的资源，形成统一管理的资源池，实现用户的按需使用，并具备良好的可扩展性。秉承“一切皆服务“的理念，将各项功能包装形成服务提供给用户，并保证快速、按需和弹性的服务，综合利用资源，向用户提供不同类型不同级别的多种服务。同时制定统一的标准及规范并提供统一的接口，第三方服务提供商按照统一标准及规范和接口开发系统应用，并部署到统一平台上，再提供给用户使用，实现服务的一体化及多元化。

建设统一的顶层系统架构，统一的系统架构是系统建设、运行、维护的依据，是系统成败的关键要素。系统架构设计是系统顶层设计的核心内容，通过将需求转化为规范的开发步骤和文档要求，制定总体的架构，指导整个项目研制活动，从而完成项目建设。

3.3 系统架构设计



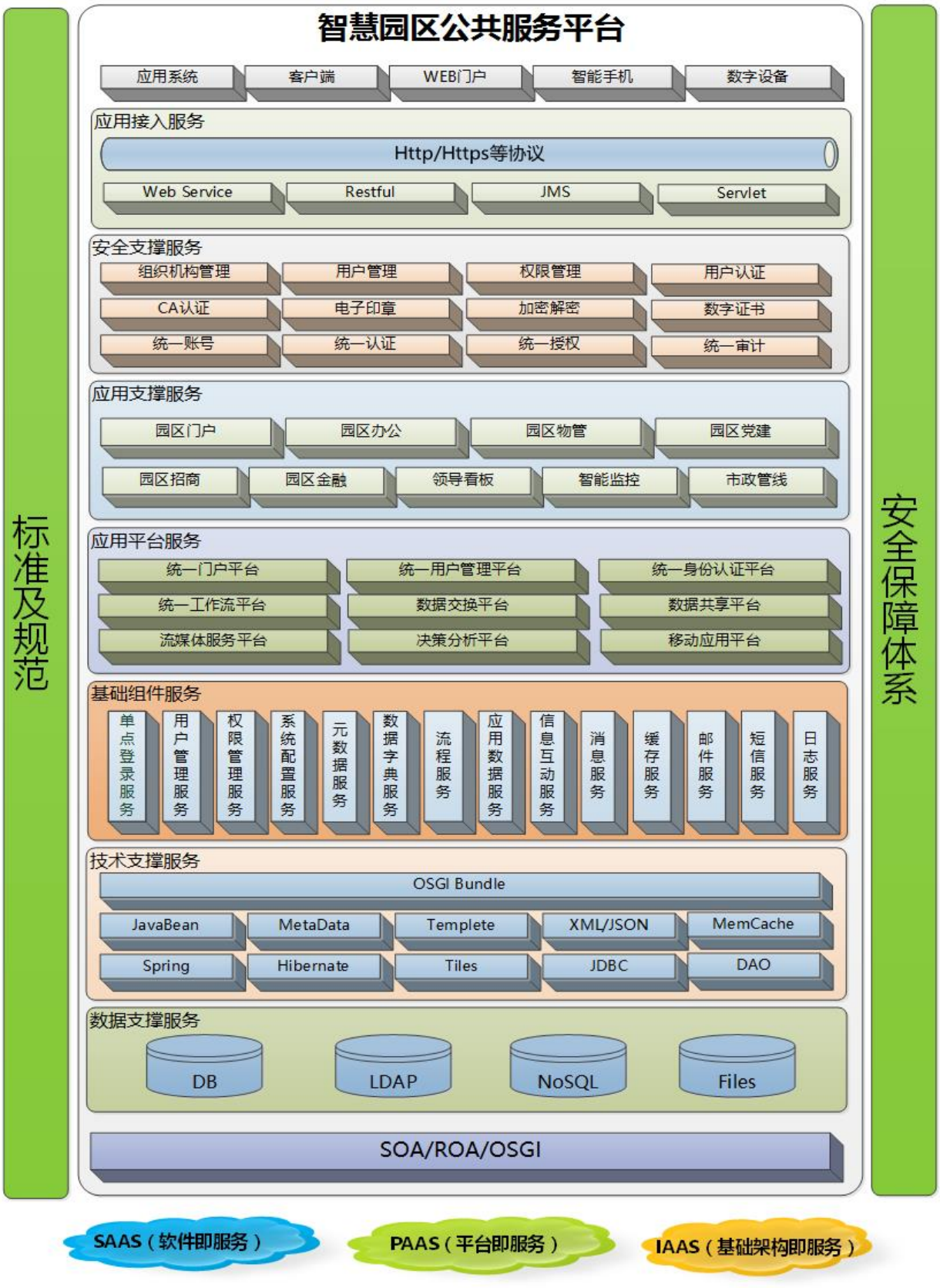
3.3.1 架构说明

1、 系统用户主要为公众、入住企业及个人、经开区管委会、园区管委会等；
2、 系统分为两大类应用，一类为 WEB 应用系统，用户通过 WEB 浏览器等访问；一类是移动办公系统，用户通过智能手机等智能设备访问；
3、 所有的访问必须通过防火墙，以保障系统安全；
4、 系统通过代理服务器访问真实系统，通过代理服务器实现负载均衡，实现缓存及压缩等处理，以提高系统性能，同时作为安全过滤器，进一步保障系统安全；
5、 应用服务器主要包含统一身份认证服务器、WEB 服务器、移动应用服务器、文件服务器、流媒体服务器等，这些服务器都可以通过双机热备的方式保证系统稳定运行；也可以部署多机，实现负载均衡，提高系统性能；
6、 统一身份认证服务器：部署统一身份认证应用，实现应用系统间的单点登录；
7、 WEB 服务器：部署 WEB 应用系统；
8、 移动应用服务器：部署移动应用服务，作为移动办公客户端与 WEB 服务器链接的中间件，实现移动应用的转换及数据处理；
9、 文件服务器：部署独立的文件服务器，实现文件存储于关系数据存储分离，提高存储效率及数据安全；
10、 流媒体服务器：对平台中涉及的流媒体及监控视频等进行统一管理，提高流媒体服务性能及质量；
11、 数据库服务器：数据库服务器独立部署，与应用系统分离，同时部署双机热备及数据库集群，以提高数据库访问性能、保障数据安全及保障系统稳定性。

