**我的长沙APP-长沙高新区一期**

**需求规格说明书**

二〇二一年七月

**目 录**

[1 引言 1](#_Toc88206722)

[1.1 编写目的 1](#_Toc88206723)

[1.2 软件需求分析理论 1](#_Toc88206724)

[1.3 应遵循的标准和规范 1](#_Toc88206725)

[1.4 采用技术 2](#_Toc88206726)

[1.4.1 JavaEE技术 2](#_Toc88206727)

[1.4.2 HTML5技术 3](#_Toc88206728)

[1.4.3 MVC架构技术 5](#_Toc88206729)

[1.4.4 面向服务的架构（SOA） 6](#_Toc88206730)

[1.4.5 NativeApp技术 6](#_Toc88206731)

[1.4.6 OAuth2.0技术 10](#_Toc88206732)

[1.4.7 CAS单点登录技术 12](#_Toc88206733)

[1.4.8 云端融合服务技术 17](#_Toc88206734)

[1.4.9 移动互联网技术 18](#_Toc88206735)

[1.4.10 中间件技术 21](#_Toc88206736)

[1.4.11 负载均衡技术 22](#_Toc88206737)

[1.4.12 数据序列化技术 22](#_Toc88206738)

[1.4.13 缓存技术 23](#_Toc88206739)

[2 项目描述 24](#_Toc88206740)

[2.1项目名称 24](#_Toc88206741)

[2.2项目背景 24](#_Toc88206742)

[2.3建设依据 25](#_Toc88206743)

[2.4项目目标 25](#_Toc88206744)

[2.4.1 建设目标及内容 25](#_Toc88206745)

[2.4.2 运营目标及内容 26](#_Toc88206746)

[2.5建设模式 27](#_Toc88206747)

[2.6建设必要性及意义 27](#_Toc88206748)

[2.6.1贯彻政策要求，配合建设城市移动端综合服务平台 27](#_Toc88206749)

[2.6.2落实规划建设任务，推进新型智慧城市建设 27](#_Toc88206750)

[2.6.3共享“互联网+城市服务”成果，提升政府服务效能 28](#_Toc88206751)

[2.6.4推进信息化建设科学投资，减少重复建设问题 28](#_Toc88206752)

[2.7预期效益 28](#_Toc88206753)

[2.7假定和约束 30](#_Toc88206754)

[2.7.1建设规模 30](#_Toc88206755)

[2.7.2项目建设期 30](#_Toc88206756)

[3 系统功能需求 30](#_Toc88206757)

[3.1建设方案 30](#_Toc88206758)

[3.1.1基础平台支撑 30](#_Toc88206759)

[3.1.2 UI设计 34](#_Toc88206765)

[3.1.2.1原型设计 34](#_Toc88206768)

[3.1.2.2UI设计 35](#_Toc88206769)

[3.1.3门户首服务 35](#_Toc88206770)

[3.1.4高新区特色专区建设 40](#_Toc88206771)

[3.2运维服务 47](#_Toc88206773)

[3.2.1响应处理 48](#_Toc88206774)

[3.2.2服务完善 48](#_Toc88206775)

[3.2.3性能提升 48](#_Toc88206776)

[3.2.4服务故障检测 49](#_Toc88206777)

[3.2.5故障受理处理 49](#_Toc88206778)

[3.2.6应急措施 49](#_Toc88206779)

[2 非功能性需求 50](#_Toc88206780)

[2.1 性能需求 50](#_Toc88206781)

[2.1.1 系统稳定指标 52](#_Toc88206782)

[2.1.2 性能及资源指标 52](#_Toc88206783)

[2.1.3 灵活性 54](#_Toc88206784)

[2.1.4 精度 54](#_Toc88206785)

[2.2 安全保障体系需求 54](#_Toc88206786)

[2.2.1 隐私保护设计 54](#_Toc88206787)

[2.2.2 安全设计目标 57](#_Toc88206788)

[2.2.3 安全风险分析 58](#_Toc88206789)

[2.2.4 安全管理保障 60](#_Toc88206790)

[2.2.5 安全技术方案 61](#_Toc88206791)

[2.3 用户界面需求 74](#_Toc88206792)

[2.3.1 GUI设计的规范 75](#_Toc88206793)

[2.3.2 GUI布局的合理性 75](#_Toc88206794)

[2.3.3 GUI风格的一致性 76](#_Toc88206795)

[2.4 软硬件环境需求 78](#_Toc88206796)

[2.4.1 硬件技术需求 78](#_Toc88206797)

[2.4.2 软件技术需求 82](#_Toc88206798)

[2.4.3 移动端运行环境需求 84](#_Toc88206799)

[2.5 扩展性需求 84](#_Toc88206800)

[2.5.1 应用中台需求表 85](#_Toc88206801)

[2.5.2 统一支付能力需求 86](#_Toc88206802)

[2.5.3 统一身份认证能力需求 88](#_Toc88206803)

[2.5.4 统一物流能力需求 88](#_Toc88206804)

[2.5.5 数据中台需求表 88](#_Toc88206805)

[2.5.6 AI中台需求表 89](#_Toc88206806)

[2.6 可维护性需求 91](#_Toc88206807)

# 引言

## 编写目的

为明确软件需求、安排项目规划与进度、组织软件开发与测试，撰写本文档。

## 软件需求分析理论

软件需求分析（Software Reguirement Analysis）是研究用户需求得到的东西，完全理解用户对软件需求的完整功能，确认用户软件功能需求，建立可确认的、可验证的一个基本依据。

软件需求分析是一个项目的开端，也是项目实施最重要的关键点。据有关的机构分析结果表明，设计的软件产品存在不完整性、不正确性等问题80％以上是需求分析错误所导致的，而且由于需求分析错误造成根本性的功能问题尤为突出。因此，一个项目的成功软件需求分析是关键的一步。

## 应遵循的标准和规范

GB/T 9385-2008：计算机软件需求规格说明规范

GB/T 9386-2008：计算机软件测试文档编制规范

GB/T 14394-2008：计算机软件可靠性和可维护性管理

GB/T 15532-2008：计算机软件测试规范

GB/T 8566-2007：信息技术 软件生存周期过程

GB/T 8567-2006：计算机软件文档编制规范

GB/T 11457-2006：信息技术 软件工程术语

GB/T 18221-2000：信息技术 程序设计语言、环境与系统软件接口 独立于语言的数据类型

GB/T 18491.1-2001：信息技术 软件测量 功能规模测量 第1部分：概念定义

GB/T 18491.2-2010：信息技术 软件测量 功能规模测量 第2部分：软件规模测量方法与GB/T 18491.1-2001的符合性评价

GB/T 18491.3-2010：信息技术　软件测量　功能规模测量　第3部分：功能规模测量方法的验证

GB/T 18491.4-2010：信息技术 软件测量 功能规模测量 第4部分：基准模型

GB/T 18491.5-2010：信息技术 软件测量 功能规模测量 第5部分：功能规模测量的功能域确定

GB/T 18491.6-2010：信息技术 软件测量 功能规模测量 第6部分：GB/T 18491系列标准和相关标准的使用指南

GB/T 18492-2001：信息技术 系统及软件完整性级别

GB/Z 18493-2001：信息技术 软件生存周期过程指南

GB/T 18905.1-2002：软件工程 产品评价 第1部分: 概述

GB/T 18905.2-2002：软件工程 产品评价 第2部分: 策划和管理

GB/T 18905.3-2002：软件工程 产品评价 第3部分: 开发者用的过程

GB/T 18905.4-2002：软件工程 产品评价 第4部分: 需方用的过程

GB/T 18905.5-2002：软件工程 产品评价 第5部分: 评价者用的过程

GB/T 18905.6-2002：软件工程 产品评价 第6部分: 评价模块的文档编制

GB/T 19003-2008：软件工程 GB/T19001-2000应用于计算机软件的指南

GB/Z 20156-2006：软件工程 软件生存周期过程 用于项目管理的指南

GB/T 20158-2006：信息技术 软件生存周期过程 配置管理

GB/T 20917-2007：软件工程 软件测量过程

GB/T 20918-2007：信息技术 软件生存周期过程 风险管理

## 采用技术

我的长沙—高新区城市移动综合服务平台移动应用开发平台基于采购的系统软件“移动应用框架软件”的功能基础上进行二次开发，实现安卓版本、iOS版本的统一管理和开发建设。主要使用了以下核心技术。

### JavaEE技术

为了保证系统的高可用性、高可靠性和可扩展性，系统必须要选择支持强大的企业级计算的成熟的技术路线。当前能够满足这些条件的计算平台首推JavaEE的企业标准。

JavaEE是主流的技术体系，JavaEE已成为一个工业标准，围绕着JavaEE有众多的厂家和产品，其中不乏优秀的软件产品，合理集成以JavaEE为标准的软件产品构建信息集成平台，可以得到较好的稳定性、高可靠性和扩展性。JavaEE技术的基础是JAVA语言，JAVA语言的与平台无关性，保证了基于JavaEE平台开发的应用系统和支撑环境可以跨平台运行。

JavaEE平台技术主要包括组件技术、服务技术、通信技术。

组件技术：由开发人员用来创建企业应用程序的主要部分，即用户界面和业务逻辑。JavaEE规范定义了以下组件：



JavaEE规范组件图

服务技术：支持提供对数据库访问、事务服务和JNDI服务的访问权的API。服务技术主要包括：数据库访问(JDBC)、Java命名与目录接口(JNDI)、事务服务、JTA(Java事务API)、JTS(Java事务服务)。

通信技术：提供在客户端与服务器之间以及不同服务器托管的协作对象之间进行通信的机制。通信技术主要包括：HTTP(S)、RMI(远程方法调用)、OMG(对象管理组协议)、JMS(Java消息服务)、JavaMail(Java电子邮件)、连接器架构。

### HTML5技术

移动应用框架整体而言，主要为满足快速开发、低成本包装的需求，开发者挑选需要的插件进行组合形成应用半成品，在半成品的基础上增加业务或体现应用特色的代码，形成最终的应用。而框架所提供的IDE或IDE插件支持将加快应用搭建速度、开发速度和编译速度。

移动应用开发框架将关注如下几个重点：

（1) 轻量。移动应用被部署于移动设备后，将适应移动设备所处的多种网络环境，甚至需要通过网络加载诸如css、js等类型的资源文件。而在移动环境中，过度的资源加载不论对用户资费还是设备续航能力而言都是不利的。因此，移动应用框架应尽可能的做到简练、突出核心，高度压缩。

（2) 兼容。移动应用开发框架为满足应用跨平台的需求，应充分考虑移动终端碎片化的特征。移动终端除操作系统的差异，还存在屏幕尺寸和浏览器的差异。可行的方案之一是为不同的浏览器或尺寸准备不同的资源文件由移动设备按需加载。

（3) 多传感器应用。移动设备虽然搭载不同的操作系统，但大部分的传感器已成为设备标配，例如：加速度计、重力感应、陀螺仪、磁力计等。充分利用传感器，发挥移动设备的输入输出能力，可以简化移动应用上的操作，提高交互的友好程度。

（4) 离线存储。移动应用开发框架满足跨平台需求主要依靠混合开发模式，结合HTML5新特性，可通过离线存储减少数据流量开销并加快数据访问速度。

HTML5语言的出现及移动终端多平台发展，使多平台适配技术的研究呈现出良好的势头。从概念上讲，HTML5增强了多媒体、Web离线及本地数据存储的能力，具备了调用移动终端本地资源的能力，促使将移动应用以WebApp形式部署在云端，将部分计算、存储功能转移到云端。移动应用开发框架着重研究使用标准且统一的跨平台开发语言、统一的跨平台API编程接口、统一的跨平台开发环境（IDE）。它将包括移动开发构件集、API封装以及开发IDE或主流IDE的插件支持。

移动应用开发框架对移动应用开发中常用到的功能或模式进行抽取和封装，根据面向应用、面向业务或面向操作系统的需求，形成不同粒度的开发构件，方便开发者通过HTML5+CSS技术进行代码量极少的简单调用，即可实现功能并达到跨平台适配的效果，屏蔽Android、iOS、WindowsPhone等操作系统带来的差异性，降低跨平台开发的成本。值得一提的是，基于构件技术的移动应用开发框架，除了提供丰富的移动端构件集外，还将提供与云端融合的移动服务端构件。

### MVC架构技术

MVC架构模式将整个应用分成Model、View和Controller三个部分，而这些组成部分其实也有着几乎相同的职责。

* 视图：管理作为位图展示到屏幕上的图形和文字输出；
* 控制器：翻译用户的输入并依照用户的输入操作模型和视图；
* 模型：管理应用的行为和数据，响应数据请求（经常来自视图）和更新状态的指令（经常来自控制器）；