3.3.2 架构特点

1、 建立统一的门户，实现信息的统一管理与整合，外网门户是对外的统一窗口；内网门户是对内的统一窗口。
2、 建立统一的数据中心，实现数据的集中存储与管理。通过数据的集中管理，实现用户数据的统一、业务数据的统一及流程数据的统一，解决数据孤岛及数据不一致的问题。
3、 通过内外网的隔离，保证数据的安全。

3.4 应用架构设计


智慧园区公共服务平台
应用系统
客户端
WEB门户
智能手机
数字设备
应用接入服务
Http/Https等协议
Web Service
Restful
JMS
Servlet
安全支撑服务
组织机构管理
用户管理
权限管理
用户认证
CA认证
电子印章
加密解密
数字证书
统一账号
统一认证
统一授权
统一审计
应用支撑服务
园区门户
园区办公
园区物管
园区党建
园区招商
园区金融
领导看板
智能监控
市政管线
应用平台服务
统一门户平台
统一用户管理平台
统一身份认证平台
统一工作流平台
数据交换平台
数据共享平台
流媒体服务平台
决策分析平台
移动应用平台
基础组件服务
单点登录服务
用户管理服务
权限管理服务
系统配置服务
元数据服务
数据字典服务
流程服务
应用数据服务
信息互动服务
消息服务
缓存服务
邮件服务
短信服务
日志服务
技术支撑服务
OSGI Bundle
JavaBean
MetaData
Templete
XML/JSON
MemCache
Spring
Hibernate
Tiles
JDBC
DAO
数据支撑服务
DB
LDAP
NoSQL
Files
SOA/ROA/OSGI
标准及规范
安全保障体系
SAAS（软件即服务）
PAAS（平台即服务）
IAAS（基础架构即服务）

3.4.1 架构说明

1、 智慧园区公共服务平台基于云架构构建，总体由表现层、接入层、安全支撑层、应用服务层、应用平台层、基础服务层、技术应用层、数据库服务层等组成。
2、 表现层支持 WEB 应用、WEB 门户、智能手机、移动终端等。
3、 系统支持 Http、Https 等协议，以满足各种终端及安全体系的需要。
4、 接入层主要实现四类系统接入，主要包括 Servlet、Web Service、Restful 以及 JMS，其中 Servlet 接收来自 WEB 应用的请求；Web Service 接收基于 SOAP 协议的 WEB 服务请求；Restful 则接收基于 Http 协议的 WEB 服务请求；JMS 接收消息类的数据。
5、 安全支撑层对组织机构及用户实现统一管理，通过单点登录实现应用系统的整合；单点登录以统一用户管理为基础，实现严格的 4A 管理。
6、 应用服务层以系统或应用模块的方式提供给用户使用，同时也可以以服务的方式为其他系统或应用提供支持。应用服务层主要以 bundle 的方式进行设计与开发，实现真正的组件化。
7、 应用平台层提供统一的基础应用平台，包括统一门户平台、统一用户管理平台、统一身份认证平台、统一工作流平台、数据交换与共享平台、流媒体服务平台及移动应用平台等。
8、 基础服务层为应用服务层提供底层技术及服务支持，实现基本应用及核心功能。主要包含等单点登录服务、用户管理服务、权限管理服务、系统配置服务、元数据服务、数据字典服务、流程服务、应用数据服务、信息互动服务、消息服务、缓存服务、邮件服务、短信服务、日志服务等。
9、 技术支持层主要是系统应用的实现技术，主要使用 Spring、Tiles、DAO、JDBC、DAO、JavaBean、Metadata、Templete、XML、JSON、Memcache 等成熟稳定的技术。
10、 数据库服务层提供数据库应用服务，实现对数据库的操作，保证事务的原子性、一致性、隔离性和持久性。数据库不仅仅是关系型数据库，也支持文档类数据库、非关系型数据库及 LDAP 等。
11、 应用架构遵循 SOA、ROA 架构技术规范及要求，完全基于 OSGI 技术规范构建系统，实现组件化设计与开发。

3.4.2 架构特点

1、 应用架构采用先进的开源框架，包括 Spring3、Tiles3、DAO、CAS 等，保障了系统的稳定性。
2、 应用系统完全基于元数据进行设计与开发，系统中使用到的所有数据以及表单等都通过元数据进行描述及操作，使系统具有很强的扩展能力。
3、 应用系统基于模板进行设计与开发，系统提供四类模板，包括编辑模板、查询模板、列表模板及查看模板，通过这四类模板快速组合应用，模板由元数据进行解释，提供了很好的扩展行及快速开发能力。
4、 应用系统提供元数据配置、模板配置、数据字典配置、系统配置、日志配置、功能菜单配置、权限配置等自定义配置功能，极大的提高了系统的可配置性及扩展性。
5、 应用系统基于 OSGI 架构进行构建，是真正实现组件化开发及管理的平台，通过 OSGI 架构能够轻松管理组件，实现组件的版本管理，以及快速部署等。
6、 应用系统支持及采用 Restful 技术，能够快速实现及整合 ROA 架构。
7、 应用系统支持及采用 Web Service 技术，能够快速实现及整合 SOA 架构。
8、 应用系统结合移动应用平台实现对智能客户端的支持，如对 Andriod、IOS 等移动平台的支持。

3.5 应用平台设计

3.5.1 统一门户平台

智慧园区在各政府部门的信息化建设基础上,需要建立起跨部门的、综合的业务应用系统,使公民、企业与政府工作人员都能快速便捷地接入所有相关政府部门的业务应用、组织内容与信息,并获得个性化的服务,使合适的人能够在恰当的时间获得恰当的服务。这就要求建设统一的智慧园区门户网站。

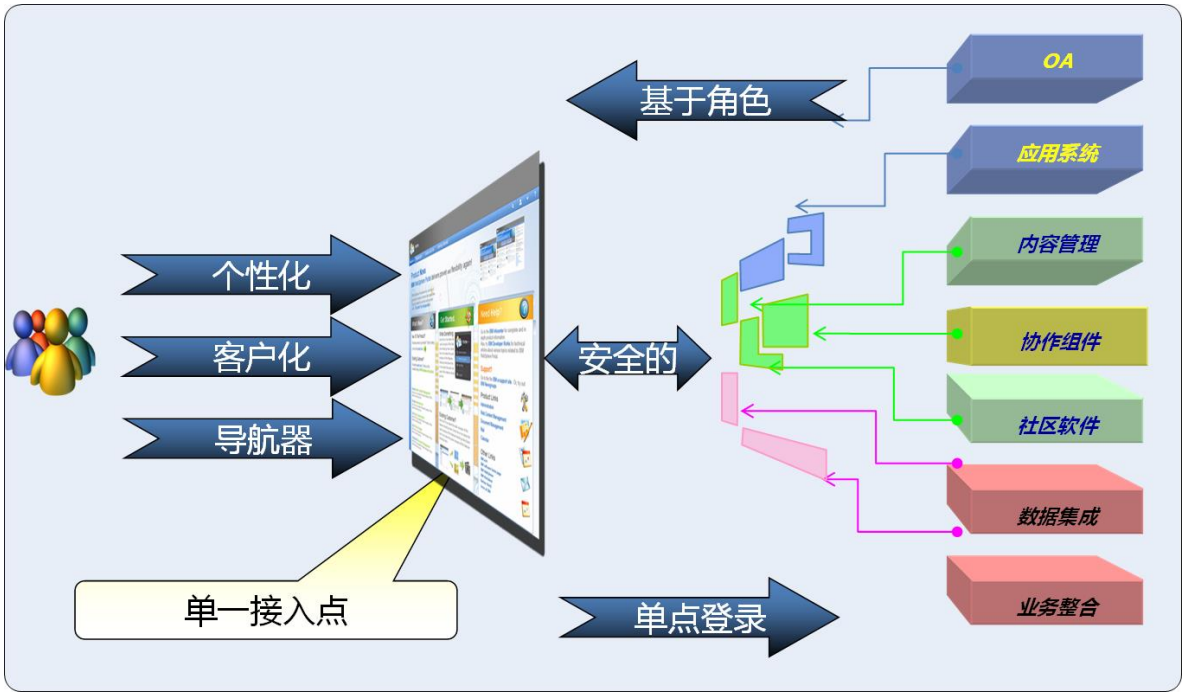
智慧园区门户网站不仅是政务信息发布平台和业务处理平台,而且也是知识加工平台、知识决策平台、知识获取平台的集成,它使政府各部门办公人员之间的信息共享和交流更加流畅,通过数据挖掘、数据加工而使零散的信息成为知识,使相关人员能够在恰当的时间使用恰当的知识,为行政决策提供充分的信息和知识支持。

智慧园区门户网站分为外网门户平台、内网门户平台、移动门户平台及微信公众平台。

园区外网门户是园区的门面，承担着园区形象的介绍及推广作用。另外，园区不但要考虑建设好园区的对外门户网站，还要考虑与其他的关系，搭建门户，以整个园区网站群的管理和控制模式进行建设。外网门户体现统一形象、统一风格，需要对网站群实现统一管理、统一技术平台、统一内容审核发布流程等功能。

园区内网门户为园区及其他机构统一办公的门户平台，为工作人员提供单一访问点，供他们访问园区工作中的各种信息和服务。内网门户不仅提供集成的内容和应用，而且还是园区一体化的协作工作空间。

移动门户平台与微信公众平台是外网门户与内网门户的延伸，公众、政府部门及其他相关人员通过移动门户及微信获取信息并进行处理的快捷通道。



3.5.2 统一用户管理平台

统一用户管理平台集中统一管理所有应用系统的用户，消除用户信息孤岛，形成统一的用户数据中心。统一用户管理平台所有应用系统标准化的用户管理基础设施，包括用户帐号的统一管理、用户属性的统一管理以及用户整个生命周期的管理，并为各个应用系统提供安全的服务与支持，为 SSO 打下坚实的基础。