控制器负责对模型中的数据进行更新，而视图向模型中请求数据；当有用户的行为触发操作时，会有控制器更新模型，并通知视图进行更新，在这时视图向模型请求新的数据，这是标准MVC模式下，Model、View和Controller之间的协作方式。

在MVC中，模型层可以单独工作，而视图层和控制器层都依赖与模型层中的数据。MVC最重要的概念就是分离展示层，如何在领域对象（DomainObject）和我们在屏幕上看到的GUI元素进行划分是MVC架构模式中最核心的问题。GUI应用程序由于其需要展示内容的特点，分为两个部分：一部分是用于展示内容的展示层（PresentationLayer），另一部分包含领域和数据逻辑的领域层（DomainLayer）。

展示层依赖于领域层中存储的数据，而领域层对于展示层一无所知，领域层其实也是MVC模式中的模型层，而展示层可以理解为VC部分。MVC最重要的目的并不是规定各个模块应该如何交互和联系，而是将原有的混乱的应用程序划分出合理的层级，把一团混乱的代码，按照展示层和领域层分成两个部分；在这时，领域层中的领域对象由于其自身特点不需要对展示层有任何了解，可以同时为不同的展示层工作。

除了分离展示层，MVC还与观察者同步关系紧密。因为在MVC模式中，模型可以单独工作，同时它对使用模型中数据的视图和控制器一无所知，为了保持模型的独立性，我们需要一种机制，当模型发生改变时，能够同时更新多个视图和控制器的内容；在这时，就需要以观察者同步的方式解决这个问题。

### 面向服务的架构（SOA）

SOA（面向服务的体系架构）提供一种构建IT组织的标准和方法，并通过建立可组合、可重用的服务体系来减少IT业务冗余并加快项目开发的进程。在应用整合中，每个应用系统向其他应用系统提供了服务的接口，供其他系统进行调用，从而达到系统互联的目的。Web服务和面向服务的体系结构（SOA）的成熟和完善带给整合的是标准化的体系结构。

基于SOA架构的应用集成开发方法，与传统的软件开发方法略有不同，角色分工更加明确。就整个项目开发周期来讲，首先由业务分析员进行业务及流程定义，然后由架构师和设计人员利用SOA方法将业务和复杂系统进行分割，抽象出对应的业务服务及流程服务；再由开发人员使用不同的开发技术，基于选定的SOA基础架构，进行组件和服务的开发实现、服务的组装与合成，并打包部署和运行调试；最后移交管理人员对服务和业务流程的运行系统进行监控和管理，SOA系统运行中，还可能会涉及操作人员参与业务流程的处理和使用。

### NativeApp技术

移动终端上的App有本地化应用(NativeApp)，基于WEB的应用WebApp，混合型应用（HybridAPP）。我的长沙—城市移动综合服务平台采用混合型应用（HybridAPP）实现。

本地化应用(NativeApp)和基于WEB的应用WebApp犹如C/S和B/S。C/S技术即系统是由客户端和服务器两部分组成。客户端部分的主要任务是提供用户交互的界面，控制应用程序的逻辑。服务器负责有效地管理系统的资源，尤其是对安全性要求较高的数据库管理和访问控制等。

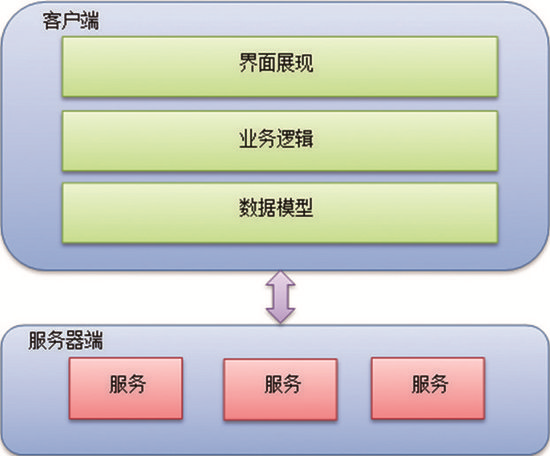
在C/S架构中，对产品开发的要求是两端都需要大量的开发工作。客户端主要是针对Windows等用户操作系统平台进行开发，使用大量与操作系统相关的API，开发工作量大，版本更新困难。服务器端主要是进行数据库管理方面的开发工作。因此，开发人员会分成两类，基本上没有交集。在系统维护上也比较复杂，最难的就是客户端的版本控制和升级工作，给维护工作带来很大的工作量。另外也不适合移植，如果用户要求要支持Linux系统的客户端，那就只能投入更多的客户端人力重新开发一套客户端软件。

随着三层C/S结构、浏览器、脚本语言、Web技术的发展，出现了B/S架构，即系统是由浏览器Browser和服务器Server两部分组成。浏览器采用用户设备上自带的各种浏览器，这样在用户设备上无须再安装客户端软件，也无须为客户端软件支付开发成本。服务器端采用三层或多层结构，利用脚本语言等形成以网页形式提供的用户交互界面，然后与业务逻辑和数据库进行协作。显然，相比C/S结构，B/S一方面可以减少客户端的开发和移植工作，节省客户端的维护费用；另一方面由于表示层、数据和业务逻辑都在服务器端，可以自由地进行系统维护和升级工作。

但B/S结构也有不足之处，比如受网络制约，同时安全性难以控制。另外B/S也不能满足所有的用户需求，比如浏览器受安全性限制，不易于操作用户设备上的更多资源。于是浏览器插件被引入进来，通过浏览器插件，一些需要使用用户本地资源的功能得以实现。

直到今天，Web技术已经发展到2.0时代，Web页面的展现效果已经非常丰富，但C/S和B/S两种架构依然同时存在，二者的优劣都相当明显，谁也无法替代对方。

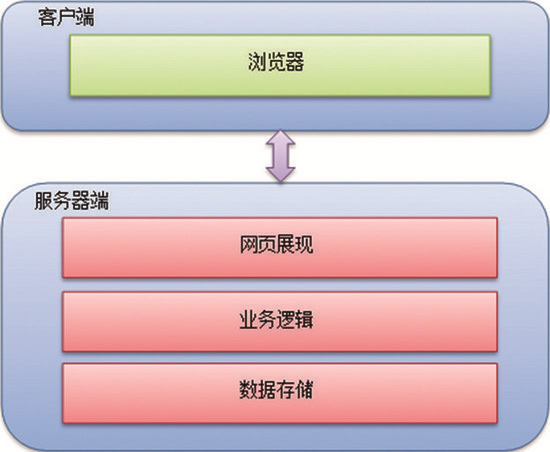
NativeApp架构的客户端中包含了界面展现、业务逻辑、数据模型三个部分。通过网络访问服务器端的各种服务。以手机导航软件为例，在手机上会使用相应操作系统的API开发界面，然后调度业务逻辑层的进行功能实现。当需要展现地图时，如果手机上没有地图数据，就会使用经纬度坐标访问服务器上的地图服务，从服务器获取地图数据，解析后再通过界面绘制出来。在这样的交互下，服务器端的服务独立性较强，其业务形态完全是由客户端控制和调度。



NativeApp架构

这与C/S结构是一样的。由于使用了客户端的众多特性，所以客户端的表现力相当丰富，性能较高，用户体验也比较出色。但劣势也比较明显：客户端的开发工作量大，逻辑复杂；客户端不利于移植，必须针对不同的操作系统进行单独的适配开发工作；客户端软件升级和维护困难；服务器端要支持多客户端，难于扩展。

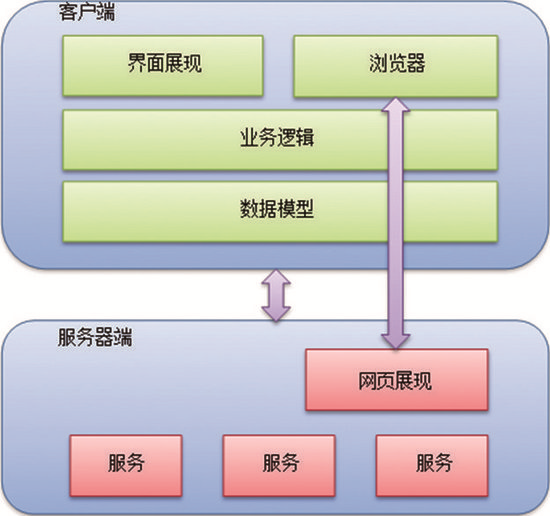
WebApp基本上对应了B/S架构。客户端不再需要开发工作，退化为使用内置的浏览器与用户交互。服务器端以HTML5、CSS3、JavaScript作为前端供浏览器展示，使用其他服务器端技术实现业务逻辑和数据库管理。相对于C/S结构，其最大优势在于无客户端，不需要专门的开发和移植工作。即使使用WebView控件的客户端，也易于开发和移植。另外的优势就是由于代码全部在服务器端，所以易于扩展和升级。



WebApp架构

同样，WebApp的劣势也比较明显：服务器端的开发工作量大，逻辑复杂；界面响应稍慢，性能弱；难于使用设备的特性比如传感器、GPS定位、本地文件系统等。

在目前WebApp受限于浏览器或前端技术未标准化的情况下，可以进行组合应用，这种应用也被称为HybridApp。在这种结构中，对于侧重性能、体验、设备特性、本地数据管理的部分，采用Native的方式，其余的部分采用Web方式，通过这种结合，可以有效地形成互补。这就像在B/S结构上增加浏览器插件一样，对二者进行融合。



HybridAPP架构

我的长沙—城市移动综合服务平台采用这种融合方案(HybridAPP)，既可以发挥本地应用的优势，又能有机地整合后端资源。对于需要本地化的部分，继续采用操作系统的API接口进行客户端开发，对于适合Server端的部分，通过嵌入WebView等浏览器控件进行实现，也可以采用一些框架来消除网页展现中难于使用设备本身特性的缺点。

### OAuth2.0技术

账号授权开放系统符合OAuth2.0国际标准协议，OAuth在"客户端"与"服务提供商"之间，设置了一个授权层（authorizationlayer）。"客户端"不能直接登录"服务提供商"，只能登录授权层，以此将用户与客户端区分开来。"客户端"登录授权层所用的令牌（token），与用户的密码不同。用户可以在登录的时候，指定授权层令牌的权限范围和有效期。

"客户端"登录授权层以后，"服务提供商"根据令牌的权限范围和有效期，向"客户端"开放用户储存的资料。

OAuth2.0定义了四种授权方式。（1）授权码模式（authorizationcode），（2）简化模式（implicit），（3）密码模式（resourceownerpasswordcredentials），（4）客户端模式（clientcredentials）。

（一） 授权码模式

授权码模式（authorizationcode）是功能最完整、流程最严密的授权模式。它的特点就是通过客户端的后台服务器，与"服务提供商"的认证服务器进行互动。

它的步骤如下：

（A）用户访问客户端，后者将前者导向认证服务器。

（B）用户选择是否给予客户端授权。

（C）假设用户给予授权，认证服务器将用户导向客户端事先指定的"重定向URI"（redirectionURI），同时附上一个授权码。

（D）客户端收到授权码，附上早先的"重定向URI"，向认证服务器申请令牌。这一步是在客户端的后台的服务器上完成的，对用户不可见。

（E）认证服务器核对了授权码和重定向URI，确认无误后，向客户端发送访问令牌（accesstoken）和更新令牌（refreshtoken）。

（二） 简化模式

简化模式（implicitgranttype）不通过第三方应用程序的服务器，直接在浏览器中向认证服务器申请令牌，跳过了"授权码"这个步骤，因此得名。所有步骤在浏览器中完成，令牌对访问者是可见的，且客户端不需要认证。

它的步骤如下：

（A）客户端将用户导向认证服务器。

（B）用户决定是否给客户端授权。

（C）假设用户给予授权，认证服务器将用户导向客户端指定的"重定向URI"，并在URI的Hash部分包含了访问令牌。

（D）浏览器向资源服务器发出请求，其中不包括上一步收到的Hash值。

（E）资源服务器返回一个网页，其中包含的代码可以获取Hash值中的令牌。

（F）浏览器执行上一步获得的脚本，提取出令牌。

（G）浏览器将令牌发给客户端。。

（三） 密码模式

密码模式（ResourceOwnerPasswordCredentialsGrant）中，用户向客户端提供自己的用户名和密码。客户端使用这些信息，向"服务商提供商"索要授权。