1、统一帐号管理

统一用户管理平台的核心功能之一是将用户的身份与用户在各个应用系统的帐号进行关联。该帐号的关联是通过用户标识来建立的，即通过用户在各个系统的属性关键项来实现关联。

2、统一属性管理

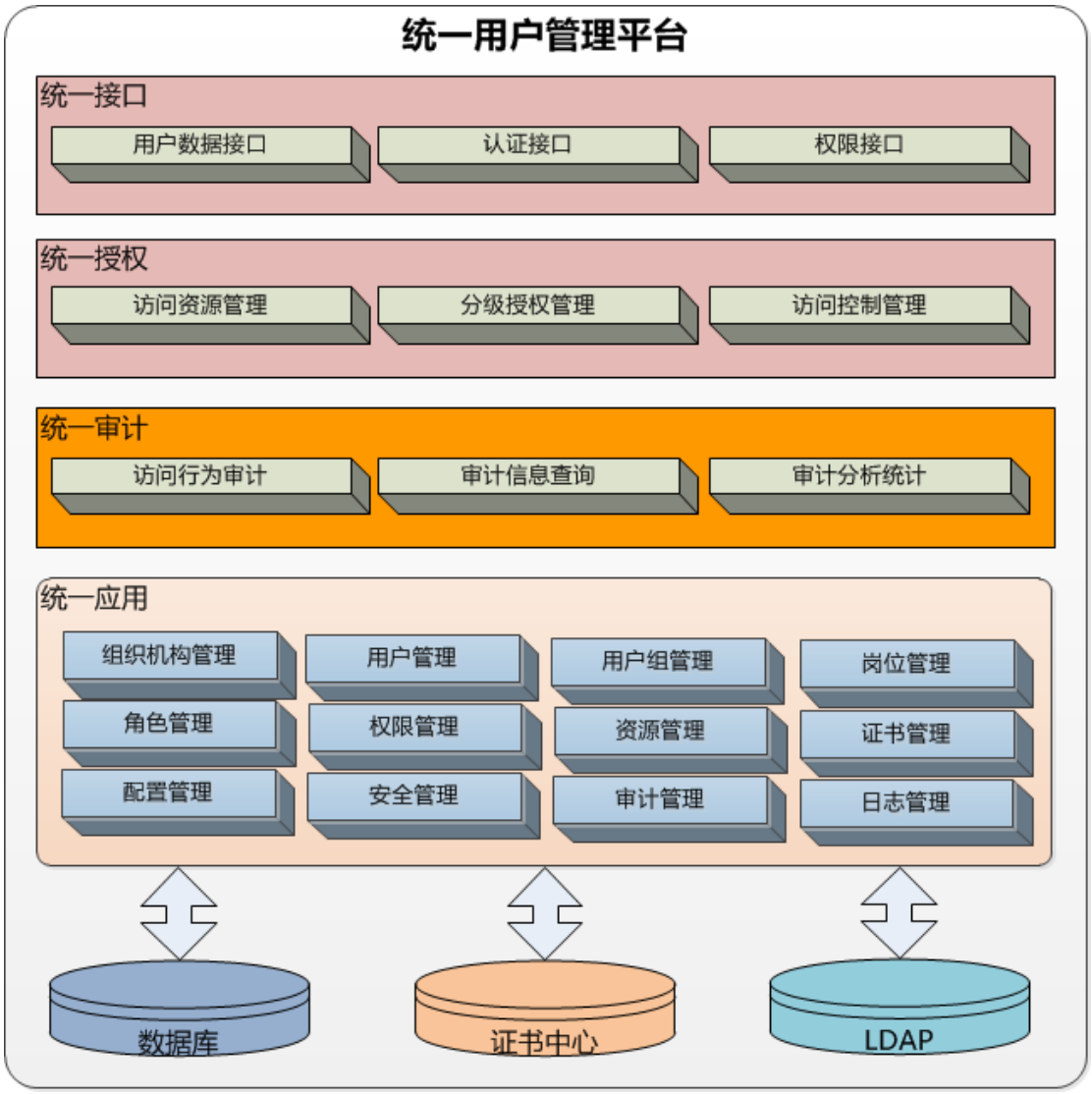
统一用户管理平台的属性管理功能，即元数据的管理功能支持 TopDown 和 Matrix 模式。TopDown 使各个应用系统都以统一用户管理系统为数据源。Matrix 模式使各个应用系统都成为属性的数据源，且每个属性项只能以一个系统的属性数据为来源。

3、用户生命周期管理

统一用户管理平台的另外一个重要功能是实现了对园区应用用户（包括教师、学生、领导等）的整个生命周期管理，实行对所有用户身份的创建、修改、删除等操作的统一

管理。

3.5.2.1 平台架构



3.5.2.2 平台特点

1、 实现用户数据的统一集中管理，建立统一用户中心，对用户管理我们实现了严格的 4A 管理，即统一认证 Authentication、统一账号 Account、统一授权 Authorization、统一审计 Audit

2、 提供统一的用户数据接口，实现应用系统间的用户数据的同步与集中管理

3、 提供统一的认证接口，为单点登录提供多种方式的认证功能

4、 提供统一的权限管理及权限接口，实现分级授权及访问控制管理

5、 对所有的用户信息及认证信息、操作信息等进行统一审计管理

6、 提供统一的组织机构管理，以及基于组织机构个岗位管理

7、 提供对用户全生命周期的管理及分组管理

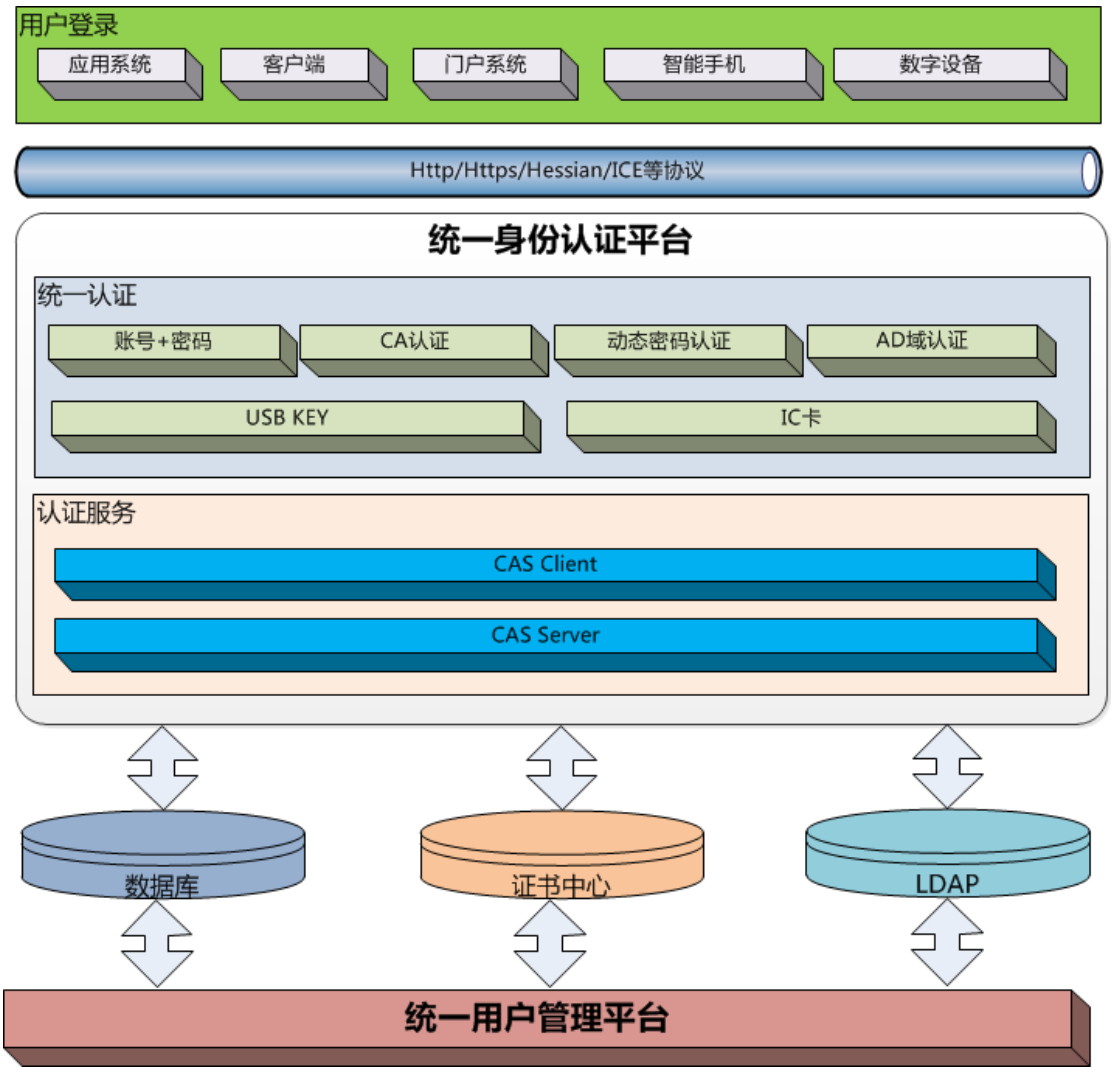
8、 提供基于 RBAC 模型的权限管理体系，支持分级授权管理

3.5.3 统一身份认证平台

统一身份认证平台，作为网络应用的授权和访问控制中心，实施由用户到应用的安全管理。它通过提供统一的认证体系，实现各应用系统的“集中认证“，规范用户操作行为，强化用户合理使用网络资源的意识。系统采用单点登录技术，用户通过一次认证后，即可获得相应权限，并使用所有授权的应用服务系统提供的服务。

统一身份认证平台主要包含两部分功能，一部分是统一认证方式，包括账号+密码、动态密码、CA 认证、AD 域认证、USB KEY 认证、IC 卡认证等多种方式；另一部分功能即单点登录功能，通过单点登录，实现用户一次登录，多系统应用的要求，同时对用户的认证及授权也进行了严格的控制。

3.5.3.1 平台架构



3.5.3.2 平台特点

1、实现了基于 CAS 架构的单点登录系统，用户基于 CAS Client 可快速接入，实现与 CAS Server 的连通及认证

2、提供多种接口方式，方便应用系统的接入，CAS Client 支持非常多的客户端(这里指单点登录系统中的各个 Web 应用)，包括 Java, .Net, PHP, Perl, Apache, uPortal, Ruby 等