在这种模式中，用户必须把自己的密码给客户端，但是客户端不得储存密码。这通常用在用户对客户端高度信任的情况下，比如客户端是操作系统的一部分，或者由一个著名公司出品。而认证服务器只有在其他授权模式无法执行的情况下，才能考虑使用这种模式。

它的步骤如下：

（A）用户向客户端提供用户名和密码。

（B）客户端将用户名和密码发给认证服务器，向后者请求令牌。

（C）认证服务器确认无误后，向客户端提供访问令牌。

（四） 客户端模式

客户端模式（ClientCredentialsGrant）指客户端以自己的名义，而不是以用户的名义，向"服务提供商"进行认证。严格地说，客户端模式并不属于OAuth框架所要解决的问题。在这种模式中，用户直接向客户端注册，客户端以自己的名义要求"服务提供商"提供服务，其实不存在授权问题。它的步骤如下：

（A）客户端向认证服务器进行身份认证，并要求一个访问令牌。

（B）认证服务器确认无误后，向客户端提供访问令牌。

### CAS单点登录技术

单点登录（SingleSign-On,简称SSO）是目前比较流行的服务于业务整合的解决方案之一，SSO使得在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

简单SSO的体系中，会有下面三种角色：User（多个），Web应用（多个），SSO认证中心（1个）。Web应用不处理User的登录，否则就是多点登陆了，所有的登录都在SSO认证中心进行。SSO认证中心通过一些方法来告诉Web应用当前访问用户究竟是不是张三/李四。SSO认证中心和所有Web应用建立一种信任关系，SSO认证中心对用户身份正确性的判断会通过某种方法告Web应用，而且判断结果必须被Web应用信任。

CAS（CentralAuthenticationService）是Yale大学发起的一个企业级的、开源的项目，旨在为Web应用系统提供一种可靠的单点登录解决方法（属于WebSSO）。CAS开始于2001年，并在2004年12月正式成为JA-SIG的一个项目。

（一） 主要特性

1、开源的、多协议SSO解决方案；

Protocols：CustomProtocol、CAS、OAuth、OpenID、RESTfulAPI、SAML1.1、SAML2.0等。

2、支持多种认证机制：ActiveDirectory、JAAS、JDBC、LDAP、X.509Certificates等；

3、安全策略：使用票据（Ticket）来实现支持的认证协议；

4、支持授权：可以决定哪些服务可以请求和验证服务票据（ServiceTicket）；

5、提供高可用性：通过把认证过的状态数据存储在TicketRegistry组件中，这些组件有很多支持分布式环境的实现，如：BerkleyDB等；

6、支持多种客户端：Java、.Net、PHP、Perl、Apache,uPortal等。

SSO实现模式一般包括以下三个原则：

1、所有的认证登录都在SSO认证中心进行；

2、SSO认证中心通过一些方法来告诉Web应用当前访问用户究竟是不是已通过认证的用户；

3、SSO认证中心和所有的Web应用建立一种信任关系，也就是说web应用必须信任认证中心。（单点信任）

SSO的主要实现方式有：

1、共享cookies。基于共享同域的cookie是Web刚开始阶段时使用的一种方式，它利用浏览同域名之间自动传递cookies机制，实现两个域名之间系统令牌传递问题；另外，关于跨域问题，虽然cookies本身不跨域，但可以利用它实现跨域的SSO。如：代理、暴露SSO令牌值等。缺点：不灵活而且有不少安全隐患，已经被抛弃。

2、Broker-based(基于经纪人)。这种技术的特点就是，有一个集中的认证和用户帐号管理的服务器。经纪人给被用于进一步请求的电子身份存取。中央数据库的使用减少了管理的代价，并为认证提供一个公共和独立的"第三方"。例如Kerberos、Sesame、IBMKryptoKnight（凭证库思想)等。Kerberos是由麻省理工大学发明的安全认证服务，已经被UNIX和Windows作为默认的安全认证服务集成进操作系统。

3、Agent-based（基于代理人）。在这种解决方案中，有一个自动地为不同的应用程序认证用户身份的代理程序。这个代理程序需要设计有不同的功能。比如，它可以使用口令表或加密密钥来自动地将认证的负担从用户移开。代理人被放在服务器上面，在服务器的认证系统和客户端认证方法之间充当一个"翻译"。例如SSH等。

4、Token-based。例如SecureID,WebID，现在被广泛使用的口令认证，比如FTP、邮件服务器的登录认证，这是一种简单易用的方式，实现一个口令在多种应用当中使用。

5、基于网关

6、基于SAML。SAML(SecurityAssertionMarkupLanguage，安全断言标记语言）的出现大大简化了SSO，并被OASIS批准为SSO的执行标准。开源组织OpenSAML实现了SAML规范。

（二） CAS的基本原理

从结构体系看，CAS包括两部分：CASServer和CASClient。

CASServer负责完成对用户的认证工作,需要独立部署,CASServer会处理用户名/密码等凭证(Credentials)。

CASClient。负责处理对客户端受保护资源的访问请求，需要对请求方进行身份认证时，重定向到CASServer进行认证。（原则上，客户端应用不再接受任何的用户名密码等Credentials）。CASClient与受保护的客户端应用部署在一起，以Filter方式保护受保护的资源。

CAS原理和协议：基础模式SSO访问流程主要有以下步骤：

1、访问服务：SSO客户端发送请求访问应用系统提供的服务资源。

2、定向认证：SSO客户端会重定向用户请求到SSO服务器。

3、用户认证：用户身份认证。

4、发放票据：SSO服务器会产生一个随机的ServiceTicket。

5、验证票据：SSO服务器验证票据ServiceTicket的合法性，验证通过后，允许客户端访问服务。

6、传输用户信息：SSO服务器验证票据通过后，传输用户认证结果信息给客户端。

CASClient与受保护的客户端应用部署在一起，以Filter方式保护Web应用的受保护资源，过滤从客户端过来的每一个Web请求，同时，CASClient会分析HTTP请求中是否包含请求ServiceTicket，如果没有，则说明该用户是没有经过认证的；于是CASClient会重定向用户请求到CASServer（Step2），并传递Service（要访问的目的资源地址）。Step3是用户认证过程，如果用户提供了正确的Credentials，CASServer随机产生一个相当长度、唯一、不可伪造的ServiceTicket，并缓存以待将来验证，并且重定向用户到Service所在地址（附带刚才产生的ServiceTicket）,并为客户端浏览器设置一个TicketGrantedCookie（TGC）；CASClient在拿到Service和新产生的Ticket过后，在Step5和Step6中与CASServer进行身份核实，以确保ServiceTicket的合法性。

在该协议中，所有与CASServer的交互均采用SSL协议，以确保ST和TGC的安全性。协议工作过程中会有2次重定向的过程。但是CASClient与CASServer之间进行Ticket验证的过程对于用户是透明的（使用HttpsURLConnection）。

CAS代理模式：该模式形式为用户访问App1，App1又依赖于App2来获取一些信息，如：User-->App1-->App2。

这种情况下，假设App2也是需要对User进行身份验证才能访问，那么，为了不影响用户体验（过多的重定向导致User的IE窗口不停地闪动)，CAS引入了一种Proxy认证机制，即CASClient可以代理用户去访问其它Web应用。

代理的前提是需要CASClient拥有用户的身份信息(类似凭据)。之前我们提到的TGC是用户持有对自己身份信息的一种凭据，这里的PGT就是CASClient端持有的对用户身份信息的一种凭据。凭借TGC，User可以免去输入密码以获取访问其它服务的ServiceTicket，所以，这里凭借PGT，Web应用可以代理用户去实现后端的认证，而无需前端用户的参与。

下面为代理应用（helloService）获取PGT的过程：（注：PGTURL用于表示一个Proxy服务，是一个回调链接；PGT相当于代理证；PGTIOU为取代理证的钥匙，用来与PGT做关联关系；）

CASClient在基础协议之上，在验证ST时提供了一个额外的PGTURL(而且是SSL的入口)给CASServer，使得CASServer可以通过PGTURL提供一个PGT给CASClient。

CASClient拿到了PGT(PGTIOU-85…..ti2td)，就可以通过PGT向后端Web应用进行认证。

CAS的SSO实现方式可简化理解为：1个Cookie和N个Session。CASServer创建cookie，在所有应用认证时使用，各应用通过创建各自的Session来标识用户是否已登录。

用户在一个应用验证通过后，以后用户在同一浏览器里访问此应用时，客户端应用中的过滤器会在session里读取到用户信息，所以就不会去CASServer认证。如果在此浏览器里访问别的web应用时，客户端应用中的过滤器在session里读取不到用户信息，就会去CASServer的login接口认证，但这时CASServer会读取到浏览器传来的cookie（TGC），所以CASServer不会要求用户去登录页面登录，只是会根据service参数生成一个Ticket，然后再和web应用做一个验证ticket的交互而已。

（三） CAS安全性

CAS的安全性仅仅依赖于SSL。使用的是securecookie。

TGC/PGT安全性。对于一个CAS用户来说，最重要是要保护它的TGC，如果TGC不慎被CASServer以外的实体获得，Hacker能够找到该TGC，然后冒充CAS用户访问所有授权资源。PGT的角色跟TGC是一样的。从基础模式可以看出，TGC是CASServer通过SSL方式发送给终端用户，因此，要截取TGC难度非常大，从而确保CAS的安全性。TGT的存活周期默认为120分钟。

ST/PT安全性。ST（ServiceTicket）是通过Http传送的，因此网络中的其他人可以Sniffer到其他人的Ticket。CAS通过以下几方面来使ST变得更加安全（事实上都是可以配置的）：

1、ST只能使用一次。CAS协议规定，无论ServiceTicket验证是否成功，CASServer都会清除服务端缓存中的该Ticket，从而可以确保一个ServiceTicket不被使用两次。

2、ST在一段时间内失效。CAS规定ST只能存活一定的时间，然后CASServer会让它失效。默认有效时间为5分钟。

3、ST是基于随机数生成的。ST必须足够随机，如果ST生成规则被猜出，Hacker就等于绕过CAS认证，直接访问对应的服务。

### 云端融合服务技术

云端融合服务包括面向移动应用的应用打包服务、消息推送服务、权限认证服务、位置服务；面向业务层的适配服务、邮件服务；以及面向数据的存储服务、内容服务、数据同步服务、行为统计服务等。

应用打包服务。以HTML5形式编写的应用能够上传,根据规则,自动编译、打包成iOS、Android、WindowsPhone等平台的应用安装包。

应用管理服务。开发者可以提交应用程序进行发布，而应用管理服务根据开发者提供的申请、文案、安装程序提供审核功能（包括自动和人工），审核通过后应用程序上架（上架内容包括文案、下载链接、二维码）。开发者同样可按上述步骤进行应用程序更新，更新审核通过后修改上架内容，并向已安装该应用的用户推送更新通知。

权限认证服务。统一的权限认证服务,面向API级别的权限控制;提供oauth2.0的开放认证。

消息推送服务。提供从云端到终端的消息推送服务。

行为统计服务。对移动终端用户操作行为进行统计。初始将需要进行统计的行为在云端注册，用户进行了注册过的操作，终端将会向云端提交操作日志（提交分为即时提交和阶段提交），可以在后期进行行为分析。

短信网关集成。云端集成短信网关，能够通过云端根据用户及用户分组向终端发送短信。

邮件服务。集成常见的邮件服务，并能和短信和推送服务连接。

内容服务。主要针对内容发布的场景，如新闻、杂志、博物馆展品等。提供发布、管理、维护内容的服务，内容的形式包括网页、PDF、epub、图片等格式或是以上的压缩格式。终端能够根据云端发布的内容目录下载对应的内容，进行阅览（在线或离线）。

存储服务。提供对普通文件的存储服务，提供对多媒体文件的存储服务,提供对所存储文档、图片、视频等缩略图服务，提供对所存储文档的分页浏览服务，提供对所存储声音、视频的流服务。

同步服务。对终端的通讯录、短信、邮件、文件等提供多样化的同步服务。

位置服务。收集和存储终端的定位数据，提供面向空间关联、时间轴线等场景的分析、统计、查询服务。

### 移动互联网技术

Widget技术。Widget(中文译名为微件)是一小块可以在任意基于HTML的Web页面上执行的代码,它的表现形式可能是视频、地图、新闻、小游戏等，其根本思想来源于代码复用。通常情况下Widget的代码形式包含DHTML（动态超文本标记语言）、JavaScript以及AdobeFlash[3]。