3、支持 HTTP、HTTPS 等协议，同时提供了 Proxy （代理）模式，以适应更加高级、复杂的应用场景

4、面向接口的架构模式，可以快速实现其他系统的用户及组织机构体系整合

5、可以快速与其他统一身份认证系统进行整合

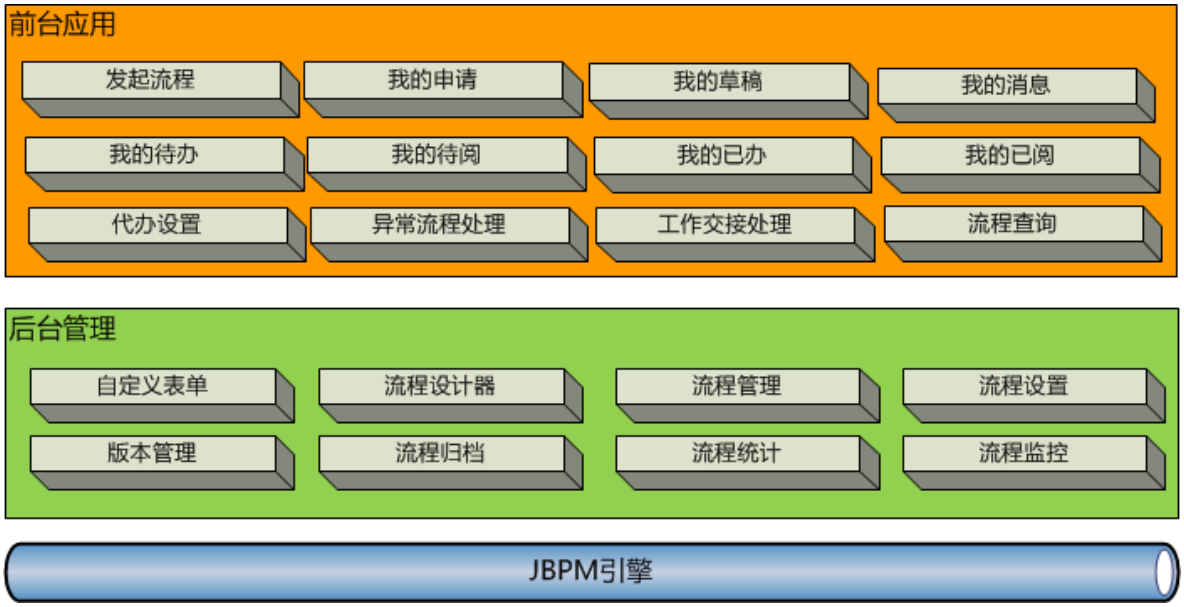
3.5.4 统一工作流平台

工作流平台即以工作流为核心，实现流程设计、流程执行、流程监控、流程统计等功能，其中流程设计完全实现可视化设计，并提供丰富的参数设置功能。表单是流程的核心，平台提供自定义表单功能，可以定制与原始表单几乎一致的表单，并实现数据的统一存储及管理。

工作流(Workflow)，就是“业务过程的部分或整体在计算机应用环境下的自动化”，它主要解决的是“使在多个参与者之间按照某种预定义的规则传递文档、信息或任务的过程自动进行，从而实现某个预期的业务目标，或者促使此目标的实现”。

工作流平台即以工作流为核心，实现流程设计、流程执行、流程监控、流程统计等功能，其中流程设计完全实现可视化设计，并提供丰富的参数设置功能。表单是流程的核心，平台提供自定义表单功能，可以定制与原始表单几乎一致的表单，并实现数据的统一存储及管理。

3.5.4.1 平台架构



工作流平台即以工作流为核心，实现流程设计、流程执行、流程监控、流程统计等功能，其中流程设计完全实现可视化设计，并提供丰富的参数设置功能。表单是流程的核

心，平台提供自定义表单功能，可以定制与原始表单几乎一致的表单，并实现数据的统一存储及管理。

3.5.4.2 平台特点

1、提供 WEB 下的自定义表单功能，能够快速定义单一表单、主子表单等多种表单

2、表单提供表单样式在线编辑及自定义功能，支持定义数据显示格式、自动合计等功能

3、表单支持 JavaScript 脚本的嵌入，提供常用的 JavaScript 方法库

4、表单数据初始以 JSON 格式存储，可以灵活的转换成关系型数据存储到数据库中，支持自动转存；同时可以方便的提供给其他应用系统或组件使用

5、提供 WEB 下自定义流程的设计，可视化的流程设计，快速定义常用的流程

6、支持流程任务节点、路由、策略节点、并行节点、子流程等多种流程元素，并提供丰富的自定义配置

7、在流程流转过程中提供加签、转办、督办、设定待办人等功能

8、流程管理员全面监控流程运行情况，对无法流转的流程提供替换办理人、流程跳转等功能，并能够随时暂停、启用流程，保障流程的正确运行

9、提供多种通知方式，如站内消息、电子邮件、即时通讯、手机短信等

10、提供完整的二次开发接口，快速实现与其他系统的对接

11、支持跨系统流程审批，快速实现与其他应用系统的整合

12、提供对流程数据及表单数据强大的统计分析功能

3.5.5 移动应用平台

随着科技水平的快速提高，科技应用范围的不断扩大，经济发展的迅猛增长，工作生活的节奏随之也日益加快，人们经常在外工作，在工作中希望能够随时、随地、随身获取信息或了解与自己相关的业务及处理情况。传统有线网络支持下的信息化系统无法提供这种即时支持，使信息化链条断裂，造成很多紧急事务无法得到及时处理，从而出现信息或工作延迟的情况，降低了整体效率。因此，有必要建设移动应用系统来完善这一重要环节，使信息沟通迅速有效，使信息系统发挥更大价值。