移动Mashup技术。Mashup将两种以上使用公共或者私有数据库的Web应用加在一起形成一个整合应用。是通过多种渠道将多个源的数据和应用功能揉合起来创建全新的服务。Mashup的典型应用：地图Mashup、视频和图像、搜索和购物、新闻Mashup、微博Mashup。

RSS技术。RSS(聚合内容)是一种描述和同步网站内容的技术，是资源共享模式的延伸。RSS技术被广泛使用在时效性比较强的内容中。例如在网站发布一个RSSFeed，这个RSSFeed中包含的信息能直接被其他站点调用，用户可以快速获取网站上最新更新的内容。

P2P技术。P2P(点对点技术)，又称对等互联网络技术，是一种用户终端之间不通过中介设备直接交换数据和资源的技术。P2P的本质是把集中处理和存储转化为分布式处理和存储，它改变了互联网以服务器为中心的状态，使得网络应用的核心从中央服务器扩散到终端设备。P2P典型应用包括服务共享、应用协作、构建充当基层架构的互联系统等。

ReactNative。ReactNative是Facebook早先开源的UI框架React在原生移动应用平台的衍生产物，目前支持iOS和安卓两大平台。RN使用Javascript语言，类似于HTML的JSX，以及CSS来开发移动应用.ReactNative能够在Javascript和React的基础上获得完全一致的开发体验，构建世界一流的原生APP。

SpringBoot是由Pivotal团队提供的全新框架，其设计目的是用来简化新Spring应用的初始搭建以及开发过程。该框架使用了特定的方式来进行配置，从而使开发人员不再需要定义样板化的配置。通过这种方式，SpringBoot致力于在蓬勃发展的快速应用开发领域(rapidapplicationdevelopment)成为领导者。

SpringMVC属于SpringFrameWork的后续产品，已经融合在SpringWebFlow里面。Spring框架提供了构建Web应用程序的全功能MVC模块。使用Spring可插入的MVC架构，从而在使用Spring进行WEB开发时，可以选择使用Spring的SpringMVC框架或集成其他MVC开发框架

socket本质是编程接口(API)，对TCP/IP的封装，TCP/IP也要提供可供程序员做网络开发所用的接口，这就是Socket编程接口；HTTP是轿车，提供了封装或者显示数据的具体形式；Socket是发动机，提供了网络通信的能力。

Socket的英文原义是“孔”或“插座”。作为BSDUNIX的进程通信机制，取后一种意思。通常也称作"套接字"，用于描述IP地址和端口，是一个通信链的句柄，可以用来实现不同虚拟机或不同计算机之间的通信。在Internet上的主机一般运行了多个服务软件，同时提供几种服务。每种服务都打开一个Socket，并绑定到一个端口上，不同的端口对应于不同的服务。Socket正如其英文原义那样，像一个多孔插座。一台主机犹如布满各种插座的房间，每个插座有一个编号，有的插座提供220伏交流电，有的提供110伏交流电，有的则提供有线电视节目。客户软件将插头插到不同编号的插座，就可以得到不同的服务。

Dubbo是一款高性能、轻量级的开源JavaRPC框架，它提供了三大核心能力：面向接口的远程方法调用，智能容错和负载均衡，以及服务自动注册和发现。

CAS（ConsoleAccessServer），控制台访问服务器，系提供电脑设备系统控制台访问的一种设备或服务器

Node是一个让JavaScript运行在服务端的开发平台，它让JavaScript成为与PHP、Python、Perl、Ruby等服务端语言平起平坐的脚本语言。[1]发布于2009年5月，由RyanDahl开发，实质是对ChromeV8引擎进行了封装。

Node对一些特殊用例进行优化，提供替代的API，使得V8在非浏览器环境下运行得更好。V8引擎执行Javascript的速度非常快，性能非常好。[2]Node是一个基于ChromeJavaScript运行时建立的平台，用于方便地搭建响应速度快、易于扩展的网络应用。Node使用事件驱动，非阻塞I/O模型而得以轻量和高效，非常适合在分布式设备上运行数据密集型的实时应用。

Hibernate是一个开放源代码的对象关系映射框架，它对JDBC进行了非常轻量级的对象封装，它将POJO与数据库表建立映射关系，是一个全自动的orm框架，hibernate可以自动生成SQL语句，自动执行，使得Java程序员可以随心所欲的使用对象编程思维来操纵数据库。Hibernate可以应用在任何使用JDBC的场合，既可以在Java的客户端程序使用，也可以在Servlet/JSP的Web应用中使用，最具革命意义的是，Hibernate可以在应用EJB的JaveEE架构中取代CMP，完成数据持久化的重任。

MongooseWebServer是一款易于使用的Web服务器，它可以嵌入到其它应用程序中，为其提供Web接口。

跨平台，支持Windows、OSX和Linux

支持CGI,SSL,SSI,Digest(MD5)认证，WebSocket和WebDAV

支持断点续传和URL重写

基于IP的ACL，支持Windows服务，支持GET,POST,HEAD,PUT,DELETE方法

ExcludingfilesfromservingbyURIpattern

下载速度限制，基于客户端子网和URI模式

体积小，可执行文件只有40k左右

可嵌入式，提供简单的API(mongoose.h).只需一个源码文件mongoose.c

嵌入式实例:hello.c,post.c,upload.c,websocket.c

提供Python和C#版本

采用MIT授权协议

Jedis是Redis官方推荐的Java连接开发工具。要在Java开发中使用好Redis中间件，必须对Jedis熟悉才能写成漂亮的代码。

### 中间件技术

中间件具有以下的一些特点：满足大量应用的需要；运行于多种硬件和OS平台；支持分布式计算，提供跨网络、硬件和OS平台的透明性的应用或服务的交互功能；支持标准的协议；支持标准的接口。程序员通过调用中间件提供的大量API，实现异构环境的通讯，从而屏蔽异构系统中复杂的操作系统和网络协议。针对不同的操作系统和硬件平台，它们可以有符合接口和协议规范的多种实现。由于标准接口对于可移植性和标准协议对于互操作性的重要性，中间件已成为许多标准化工作的主要部分。对于应用软件开发，中间件远比操作系统和网络服务更为重要，中间件提供的程序接口定义了一个相对稳定的高层应用环境，不管底层的计算机硬件和系统软件怎样更新换代，只要将中间件升级更新，并保持中间件对外的接口定义不变，应用软件几乎不需任何修改，从而保护了企业在应用软件开发和维护中的重大投资。

中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源。中间件管理着客户端程序和数据库或者早期应用软件之间的通讯。

中间件在分布式的客户和服务之间扮演着承上启下的角色，如事务管理、负载均衡以及基于Web的计算等。

利用这些技术有助于减轻开发者的负担，使他们利用现有的硬件设备、操作系统、网络、数据库管理系统以及对象模型创建分布式应用软件时更加得心应手。由于中间件能够保护企业的投资，保证应用软件的相对稳定，实现应用软件的功能扩展；同时中间件产品在很大程度上简化了一个由不同硬件构成的分布式处理环境的复杂性，所以它的出现正日益引起用户的关注。

### 负载均衡技术

互联网负载均衡，是对多台云服务器进行流量分发的负载均衡服务。可在多个实例间自动分配应用程序的对外服务能力，通过消除单点故障提升应用系统的可用性，让您实现更高水平的应用程序容错能力，从而无缝提供分配应用程序流量所需的负载均衡容量，为您提供高效、稳定、安全的服务。

Nginx是一款轻量级的Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器，并在一个BSD-like协议下发行。其特点是占有内存少，并发能力强，事实上nginx的并发能力确实在同类型的网页服务器中表现较好，中国大陆使用nginx网站用户有：百度、京东、新浪、网易、腾讯、淘宝等。

Keepalived，它是一个高性能的服务器高可用或热备解决方案，Keepalived主要来防止服务器单点故障的发生问题，可以通过其与Nginx的配合实现web服务端的高可用。

### 数据序列化技术

本项目的业务数据，采用Google Protocol Buffer( 简称 Protobuf) 技术，进行数据结构序列化、反序列化，以实现高效的压缩、存储。

Protobuf是一种轻便高效的结构化数据存储格式，可以用于结构化数据串行化，或者说序列化。它很适合做数据存储或 RPC 数据交换格式。可用于通讯协议、数据存储等领域的语言无关、平台无关、可扩展的序列化结构数据格式。

Protobuf的优点：

（1)数据更安全，性能更高。它以高效的二进制方式存储，Protobuf同XML相比，比XML小3到10倍，快20到100倍。数据经过序列化之后，数据转换为字节流，如没有Protobuf的格式定义，是无法反序列化的，因此数据更安全。

（2)可以自定义数据结构，然后使用代码生成器生成的代码来读写这个数据结构。无需重新部署程序的情况下更新数据结构。

（3)“向后”兼容性好，用户不必破坏已部署的、依靠“老”数据格式的程序就可以对数据结构进行升级。这样程序就可以不必担心因为消息结构的改变而造成的大规模的代码重构或者迁移的问题。因为添加新的消息中的 field 并不会引起已经发布的程序的任何改变。

### 缓存技术

应用缓存技术有助于优化系统性能和减少不必要的跨服务器访问，如果选择了正确的缓存解决方案，它可以随着企业应用的增长而扩大，而无需进行昂贵且耗时的重建。

对象缓存：简单的说使用内存镜像缓存的基本原理是，将那些经常访问，或者访问量大的信息，直接存储在内存中，需要时，就直接从内存中获取，同样也不去查询数据库。例如，有一些数据需要从数据库多个表中查询获得，且几乎每个页面都要调用这些数据。这时，将这些数据缓存在内存中，将会提高不少的性能。

数据库连接缓存：数据库连接缓存，其实就是我们通常所说的连接池Connection Pool，其主要职责就是将数据库的连接进行缓存，将使用完的数据库连接暂时存放在“池”中，需要时，再从“池”中重新获取，可以减少服务器资源消耗，提高请求响应的效率。

CDN加速：将APP中的静态资源分离出来，如：图标、图片，存放在独立的CDN静态文件服务器上，实现静态资源缓存，有效的降低用户访问时的带宽消耗，从而达到用户访问APP速度快、流畅不卡顿的效果。

# 项目描述

## 2.1项目名称

我的长沙-高新区城市移动综合服务平台项目需求规格说明书。

## 2.2项目背景

“我的长沙”作为长沙市官方唯一的城市级综合服务平台，秉承“以市民为中心”的理念，整合全市直各委办部门移动办事终端，汇集政务、公共和社会服务、融媒体资讯于一体，打造移动端城市服务统一入口，实现一个账号即可在线查看、咨询、办理数百项办事服务，让市民足不出户就可以享受到方便快捷、统一规范、优质高效的城市服务。

根据建设理念，2019年市长办公纪要中表示：原则上同意全市所有移动端政务服务和公共服务逐步整合到“我的长沙”APP；充分运用好市场和政府的力量，广泛开展宣传发动，强力推广“我的长沙”APP，要不断完善功能，优化用户体验，真正将“我的长沙”APP 打造成功能最丰富、使用最方便和覆盖最广泛的长沙城市综合服务移动平台，明确界定市、区县 （市） 在智慧城市建设中的职责分工，做到统分结合，避免重复建设。

根据具体落实2020年11月20日长沙市数据资源管理局出台关于开展“我的长沙”区县（市）版块建设的通知，明确提到建设以下内容：

1.工作目标：2021年6月30日前，各区县完成“我的长沙”app区县（市）专区建设，加强推动各区县（市）各类政务服务，公共服务功能向“我的长沙”聚集，形成各区县（市）城市服务统一入口，让市民和企业享受一站式、线上线下相结合的城市服务体验，全力打造掌上办事之城。

2.建设内容：依托长沙市政府唯一城市移动综合服务平台“我的长沙”APP整合框架，建成具有区县（市）特色的城市服务统一入口，覆盖民生保障、交通出行、医疗健康、生活缴费、人才教育、住房服务、企业服务等政务，公共及社会服务，打造不低于2个拥有本地特色服务的服务专区。

本次“我的长沙”—“我的长沙高新”建设主要目的为在市级服务基础上汇聚本区服务全覆盖、双下沉基础，落实完成关于长沙市数据资源管理局“我的长沙”区县（市）版块建设的通知中内容，做到“家门口”政务服务、公共服务和社会服务汇聚一专区，实现“数据多跑路，群众少跑腿”的效果，让长沙高新区集成数据管理台阶上更上一层，最终达到高新移动端“一屏”直览、服务汇聚的目标。

## 2.3建设依据

1、《市长办公会议纪要》[2019]65号

2、《市政办公会议纪要》[2020]28号

3、《“我的长沙”APP应用推广优化工作调研会会议纪要》

4、《2020年政府工作报告》

5、《长沙市数据资源管理局关于开展“我的长沙”区县（市）版块建设的通知》

6、《长沙市新型智慧城市示范城市顶层设计（2020-2025）》

7、《长沙市新型智慧城市示范城市建设三年行动计划（2020-2022）》

8、《“我的长沙”区县（市）入驻指南》

## 2.4项目目标

### 2.4.1 建设目标及内容

依托市级平台，加强和规范高新区政务服务和民生服务移动应用建设管理，积极推进覆盖范围广、应用频率高的服务事项向移动端延伸。

利用“我的长沙”的集成数据管理能力，支持跨部门的服务协同，实现“一屏”直览服务汇聚的目标，具体建设内容如下：

1. 依托“我的长沙”架构体系，定制高新区特色服务频道，实现平台建设及服务创新模式。具体内容基于“我的长沙”建设1个长沙高新区特色服务频道，接入5个特色专区，建设1个特色专区。

2. 基于“我的长沙”统一实名认证用户体系，通过用户授权方式实现长沙高新区特色服务频道及特色服务的单点登录和自动填表；进行用户权限管控，实现部分服务实名访问，部分服务普通帐户即可访问，达到一号通行的服务目标。

3. 依托运营管理平台，实现长沙高新区内信息发布和维护功能，发布活动信息、新闻动态。

4. 提供长沙高新区城市服务平台及运维服务，面向长沙高新区市民提供本地化特色城市服务。

### 2.4.2 运营目标及内容

通过多样化的运营手段，结合用户反馈优化服务及操作体验，提高服务的实用性和易用性，增强用户粘性，保证用户对APP的忠诚度。

“我的长沙”—“我的长沙高新”项目，通过专业、有效的应用推广工作开展，实现长沙高新专区全年访问次数达到50万，半年访问次数达到25万，平均月活跃度达到高新区常住总人口数(40万)的7%。具体运营内容包括：

内容运营：保障“我的长沙高新”专区用户每阶段有新的内容及信息浏览，促进“我的长沙高新”专区日活用户增长，提高用户的活跃频次。

产品运营：整理收集的反馈（问题、建议），确保用户与产品信息互通。从而分析用户使用习惯及产品发展需求，不断更新换代、优化产品，最终实现用户达到最佳的体验感。

用户运营：保障“我的长沙高新”用户帐户信息安全、日常活跃度的稳定，利用用户体系及积分体系，结合推送功能提高“我的长沙高新”专区日活用户的活跃度。

数据运营：对“我的长沙高新”平台的总体数据指标及报表进行管理和输出，从全局统计和分析数据的增长或下降趋势。提供分析报表和解决方案，为“我的长沙高新”运营团队后续工作方向提供数据论证。

活动运营：保障阶段性的用户大量增长及专区活跃度提升，利用各种有效的手段，以最小的成本获取最多最优质的用户。

宣传推广：保障“我的长沙高新”用户的持续增长和品牌及口碑的持续传播，通过不同的手段和渠道建立不同的推广方式，以最小的代价获取最多的用户活跃。

## 2.5建设模式

我的长沙高新”专区定位为长沙高新区唯一官方移动端服务总入口，是为本区市民量身定做的移动端服务平台。通过“我的长沙高新”专区，市民能够更快速、便捷的查询专属本区的移动应用服务，为市民打造可信、可及的优质指尖服务。

## 2.6建设必要性及意义

### 2.6.1贯彻政策要求，配合建设城市移动端综合服务平台

2020年8月27日，长沙市市长办公会特别指出“加快推动全市各类政务服务、公共服务类 APP 功能向‘我的长沙’集聚，形成城市服务统一入口”。同年11月20日，长沙市数据资源管理局发布《关于加快推进“我的长沙”APP区县（市）专区建设的通知》（长数管函[2020]120号），要求各区县（市），建好用好“我的长沙”APP，构建功能丰富、使用方便、覆盖广泛的城市综合服务移动平台，打造不低于2个拥有本地特色服务的服务专区。

根据上级政策要求，“我的长沙”APP高新专区建设势在必行。通过统筹区级各部门单位的移动应用平台，将政务服务、公共服务和社会服务接入或者并入到“我的长沙”APP，构建高新专区应用，满足企业、市民和外访游客的服务需求。

### 2.6.2落实规划建设任务，推进新型智慧城市建设

根据《长沙市新型智慧城市示范城市顶层设计(2021-2025年)》的要求，加快推进“我的长沙”城市移动综合服务平台在移动端对各类政务服务、社会服务和社会机构提供服务事项的统筹。

推进“我的长沙”APP高新专区建设，是落实市区新型智慧城市规划建设任务的具体举措，是加快城市服务升级、城市智慧化改革的重要抓手，以移动端高新专区建设，促进高新区新型智慧城市发展。

### 2.6.3共享“互联网+城市服务”成果，提升政府服务效能

移动设备具有方便、快捷、高效的特性，已成为市民生活中不可缺少的必需品。在移动端提供政务服务、公共服务及社会服务，让市民随时随地可办理，将有助于解决市民办事的堵点、痛点及难点，大幅提升公共服务均等化、普惠化、便捷化水平，极大程度上满足民众对于“互联网+政务服务”的需求，进一步提升市民办事的便捷性。

目前长沙市政务一体化平台和“互联网+政务服务”建设已经取得了重大成果，“我的长沙”APP作为移动端服务窗口，已与“互联网+政务服务”一体化平台对接，高新专区基于“我的长沙”平台架构，进一步对接区内“互联网+”平台和数据资源，给本区市民提供移动场景服务，提升政务服务效能，让本区市民享受更多的智慧化城市服务。

### 2.6.4推进信息化建设科学投资，减少重复建设问题

统筹移动端平台接入高新专区，避免区级各部门单位重复投资，促进信息化建设的科学投资。以高新专区建设为抓手，加强区内各移动端平台的接入，梳理各平台重复应用场景和功能，规避“僵尸平台”的资源浪费。着重对接重点产业和领域平台，提升数据赋能能力，将高新区发展重点凸显到移动端门户，助推城市整体规划建设。

信息化和智慧化在解决城市服务、资源浪费等城市化问题方面有重大创新和突破性进展。通过改进城市服务供给模式，激发社会创新活力，破解民生热点、难点问题，提升全区城市服务水平。

## 2.7预期效益

本次项目将大大推进线下城市服务与网上服务的融合发展，适应“互联网+政务服务”发展需要，打造线上线下功能相辅相成的城市服务新模式，依法有序开放网上城市服务资源和数据，提升政府各部门间的数据共享、交换服务能力，构建城市服务“一站式”服务平台，提供多样化、创新性的便民服务，提升政府各部门间的数据共享、交换服务能力，进一步提升政务部门的公共服务能力，提升办事效率、提升办事满意度，从而提供真正便民的城市服务，使得市民有更强的城市服务和智慧城市的获得感。预期的效益包括：

1、创新城市服务新模式

通过提供“一站式”的城市服务，面向市民提供覆盖各类特色服务及特色专区等方面的统一入口的一站式服务，打破传统线下城市服务的模式，创新新型公共服务新模式，汇聚整合各类便民应用，通过场景式提供服务，覆盖市民的全生命周期，为市民提供城市服务新模式，提升城市服务质量。

2、完善城市服务体系

通过对项目采购城市服务进行运营推广，面向不同层次的市民，提供需要的城市服务内容，实现城市服务信息的推广和宣传，同时实现市民对城市服务的沟通和交流，从而倒逼政务部门对城市服务体系进行完善，为市民提供更加优质的公共服务。

3、整合资源、拉动产业

目前各类社会管理和服务平台大多属于“垂直”的平台建设和运营服务模式，缺少横向的的业务协同。本项目运营将进一步整合现有数据资源，通过互联网技术，与平台提供的增值服务对接，形成集中管理运营模式，实现信息通畅、信息验证、不见面审批的节约型政务服务模式，同时本项目运营涉及多个领域和行业的推广宣传，将为各行各业发展带来巨大的经济效益。

4、营造良好的商业环境，促进城市服务提升、服务经济增长

本项目的运营推广，通过项目内容运营的进行，促进城市服务个性化、城市管理精细化、政府服务便捷化的应用格局。通过收集并分析数据和智能信息来更准确地规划业务基础架构和城市服务，从而创造具有竞争力的商业环境来吸引投资者，促进城市服务提升和服务经济发展。

5、构建新城市生态系统，提升城市生活质量。

通过互联网技术将本次项目采购的城市服务，通过线上、线下、活动等多渠道的推广，使得城市服务尽可能的扩大，覆盖人群惠及更多用户，实现“大数据服务美好生活”的目标，让市民更加体会到智慧城市的成果，提升生活质量，从而提升智慧城市的获得感。

## 2.7假定和约束

本项目于实施建设过程需根据该章节里包含的假定及约束条件做为实施标准。

### 2.7.1建设规模

本项目建设我的长沙—高新区移动综合服务平台1套，包含平台建设。

### 2.7.2项目建设期

本项目建设期为2个月，从2021年5月至2021年7月。

# 系统功能需求

本次项目建设终端应用建设APP终端应用

APP端涵盖全部的城市服务，产品完善成熟，是用户享受城市服务的标配，APP 包含我的办事、我的服务、我的资讯、我的生活、个人中心和在线客服等服务模块。

## 3.1建设方案

### 3.1.1基础平台支撑

基于“我的长沙”整体框架和建设成果，为“我的长沙APP-高新区”提供统一的服务入口、统一的用户认证、统一的数据库服务。

3. 1. 1. 1. 统一用户认证服务

“我的长沙APP-高新区”采用“我的长沙”APP的用户统一认证系统。统一认证的基本方式是轻应用通过标准接口调用认证服务，“我的长沙”APP认证成功后将认证结果返回给轻应用，完成认证流程。

统一用户集成是指用户可使用一个账号登录不同的系统，由该账号管理方为其他系统提供认证服务。政府部门轻应用采用实名账号统一认证服务既可提高建设效率，又可极大地方便用户。

统一用户集成的基本方式是轻应用调用认证服务接口，弹出登录页，由用户输入账号（用户名）和登录口令，账号管理方认证后将结果返回给轻应用。前提条件是轻应用已经注册并获得应用标识app\_ID、应用密钥app\_KEY和数据授权范围，即双方已建立信任和合作关系。而认证成功后通过返回的密钥字code和授权令牌token，轻应用可以获取授权的数据。

统一用户集成支持OAuth2.0国际标准协议与CAS单点登录，其对接流程具体如下：

1、由政府部门轻应用在用户的浏览器内发起调用操作，调用平台的授权接口，由用户的浏览器跳转至平台接口；

2、平台的授权接口，接收到由平台发起的用户授权请求，授权接口判断用户当前在平台的登录状态；

3、用户未登录时，浏览器跳转至平台登录界面，并引导用户进行登录操作，用户在平台的界面中输入用户名和密码；

4、 平台后台判断用户的用户名、密码是否正确，如果输入错误，则浏览器中弹出错误提示框，成功，则进入下一步；

5、 平台判断用户是否需要显示的进行授权操作，以下两种情况，不需要用户进行二次授权：

a) 如果平台用户在之前已经授权过，并且授权校验还在时间范围内；

b) 轻应用方和平台已达成互信协议，不需要进行用户授权；

6、 如果需要授权，平台将浏览器跳转至用户授权界面，在授权界面中告知轻应用将要获取的权限，并引导用户进行授权；

7、用户完成授权后，平台生成授权码code，并将浏览器重定向到轻应用的接口，告知授权成功；

8、 轻应用的后台，使用用户授权码，访问平台的token接口，用于获取用户唯一凭证token；

9、平台后台接收token获取请求后，判断用户授权码是否正确，如果鉴权成功，则返回用户唯一凭证token；

10、 轻应用使用用户唯一凭证token，获取用户个人信息。

* + - 1. 统一数据库服务

与“我的长沙”APP共享用户信息库、应用服务信息库等，保证基础信息一致，避免系统信息数据不对称导致的服务问题。

* + - 1. 用户信息库

实名认证信息库主要包含居民基本信息，是反映全市居民个人的人口学及社会经济学等特征的一组信息，记录内容相对稳定、客观性强，其中一些记录反映了个人固有特征且贯穿整个生命周期，是居民档案的重要组成部分。