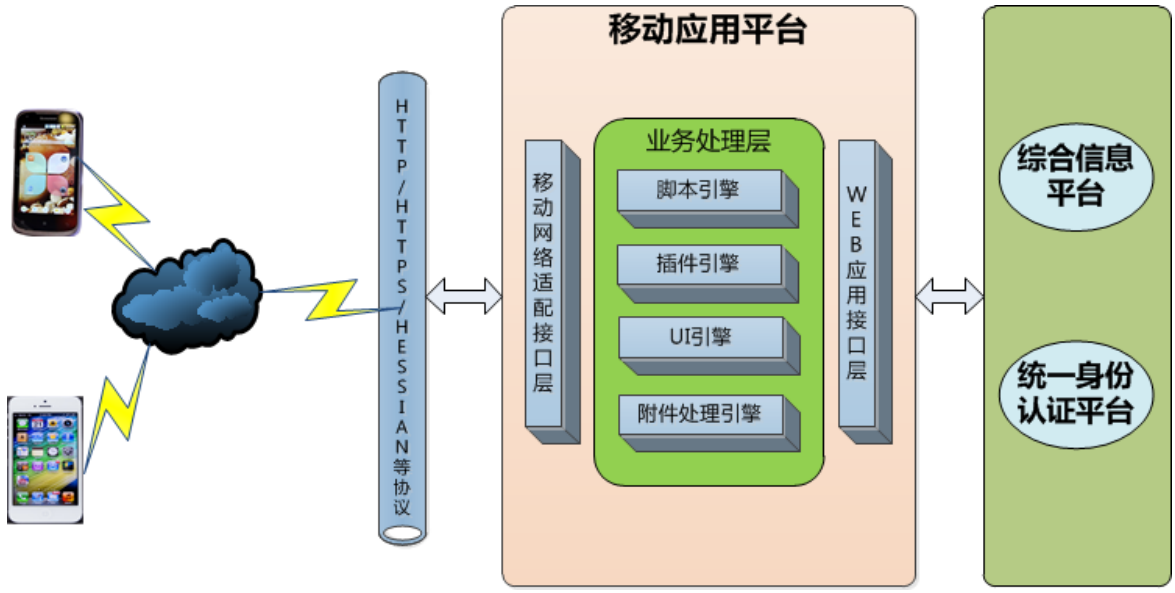
移动应用服务就是利用移动设备（例如笔记本计算机、手机、PDA 等），实现信息移

动化的全新方式，提高了信息利用率，极大的提高了信息的时效性，它是移动通信、PC电脑与互联网三者融合的信息化成果。

微信作为另外一种移动应用的延伸，已经成为人们的一种生活方式，被越来越多的人所接受与使用，智慧园区也需要建设自己的微信公众平台，提供给用户更多的获取信息的渠道及方式。

移动应用平台则是移动应用服务及微信公众服务的平台保证，移动应用平台为移动应用服务及微信公众服务提供安全认证、信息查阅、流程审批、消息推送及提醒、收发邮件等功能，支持对 office、PDF、TXT、JPG 等多种格式文件的读取功能，提供终端绑定、黑白名单管理、严格的权限管理等功能，保障用户数据及系统的安全。

3.5.5.1 平台架构



3.5.5.2 平台特点

1、基于 W3C 标准，与 IOS 和 Android 原生开发技术相结合，实现移动应用操作

2、完全采用 HTML5+CSS3 技术，轻松实现跨平台应用

3、通过多种类型的接口，快速实现与应用系统的整合及功能定制

4、支持苹果 IOS、Android 等平台自动适配分辨率

5、支持版本更新，自动生成差异资源文件

6、组件化的应用管理，实现应用组件的自由组合

7、实现严格是授权管理，支持黑白名单管理

8、提供功能完善的设备管理，包括设备绑定，设备启停等功能

3.6 安全支撑服务

安全支撑服务实现应用系统间的单点登录及安全保护，为系统及平台的安全提供统一的安全防护功能。系统提供强大且功能完善的单点登录功能，实现严格的 4A 认证，即统一账号、统一认证、统一授权、统一审计；平台提供统一的组织机构管理、用户管理、权限管理及用户认证管理，同时提供多种安全方式，如用户名+密码、CA 认证、数字证书、电子印章及加密解密等。

3.6.1 统一组织机构与用户

为了减少各应用系统数据资源重复存储，方便各应用系统对用户、组织机构的使用，保证用户、组织机构数据的安全、真实、唯一，智慧园区云平台需要构建一个对组织机构、用户信息统一管理和数据共享的平台。

组织机构与用户管理同时应包括对组织机构信息和用户信息的管理。组织机构是应用系统建设的基础，是个应用系统的业务核心数据来源之一。组织机构模型应该支持直线型、矩阵式等多种组织机构管理方式。组织机构与用户管理应提供如下功能：

1、支持直线制、职能制、直线－职能制、矩阵制等组织结构模式。允许用户根据自身战略制订适合自己业务需要的组织结构模式；支持虚拟组织和团队；

2、支持多层级的分级用户管理，支持多级子管理员，子管理员能够完全管理本级用户；

3、提供用户全生命周期的管理，完成用户从创建一直到注销的整个过程的管理，主要实现以下功能：实现用户账户的全面管理，包括创建、修改、检查、删除等；建立组织架构和用户的全局视图；

4、提供组织机构事件记录功能，对于部门的设立、撤销，员工的入职、升职等提供完备的组织机构事件记录；

5、支持从不同的维度对组织结构进行观测，如从人力资源层面、计划、考核等视角进行切分；

6、支持组织结构组件的分布式部署和基于 LDAP V3 国际标准的组织核心级数据共享；

7、提供批量用户信息的导入、导出功能。

3.6.2 统一身份认证及单点登录

统一身份认证平台是为各个渠道接入公共平台提供统一的认证入口，并在此基础上提供公共平台的单点登录功能，主要目标有：

1、提升用户感知：

（1）通过统一的用户身份、认证信息管理、统一的认证方式、单点登录只需要登录一次就可以访问所有相互信任的应用系统，便捷用户对门户和业务平台的使用，提升用户使用感知；