* + - 1. 用户行为信息数据库

用户行为信息主要是指用户的操作信息，如用户在使用平台时产生的数据，如登录次数数据、登录时间数据，服务使用数据、服务使用频次数据等，通过对该数据的分析，为以后应用推广分析作支撑。

* + - 1. 积分数据服务库

积分数据服务主要是指对积分服务产生的数据进行统一的采集、检查、入库、更新。

* + - 1. 统一入口

“我的长沙APP-高新专区”依托在“我的长沙”统一入口之上，一键登录，避免二次登陆，服务以轻应用等方式呈现在“我的长沙APP-高新专区”，市民通过“我的长沙”APP切换区县频道，即可访问“我的长沙APP-高新专区”，并享受各项特色服务。

有用户体系的第三方应用，需和“我的长沙APP-高新专区”用户体系打通；包括但不限于以下逻辑：

1、“我的长沙APP-高新专区”的用户可直接访问该应用（使用平台账号）；不用再进行二次注册和登录，仅需通过授权模式，一站式访问。

2、在“我的长沙APP-高新专区”用户授权基础上，实现页面自动填表。（申请、预约、报名等应用）

3、“我的长沙APP-高新专区”用户的任何通知或状态信息以数据或回调页面方式返回给平台；由“我的长沙APP-高新专区”呈现给用户。具体模式视业务确定。

* + - 1. 企业登录接入及办理

通过与中台的接口对接，将企业登录接入“我的长沙”APP登录体系；企业如需办理企业业务，点击企业办事服务即可弹出企业登录框，企业账号可输入法人信息或公司信息即可完成企业登录，并办理与企业相关的服务事项。

流程如下(以“企业百事通”服务为例)：

1）普通用户点击进入到高新区，点击企业百事通，通过“我的长沙”APP个人用户登录体系进入到专区页面；

2）企业账号点击进入高新区，点击企业登录即可弹出企业登录弹框。

3）企业账号支持密码登录。如未注册过企业账号，则可以点击注册按钮进行注册。

4）企业账号注册需要填写完账号和密码之后，详细填写企业信息，最后再填写申请人信息，同时请求接口进行比对，比对信息无误。企业账号可点击下一步进行申请人人脸识别。

5）人脸识别成功，接口比对无误，则可完成企业账号注册。企业账号可进入直接进行企业办事服务办理。

* + - 1. 我的频道

1、电子证照服务

电子证照是时代信息化发展的必然趋势，通过电子信息化，将纸质文件、证照证明通过信息化的手段实现电子存档并直接显示在移动端，避免市民及法人在具体使用场景中随身携带大量纸质证明材料。目前“我的长沙”APP已上线身份证、驾驶证、行驶证、职业资格证道路运输证等21种电子证照和电子证明，且已在具体场景中使用，将推动市民办事无纸化，协助政府实现政务办事省时间、省材料、省环节。

电子证照服务面向全市市民提供，在我的频道中，高新区用户可直接选择添加、查看、删除个人电子证照信息。

2、我的钱包服务

服务提供个人数据银行和我的钱包服务，个人数据银行提供统一的个人数据查询入口，可汇聚整个APP使用过程中涉及到的个人数据信息，包括但不限于水电煤缴费记录、通信费缴费记录等。提供个性化的分类型、分日期查询，并提供月度报表，详单查询。汇总用户数据使用记录，让用户对自己的数据情况做到一目了然。

3、个人积分体系服务

个人积分体系与“我的长沙APP-高新专区”服务关联，引导用户点击“我的长沙APP-高新专区”服务增加个人积分，进一步促进专区活跃度。

提供具有本地特色的积分服务入口和完善的积分获取规则，积分等级设定规则，积分兑换规则等，利用完善的积分服务体系，鼓励用户积极参与到平台服务中来，增强用户活跃度与用户黏性，实现从新用户到高价值用户，从沉默用户到活跃用户的转变，利用积分及福利促进其成长，实现活跃用户精准定位。

### 3.1.2 UI设计

“我的长沙APP-高新区”首页的UI设计应基于高新区特色进行界面定制，如专区头部图片设计区别于“我的长沙”市级平台可采用实景大图加上三张图片轮播的方式，图片也采用具有高新区特色地标或景观等的高清图片；UI首页服务呈现方式可有三种方案1、短横线标识，2、高亮显示标识，3、高亮+长横线标识ICON设计也需结合高新区特色进行定制；服务超市呈现方式可有二种方案 1、上下结构，2、左右结构；高新区特色专区呈现方式可有二种方案1、左一右二，2、三个并列。

专属UI定制思路：UI设计主要考虑人机交互、操作逻辑、界面美观等方面，那么本区在考虑设计风格的时候，不仅要有个性有品位，还要让市民在操作上变得更舒适简单、自由。而在布局、导航、按钮、视图、图标等细节上会根据高新区独有的政务特色、园区特色等内容进行深层UI设计，打造出专属“我的长沙APP-高新区”风格的UI设计。

开发内容包括：首页框架定制开发、服务分列呈现开发、服务超市左右结构呈现定制开发、专区版面定制开发、资讯接口更新调试等。



### 3.1.2.1原型设计

产品的原型设计实现一般区分整体和局部，整体上考虑信息架构的设计，如功能结构、导航、菜单、布局排版等方面的，局部上考虑功能上的交互设计，如按钮点击、反馈、页面切换、局部模块的整体展示等。主要包括确定产品的整体结构，确定产品的排版布局，确定产品功能模块，确定功能模块实现的原理，对每个模块进行交互设计，交互效果测试。

### 3.1.2.2UI设计

UI设计需要负责美观、品牌风格、浏览体验、阅读体验等内容。这些基本以UI设计稿的形式来呈现，主要工作内容包含：版线框图、确定关键界面里的UI元素和布局，以及全局的布局排版风格。确定产品界面的视觉设计风格。完成全部界面的线框图（1:1的）设计，最终完成全部界面的UI视觉设计。

3.1.2.3页面开发

前端开发：将设计图制作为网页可用的格式，保障网页符合“我的长沙APP-高新专区”开发标准，与后端联调接口，保障页面功能正常使用。

程序开发：后端与第三方联调接口，将接口转化为符合“我的长沙APP-高新区”接入的标准接口，并与前端进行联调，保障接口使用正常。保障接入的功能正常使用。

### 3.1.3门户首服务

* + - 1. 首页-服务频道

#### 1定位

用户首次登录，定位到“长沙”，根据定位信息，若市民定位在长沙高新区，则提示市民是否切换到长沙高新区专区频道。

#### 2形象Banner图

提供长沙高新区形象banner位及后台配置管理服务平台实时更新，在主题风格上可围绕高新党政、司法、两会会议、政务等主题风格来展开展示，还可选择如麓谷、东方红、雷锋、白马、信息产业园各区域内元素来进行banner轮播。

#### 3智能推荐服务

依托人工智能及大数据技术，通过对区县用户标签及用户行为轨迹分析，依据区县服务超市，为用户提供智能的、个性化的独立服务推荐，将用户常用的、感兴趣的服务放到首页和可能即将用到的服务，展示在用户首页界面，为用户提供千人千面的服务，进一步做到想用户所想。

#### 4智能搜索服务

依托人工智能及大数据技术，通过对区县用户标签及用户搜索轨迹和历史查看信息分析，提供搜索热榜服务、搜索攻略服务、猜你喜欢搜索推荐服务、热门搜索服务、智能搜索标签库服务、搜索范围、搜索历史等，简化用户搜索操作。

#### 5市级服务下沉

“我的长沙”目前接入了丰富的市级服务项目，部分服务与长沙高新区居民生活息息相关，如公积金/社保服务、体育馆预约、电费缴纳、教育缴费、防汛抗旱专区等服务。此类服务可由“我的长沙”市级服务下沉到长沙高新区特色服务频道中，居民可通过长沙高新区特色服务频道便捷地享用市级服务。

#### 6便民消息栏

依托“我的长沙”APP智能推送服务，关联用户实名认证信息，通过个人消息栏提供用户个人相关信息推送服务，如账单信息、证照到期信息等，方便用户可以直接查看到个人有关服务信息情况。

#### 7长沙高新头条

通过长沙高新头条版块发布高新区级的相关新闻资讯，用户通过长沙高新区特色服务频道即可及时查询了解，方便区/市级重要信息公开。

可通过后台发布长沙高新区新闻资讯内容，在长沙高新区特色服务频道首页显示最新3条新闻资讯，且可左右滑动切换；点击资讯标题可进入新闻详情页面；通过该模块右上角“更多”按钮即可进入到新闻资讯列表页面。

#### 8走进长沙高新区

通过走进长沙高新区模块，为本地市民及外地游客，介绍长沙高新区概况、地理环境、人文历史等信息，让市民快速了解长沙高新区，在线为长沙高新区用户提供掌上长沙高新区直观感受。

#### 9园区领导信箱

提供用户与园区领导的互动沟通渠道，建立互动应用平台，园区领导可在移动端与公众对话交流，回复和解决用户关心的问题。改造后功能包括：

我要写信：包括诉求信息、联系方式、提交附件

我要投诉：包括投诉内容、联系方式、提交附件

信件列表：列表展示所有信件，支持信件查看、修改、回复；

同时提供满意度获取、信件状态管理、来信须知等功能。

1、首页接口数量统计

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | | 数量 |
| 1 | 高新区资讯 |  | 1 |
| 2 | 走进高新区 | 高新概况 | 1 |
| 历史沿革 | 1 |
| 经济发展 | 1 |
| 园区地图 | 1 |
| 联系我们 | 1 |
| 3 | 高新区定位 |  | 1 |
| 4 | 园区信箱 |  | 1 |
| 5 | 个人积分 |  | 1 |
| 合计 | | | 9 |

2、市级高频服务下沉接口数量统计

|  |  |  |
| --- | --- | --- |
| 一级分类 | 一级服务名称 | 接口 |
| 民生保障 | 社保服务 | 1 |
| 公积金 | 1 |
| 居住证 | 1 |
| 户口服务 | 1 |
| 交办与督办 | 1 |
| 人才办事 | 1 |
| 人才资讯 | 1 |
| 人才绿卡 | 1 |
| 工伤保险专区 | 1 |
| 电子社保卡 | 1 |
| 警务预约 | 1 |
| 交通出行 | 扫码乘车 | 1 |
| 机动车联系方式变更 | 1 |
| 机动车免检标准核发（省内） | 1 |
| 机动车免检标准核发（省外） | 1 |
| 驾驶证联系方式变更 | 1 |
| 注销驾驶证 | 1 |
| 核发驾驶人信用证明（3年无事故证明） | 1 |
| 申请驾驶证延期换证 | 1 |
| 申请驾驶人延期体检 | 1 |
| 实时路况 | 1 |
| 车检预约 | 1 |
| 城管理赔 | 1 |
| 快处直赔 | 1 |
| ETC办理点 | 1 |
| 汽车购票 | 1 |
| 交通从业资格证领取 | 1 |
| 医疗健康 | 预约挂号 | 1 |
| 医保服务 | 1 |
| 异地就医 | 1 |
| 养老机构 | 1 |
| 药具申领 | 1 |
| 生活服务 | 健康码 | 1 |
| 电费缴纳 | 1 |
| 燃气缴费 | 1 |
| 水费缴纳 | 1 |
| 有线电视 | 1 |
| 电信营业厅 | 1 |
| 联通营业厅 | 1 |
| 移动营业厅 | 1 |
| 不动产查询 | 1 |
| 物业维修金 | 1 |
| 预售许可证 | 1 |
| 商品房签订 | 1 |
| 商品房备案 | 1 |
| 隐患随手拍 | 1 |
| 便民公告 | 1 |
| 防疫专区 | 1 |
| 电力申办 | 1 |
| 垃圾分类 | 1 |
| 低保公示 | 1 |
| 证件照 | 1 |
| 残疾人服务 | 1 |
| 企业服务 | 通知公告 | 1 |
| 政策查询 | 1 |
| 会议培训 | 1 |
| 工业地产 | 1 |
| 产品供需 | 1 |
| 政策兑现 | 1 |
|  | 办事指南 | 1 |
|  | 金融服务 | 1 |
|  | 企业查询 | 1 |
|  | 麓谷指尖办（特色专区） | 1 |
|  | 企业百事通（特色专区） | 1 |
|  | 麓谷人才（特色专区） | 1 |
|  | 企业创新积分（特色专区） | 1 |
|  | 健康伴我行（特色专区） | 1 |
| 合计 | | 67 |

### 3.1.4高新区特色专区建设

一期建设内容主要聚焦政府服务和公共服务等便民服务，让高新区企业能通过“我的长沙APP-高新专区”的建设实时感受到政府信息化带来的福利，提高市民智慧生活的获得感，市民生活变得更加便捷、灵活，从而提高用户活跃度与用户粘性。一期建设专区上线服务包含自然资源局专区、行政执法局专区和文化旅游广电体育局专区三个专区。其中自然资源局专区、文化旅游广电体育局专区采用第三方H5应用入驻模式，行政执法局专区采用接口对接入驻模式。第一期建设不涉及定制开发应用服务系统。

“我的长沙APP-高新专区”服务入驻模式分为二种：

1、模式一：我的长沙App提供第三方H5应用入驻：

涉及用户的服务，需要做用户打通，联系平台技术对接人，获取应用appKey后，调用账户接口获取账户信息。

查询、资讯等不需要用户信息的服务，页面应用地址直接提给平台技术人员即可。

2、模式二：接口对接：

根据业务需求进行梳理，由自建业务系统提供接口文档，“我的长沙APP-高新专区”团队根据接口要求进行相关页面开发。

网络要求：市政务外网或互联网。

* + 1. 1. 高新政务服务“指尖办”专区

政务服务“指尖办”服务（长沙高新区特色政务服务一体化平台及智慧政务大厅项目所提供的政务服务内容）将以H5方式接入“我的长沙高新”专区。该专区内将上线长沙高新区可移动办事项（最终上线事项及数量以区行政审批局提供的为准），市民可实现在线预约、申报、办理等服务，大大优化市民办事的流程及体验，真正实现“数据多跑腿，群众少跑路”的政务服务宗旨。

1、麓谷指尖办专区页面统计

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 页面数量 |
| 1 | 基础模块 | 77 |
| 2 | 基础组件模块 | 17 |
| 3 | 个人中心模块 | 2 |
| 4 | 企业模块 | 7 |
| 5 | 公共错误模块 | 1 |
| 6 | 帮扶模块 | 7 |
| 7 | 工业地产模块 | 5 |
| 8 | 问题模块 | 3 |
| 9 | 管理模块 | 60 |
| 10 | 会议模块 | 5 |
| 11 | 消息模块 | 2 |
| 12 | 通知消息模块 | 2 |
| 13 | 通讯录模块 | 2 |
| 14 | 政策兑现模块 | 13 |
| 15 | 日程模块 | 2 |
| 16 | 公共查询模块 | 1 |
| 17 | 服务项目模块 | 2 |
| 18 | 短信模块 | 2 |
| 合计 | | 210 |

* + - 1. 企业百事通板块

通过企业模块、帮扶模块、问题模块、消息模块、通讯录模块、政策兑现模块、公共查询模块等功能，实现全区各职能部门和专业化服务机构在资金、信息、技术、人才、项目等资源要素方面实现便捷流动和共用共享，帮助园区企业整合信息与资源，从而低成本、高效率地解决政策、办事、融资、人才、管理的提升和产业转型升级，不断促进优化园区的政务环境、经营环境、法治环境和政商环境。

1、企业百事通专区页面统计

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **页面数量** |
| 1 | 基础模块 | 77 |
| 2 | 基础组件模块 | 17 |
| 3 | 个人中心模块 | 2 |
| 4 | 企业模块 | 7 |
| 5 | 公共错误模块 | 1 |
| 6 | 帮扶模块 | 7 |
| 7 | 工业地产模块 | 5 |
| 8 | 问题模块 | 3 |
| 9 | 管理模块 | 60 |
| 10 | 会议模块 | 5 |
| 11 | 消息模块 | 2 |
| 12 | 通知消息模块 | 2 |
| 13 | 通讯录模块 | 2 |
| 14 | 政策兑现模块 | 13 |
| 15 | 日程模块 | 2 |
| 16 | 公共查询模块 | 1 |
| 17 | 服务项目模块 | 2 |
| 18 | 短信模块 | 2 |
|  | 合计 | 210 |

* + - 1. 企业创新积分专区

以科技创新办公室“创业积分制小程序”作为服务能力提供方，通过H5的方式，接入“我的长沙高新”专区。向社会公众提供查询、展示以及创新榜单发布等功能。主要功能为客观呈现园区企业的科技创新能力，由园区各对口管理部门对企业进行评分，对于优质企业由园区牵头提供金融信贷、政策推荐、项目推荐等扶持服务。

1、企业创新积分专区页面统计

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **页面数量** |
| 1 | 首页展示 | 1 |
| 2 | 统一认证 | 1 |
| 3 | 积分查询 | 1 |
| 4 | 企业详情信息 | 1 |
| 5 | 历史积分查询 | 1 |
| 6 | 金融超市列表展示 | 1 |
| 7 | 金融超市详情展示 | 1 |
| 8 | 我的政策列表展示 | 1 |
| 9 | 我的政策详情展示 | 1 |
| 10 | 我的政策附件查看 | 1 |
| 11 | 我的政策附件下载 | 1 |
| 12 | 积分政策列表展示 | 1 |
| 13 | 积分政策详情展示 | 1 |
| 14 | 积分政策附件查看 | 1 |
| 15 | 积分政策附件下载 | 1 |
| 16 | 个人资料展示 | 1 |
| 17 | 个人资料修改-手机验证 | 1 |
| 18 | 个人资料修改-电子邮箱修改 | 1 |
| 19 | 解除绑定 | 1 |
| 20 | 创新积分搜索 | 1 |
| 21 | 创新积分重置 | 1 |
| 22 | 创新积分分析 | 1 |
| 23 | 单项积分查询 | 1 |
| 24 | 单项积分筛选 | 1 |
| 25 | 历史积分查询 | 1 |
| 26 | 积分政策详情 | 1 |
| 27 | 积分政策附件查看 | 1 |
| 28 | 积分政策附件下载 | 1 |
| 29 | 个人资料展示 | 1 |
| 30 | 个人资料修改-手机验证 | 1 |
| 31 | 个人资料修改-电子邮箱修改 | 1 |
| 32 | 个人资料修改-联系人修改 | 1 |
| 33 | 个人资料修改-职能部门选择 | 1 |
| 34 | 个人资料修改-职务选择 | 1 |
| 合计 | | 34 |

* + - 1. 健康伴我行专区

以“健康伴我行”微信公众号作为服务能力提供方，通过H5的方式，接入相关服务。提供基层医疗机构、医生宣传窗口；开展机构的线上健康教育服务；提供居民家庭医生签约，线上预约，报告查询等服务。基层卫生机构能够快速、便捷的搭建专属自己的移动互联网应用门户，为社区（村）居民打造可信、可及的“O2O”健康服务模式。

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **页面数量** |
| **1** | 医院列表 | 1 |
| **2** | 医院详情 | 1 |
| **3** | 科室信息 | 1 |
| **4** | 机构导航 | 1 |
| **5** | 医生列表 | 2 |
| **6** | 医生简介 | 2 |
| **7** | 医生评价 | 2 |
| **8** | 关注医生 | 2 |
| **9** | 在线预约 | 12 |
| **10** | 新冠疫苗接种 | 12 |
| **11** | 专家预约 | 12 |
| **12** | 预约取消 | 4 |
| **13** | 签到取号 | 4 |
| **14** | 我的预约 | 6 |
| **15** | 预约提醒 | 1 |
| **16** | 健康日报 | 3 |
| **17** | 微讲座 | 20 |
| **18** | 健教宣教 | 3 |
| **19** | 通知消息 | 2 |
| **20** | 文章通告 | 2 |
| **21** | 商品列表 | 2 |
| **22** | 商品支付 | 3 |
| **23** | 订单查询 | 2 |
| **24** | 报告查询 | 3 |
| **25** | 个人信息维护 | 3 |
| **26** | 家庭成员管理 | 3 |
| **27** | 我的预约 | 2 |
| **28** | 我的订单 | 2 |
| **29** | 我的社区医院 | 2 |
| **30** | 我关注的医生 | 2 |
| **31** | 我的健康历程 | 2 |
| **32** | 家医签约 | 4 |
| **33** | VIP增值服务 | 2 |
| **34** | 黑名单列表 | 2 |
| **35** | 黑名单解冻 | 2 |
| **36** | 计免查验证 | 3 |
| **37** | 母子健康手册申领 | 3 |
|  | 合计 | 135 |

* + - 1. 高新人才专区

以“长沙高新区人才网”作为服务能力提供方，通过H5方式，接入相关服务。包含现场招聘发布、网上招聘发布、求职入口（招聘月活动）、公共服务（资讯发布）等功能。依托高新区人才网积极开展线上对接服务，做好“六稳”工作、落实“六保”等具体工作，保障企业复工复产，为企业和高校毕业生搭建人才交流平台，变线下招聘会为线上招聘会。

|  |  |  |
| --- | --- | --- |
| **序号** | **子功能** | **调整页面数** |
| **1** | **登录** | **1** |
| **2** | **注册** | **1** |
| **3** | **关键指标** | **4** |
| **4** | **面试安排** | **1** |
| **5** | **人才推荐** | **1** |
| **6** | **应聘简历** | **4** |
| **7** | **已收藏简历** | **1** |
| **8** | **简历回收站** | **1** |
| **9** | **应聘职位，薪资范围，更多** | **3** |
| **10** | **招聘大会厅** | **2** |
| **11** | **职位管理** | **1** |
| **12** | **发布管理** | **1** |
| **13** | **邀投递** | **1** |
| **14** | **简历搜索** | **1** |
| **15** | **修改资料** | **1** |
| **16** | **搜索** | **1** |
| **17** | **职能，薪资，更多(功能)** | **1** |
| **18** | **列表展示** | **1** |
| **19** | **职位详情** | **3** |
| **20** | **公司详情** | **1** |
| **21** | **消息** | **2** |
| **22** | **看过我** | **1** |
| **23** | **在线简历** | **1** |
| **24** | **我的申请** | **1** |
| **25** | **我的收藏** | **1** |
| **26** | **简历附件** | **1** |
| **27** | **隐私设置** | **1** |
| **28** | **修改密码** | **1** |
| **29** | **退出** | **1** |
| **30** | **招聘会** | **1** |
| **31** | **招聘会大厅** | **2** |
| **32** | **创建简历** | **1** |
| **33** | **我的投递** | **1** |
|  | **合计** | **46** |

## 3.2运维服务

项目验收后三年提供一站式售后维护整体服务，以优质的运行维护服务、快速到位的故障响应、及时可靠的支撑保障，确保系统及应用可靠运行，保障“我的长沙APP-高新专区”的长效运行。

本项目不涉及硬件运维。

运维人员安排：

|  |  |  |
| --- | --- | --- |
| **服务名称** | **人员安排** | **具体工作** |
| 运维服务（三年） | 维护管理员（1人） | 维护工作的总协调，负责接受维护申请并与其他人员进行沟通。 |
| 维护负责人（1人） | 修改控制决策机构，管理整个运维团队。 |
| 系统监督员（1人） | 编制维护报告，对当前维护情况作出评价，并上报至维护负责人。 |
| 配置管理员（1人） | 负责和分析程序的维护要求并且进行程序的修改工作，根据市级平台服务接入情况，分析判断需要下沉至高新专区的服务 |
| 每天安排专人对专区进行对系统的使用情况进行了解并进行常规性检查、调试和清理工作，记录系统的运行情况。 |
| 维护工程师 （3人） | 7\*24小时远程或者现场故障诊断，快速定位故障原因及处理。平台如发生故障可提供1名工程师现场服务，可提供4名二线工程师远程技术支持。 |
| 平台升级、市级高频服务下沉接入及完善 |

### 3.2.1响应处理

运维人员平时应做好应急事件的监控工作，对于突发事件应认真分析、准确判定故障发生的数据域，负责跟踪该事件直至其结束。事后做好文档登记工作上报领导。

正常情况下，要求运维人员在10分钟内进行事件确认。如果属于一般事件则按照事件流程进行分派处理，否则应迅速启动《应急预案》，并严格按照《应急预案》所规定的步骤快速实施应急处置，及时汇报上级领导，掌握实时处理情况。

在处理过程中，如需其他部门配合，应及时向上级领导部门汇报，协调沟通，尽快联系相关人员进行援助处理。

### 3.2.2服务完善

“我的长沙”目前接入了丰富的市级服务项目，部分服务与高新区企业办事息息相关，如如麓谷之间办、企业百事通、企业创新积分、健康伴我行、麓谷人才等专区服务等服务。此类服务高新区的特色服务，企业办事人员可通过“我的长沙APP-高新专区”便捷地享用市级服务。平台会对市级下沉的服务不断接入与完善，为市民提供更多优质的市级服务。