（2）通过对更高安全级别要求的认证方式的支持，提升用户的安全感知。

2、优化 IT 架构，实现可持续发展

（1）构建数据共享、集中管理、统一认证、安全高效的认证体系，实现用户认证的“专业化、平台化、标准化“；

（2）解决各个门户系统、业务平台分散认证导致的功能重复建设、认证信息和认证处理逻辑不一致、不完整等诸多问题，同时为其他业务系统的接入降低成本；

（3）建立灵活可扩展的 IT 技术架构，适应现有的和将来可能出现的不同类型、不同规模的业务系统的接入。

3.6.2.1 统一身份认证

统一身份认证主要实现如下功能：

1、支持基于传统关系数据库的认证、基于 LDAP 的身份认证，支持单点登录（SSO），支持数字证书；

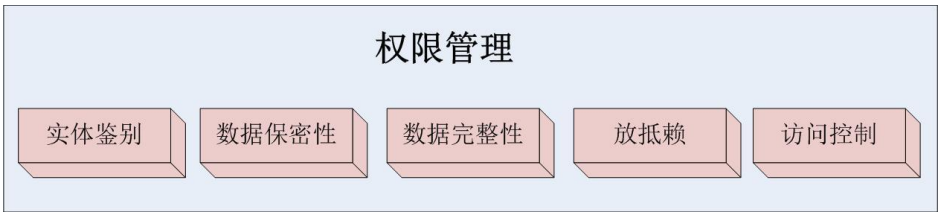
2、支持数字签名和消息摘要；

3、提供功能强大的审计功能，捕获安全性相关事件记录的操作，预防和追究非法操作；

4、集中授权：对用户访问和使用相关产品及系统资源的权限进行鉴定，并赋予相应的权限

5、统一权限规范

6、根据 ISO7498-2 的定义，一个完整的权限安全管理必须提供如下服务：实体鉴别（Entity Authentication）、数据保密性（Data Confidentiality）、数据完整性（Data Integrity）、防抵赖（Non-repudiation）和访问控制（Access Control）。



权限管理服务构成图

7、权限安全管理要直观而且灵活，提供细粒度的权限管理。实现用户、角色、权限的统一管理，并实现操作上的分级管理。一般情况下用户同角色关联，角色同权限关联，同时也要提供良好的灵活性，支持用户直接与权限关联。

8、支持 MD5/SHA 等传统的加密算法，可根据自身安全需要灵活扩展自己的加密算法；

9、支持角色访问控制（RBAC）模式，同时支持按用户授权和按角色授权两种模式；

10、提供统一的权限管理规范，同时支持多种粒度的权限管理，既要支持集中管理系统级粗粒度权限，也要支持对各业务系统功能、操作和数据级的细粒度权限管理；

11、在制定统一安全策略的前提下实行分级授权，不同级别的组织机构可以各自设立管理员，在总授权范围内灵活设定角色和用户安全策略；

12、加强信息安全，实现信息保密性和用户行为的不可抵赖性；

13、提供在线用户监控和安全日志监控等权限审计功能，捕获安全性相关事件记录的操作，允许管理员实时跟踪和分析在线用户的行为动向以利于发现系统中可能存在的问题，预防和追究非法操作。

14、支持国际信息技术标准委员会制定的 RBAC 96 标准和安全管理学界流行的自主访问控制标准。

3.6.2.2 单点登录

单点登录主要实现如下功能：

1、建立统一认证体系，提供对所有新建应用系统和有条件进行改造的原有系统在用户认证方面的统一管理，实现认证方式的统一；

2、支持标准化单点登录，能够支持跨 DNS 域单点登录；

3、支持 B/S、C/S 等框架下单点登录，并支持与第三方 CA 集成实现统一认证、单点登录；

4、既要支持所有业务系统使用一套相同用户数据的用户数据统一方式，也要支持遗留系统通过关联映射关系实现的用户数据统一方式；

5、支持用户名/口令、数字证书单独或组合使用方式的用户登录，并支持验证码；

6、支持基于传统关系数据库的认证、基于 LDAP 的身份认证，支持 CA 认证；

7、支持登录次数、密码策略、IP 策略等多种安全策略来增强用户登录的安全性。

3.6.3 电子印章与电子认证

智慧园区云平台所涵盖各业务系统都有需要处理的敏感数据，例如事项申报、各业务系统的业务流程上的审核、批复、签字环节等，为保证数据的安全、真实、高效，需要提供电子印章与电子认证服务。

智慧园区云平台对电子印章与电子认证产品进行封装与整合，统一对外提供服务，

具体功能需求如下：

1、电子签章与电子认证服务应该符合《中华人民共和国电子签名法》中规定的电子签名规范。

2、电子印章与电子认证服务应该达到国家信息安全技术标准：GB/T18336-2001《信息技术 安全技术 信息技术安全性评估准则》和 GB/T17903-1999《信息技术安全技术 抗抵赖》。

3、公章文件及签名认证文件要加密存储，只有得到公章管理员的授权方可使用公章。

4、公文盖章或签字后，不允许修改。

5、印章及签名应该具备防复制、防拷贝、防篡改等功能。

6、公文的存储和传输都经过加密。

7、用户可以验证公章及签名文件的真假（包括本地验证、在线验证）。

8、只有合法用户可以阅读公文。

9、签章信息的验证。比如：签章时间、签章人、印章信息等。

10、电子认证要确保信息的真实性、完整性、机密性、不可否认性。