### 3.2.3性能提升

针对系统可靠性、用户并发指数、平台响应时间三个方面进行性能稳定维护与提升，保障“我的长沙APP-高新专区”稳定、长效运行。

### 3.2.4服务故障检测

提供人工巡检和智能自动巡检两种方式，检测“我的长沙APP-高新专区”所提供服务是否存在故障。

### 3.2.5故障受理处理

根据平台发生的故障现象，提供远程或者现场故障诊断，快速定位故障原因；

对故障进行应急处理：采取各种措施尽可能先快速恢复业务，再进一步解决具体故障；

记录故障原因、处理情况、故障历时，并向客户提供故障处理报告；

故障升级管理：在故障管理服务中，按照职能、层次分别进行升级；

安排1名工程师可提供现场服务，安排4名二线工程师可提供远程技术支持，提供快速及时的“我的长沙APP-高新专区”故障受理响应及处理服务；

服务时间：7\*24小时

故障管理时间指标承诺

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 故障类型 | 区域范围 | 支持方式 | 响应要求 | 修复时间 |
| 系统严重故障、部分重要服务不正常 | 本平台范围内应用 | 远程、现场 | 30分钟 | 2小时 |
| 系统个别服务不正常 | 本平台范围内应用 | 远程、现场 | 60分钟 | 24小时 |

### 3.2.6应急措施

|  |  |  |
| --- | --- | --- |
| 故障级别 | 响应时间 | 故障排除及系统恢复时间 |
| 一级：重大故障。系统瘫痪，数据丢失。 | 0.5小时 | 2小时 |
| 二级：部分设备故障。部分设备工作不正常，影响和限制了部分的正常使用。 | 1小时 | 12小时 |
| 三级：一般性技术故障。 | 4小时 | 24小时 |

突发事件是指系统运行过程中突然出现的造成服务中断或服务质量下降的突发现象，突发事件的处理目标是尽可能地快速的处理事故，恢复IT资源的正常运行，避免业务中断，使事故对业务运营的影响降至最低，以保证IT资源的可用性水平与保持IT运维的最佳服务水平。

当突发事件出现是，根据运行维护管理方案中的应急方案，首先对事件进行记录，然后经过分类和初步的支持、调查与诊断试图进行故障解决和恢复，直到解决后与客户确认进行事件的关闭。如果某一事件在规定的时间内不能由一线支持小组解决，则需要对事件进行升级，让更多有经验的人员和有更高权限的人员将参与进来。

突发事件的处理过程中，事件记录员负责事件的记录并寻找相应的人员对事件进行分析处理以及后续的事件跟踪和编写事件分析报告；事件分析员对突发事件进行分析解决，并反馈事件产生的原因以及解决办法。

按照故障等级进行分级，针对不同的故障等级要求运维单位进行分级响应。

维护单位提供服务报修专线，提供7X24服务。

# 非功能性需求

## 性能需求

“我的长沙”平台按照信息系统安全等级保护三级标准进行设计建设。充分考虑应用层的安全性，做好信息资源的访问控制；系统应能够提供用户权限配置及用户操作审计控制。

（1）系统定级和关键信息基础设施评估要求

信息系统应在设计之初，依据信息系统安全等级保护定级指南，确定定级对象，分别确定定级对象的系统服务和业务信息的安全保护等级，进而确定定级对象的安全等级。初步评估建设对象是否可能为关键信息基础设施。

（2）信息系统安全功能设计要求

信息系统在进行功能设计时应包括身份认证、权限管理、安全审计、交互安全、数据分类、数据传输和存储安全等功能，为应用系统提供安全服务。

权限管理功能：对系统用户进行权限管理，为相关职能部门以及各级机构提供权限内服务；

安全审计功能：记录用户操作业务系统与安全相关的行为和操作数据，形成审计记录，保留不少于6个月的时限以供审查。并通过实现对审计记录的分析，实现快速准确定位业务系统的安全状态；

交互安全功能：应用系统应对人机交互及系统间调用接口实现安全保护等。

数据分类功能：对数据不同类别进行标记，并进行相应保护；

数据传输和存储安全功能：对重要数据和个人信息进行非明文传输和存储保护。

（3）信息系统源代码编码安全要求

信息系统应在设计、开发阶段遵循源代码安全要求，包括对输入校验、输出编码、会话管理、文件系统访问、数据传输及存储、异常处理和代码注释等进行规范。

（4）数据保护要求

系统关键信息应在应用程序中实现用户真实身份信息的验证和内容审核流程的功能开发，并对关键业务数据进行分类、加密、脱敏、封装和关联性隔离以及容灾备份等，保障数据在产生、传输、处置和存储等流程中的真实性、完整性、保密性。

（5）部署运行安全要求

应当依据国家有关法规、政策及标准要求，针对网络结构、服务器操作系统、数据库系统等领域进行安全防护设计、选型和实施，做到网络结构清晰；网络边界、安全域边界、业务边界隔离防护合理、措施有效；操作系统、数据库等关键设施自身安全防护可达到信息系统相应等级的安全要求等。

应在信息系统的设计、建设实施等工作开展中形成并不断完善系统安全规划、实施、运行方案，对信息系统的部署、使用、应急响应及恢复处置等过程进行详细规定。

（6）安全测评

应开展信息化工程竣工验收时的安全验收测评（含源代码安全审查）、软件验收测评和安全等级测评。

### 系统稳定指标

系统总体可用率>99.9%，数据库应用可用率>=99.9%，可用率>=99.9%。（或7×24小时不间断运行）

### 性能及资源指标

需求规格方案在继承与融合了初步设计方案，在性能指标方面表现在PV响应时间、页面响应时间、用户简单/复杂查询，系统响应速度、服务器并发次数等参数的一致性。详细情况如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 业务类别 | 平均时间/百分比 | 最大时间/百分比 | 备注 |
| PV响应 | 1-3s | <5s | 无 |
| 页面响应 | 1-3s | <5s | 无 |
| 用户简单事物查询 | ≤3s | <5s | 无 |
| 复杂事务处理 | ≤10s | 用户操作时间时长有关 | 用户实名审核、用户实名状态变更、用户办事预约 |
| 第三方业务 | ≤5s | 第三方网络与服务有关 | 支付宝登录、微信登录、服务集成等涉及第三方网络交互的操作 |
| 地图查询 | 1-3s | <5s |  |
| 系统响应速度 | <20% |  | 在非硬件系统问题的情况下，数据量对软件系统响应速度百分比 |
| 服务器并发 | 总量20000 |  |  |
| 网络性能需求 | 网络响应时间的要求 | 网络可靠性的要求 | 网络恢复时间的要求 |
| ≤40ms | 7\*24 | 30分钟内完成核心网络的恢复，1小时内恢复整体网络 |
| 灾备需求类别 | 容灾指标目标 | 备注 |  |
| 服务器备份 | 每日镜像备份系统 | 无 |  |
| 灾备恢复时间 | 整体恢复时间应小于1小时 | 由于自然灾害等不可抗因素导致的服务器损毁等严重灾害，整体恢复时间应小于1天 |  |

表 4.1.2‑1系统性能分析表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系统日志存储空间需求 | 服务数量/人 | 日志/人/天 | 保存时间 | 日志总量 | 日志备份冗余50%计算 |
| 500项 | 50MB | 12个月 | 8TB | 4TB |
| 操作系统存储空间需求 | 服务器数量 | 硬盘空间 | 磁盘空间总量 |  |  |
| 40-50/台 | 100GB | 4TB |  |  |
| 存储空间总计: 8T + 4T + 4T = 16TB | | | | | |

系统容量分析表

### 灵活性

为保证系统的灵活性，从以下几个方面做有针对性的个性化处理：

1、实现各项功能的完全的可配置；

2、预留接口充分，可方便的添加新功能；

3、功能模块的组件化，各模块有清晰的边界，每个模块编译为程序集，可自由组合；

4、同其他软件接口的对接在设计上是采取的网关模式，如果接口发生变化，只需少量调整并重启网关服务，不影响主服务的正常运行；

5、及时收集当前版本问题以及新需求，定期对产品进行优化。

### 精度

当通过互联网接入系统的时候，期望被监督单位名称搜索或者其他搜索最长查询时间<15 秒。计算的精确性到小数点后 7 位。

## 安全保障体系需求

根据国家标准《信息安全技术-网络安全等级保护基本要求》GB/T 22239-2019）有关要求，我的长沙-城市移动综合服务平台按照网络安全等级保护基本要求中的第三级标准进行建设，本项目部署在长沙市“政务云”平台软硬件基础平台之上，项目的管理安全、基础设施安全、应用安全、业务安全等，满足本项目信息安全的各项要求。不属于本项目的建设范畴。

### 隐私保护设计

#### 密码策略

密码采用不可逆算法加密后存储再数据库，同时加盐计算，保证密码数据的安全性，即使能获取数据，也无法反加密得到密码，最大限度保障密码数据安全。

同时APP端密码设置支持两种模式设置：

1、密码强度限制为：大小写字母、数字、特殊符号至少四选三，长度为8～16位；

2、密码强度限制为：字母、数字、特殊符号至少三选二，长度6～16位。

#### 接口加密

统一对数据接口进行加密签名，签名算法主要使用以下几个字段：

1、x-tif-timestamp：当前时间unix 时间戳，精确到秒

2、x-tif-nonce：由调用者/被调用者/网关生成的非重复的随机字符串（十分钟内不能重复）

3、Token：创建应用时分配的加密密钥。

#### 签名算法：

1. x-tif-signature = sha256(x-tif-timestamp + Token + x-tif-nonce + x-tif-timestamp)
2. 签名字符串签名算法说明如下：

package main

import (

"crypto/sha256"

"fmt"

"log"

"strconv"

"strings"

"time"

)

func checkSign(secret, timestamp, nonce, sign string) bool {

ts, \_ := strconv.ParseInt(timestamp, 10, 64)

// 如果请求头时间与当前时间相差超过180秒，则认为请求不合法(结合x-tif-nonce，可以防止请求重放)

now := time.Now().Unix()

if ts > now+180 || ts < now-180 {

log.Printf("time expired")

return false

}

signData := fmt.Sprintf("%s%s%s%s", timestamp, secret, nonce, timestamp)

log.Printf("signdata: %s", signData)

res := strings.ToUpper(fmt.Sprintf("%x", sha256.Sum256([]byte(signData))))

log.Printf("signres: %s", res)

return res == sign

}

func main() {

secret := "Nu4WmXGBauU99NsNuwXjbV7hO2xwEef91Rp9rKX6WatcmiwWqXyk"

headerTimestamp := "1523340394"

headerSeq := "ab570e0a:015a1d0fbef0:00cb3d"

headerSign := "B6CD9D9377EDB58CA445B4A6A753F884C156DBD6344F058E7B88658E9AF54F71"

if checkSign(secret, headerTimestamp, headerNonce, headerSign) {

log.Printf("sign successs")

}

}

#### 授权模式

1、授权机制

用户授权采用OAuth2.0授权机制，OAuth2.0是目前安全的流行的授权机制，用来授权第三方应用，用户数据所有者告诉系统，同意授权第三方应用进入系统，才能获取这些数据，系统从而产生一个短期的进入令牌（token），用来代替密码，供第三方应用使用。

2、令牌与密码

令牌（token）与密码（password）的作用是一样的，都可以进入系统，令牌特点

令牌是短期的，到期会自动失效，用户自己无法修改

令牌可以被数据所有者撤销，会立即失效

令牌有权限范围（scope）

上面这些设计，保证了令牌既可以让第三方应用获得权限，同时又随时可控，不会危及系统安全。

#### 等保测评

委托三方机构做等保测评，标准等保三级。



### 安全设计目标

我的长沙-城市移动综合服务平台我的长沙-城市移动综合服务平台的信息系统安全，是构成信息系统的组件、环境和人（用户和管理者）的物理安全、网络安全、系统安全、数据安全、信息内容安全、信息基础设施安全的总和，其安全目标可以概括为保护信息资源价值不受侵犯，保证信息资产的拥有者面临最小的风险和获取最大的安全利益，使我的长沙-城市移动综合服务平台的信息基础设施、信息应用服务和信息内容为抵御安全威胁而具有安全性、完整性、真实性、可用性和可控性的能力。

网络安全设计的目标具体表现为：

1、网络的可用性

网络是业务系统的载体，安全防护系统必须保证网络的持续有效的运行，防止对网络设施的入侵和攻击、防止通过消耗带宽等方式破坏网络的可用性。

2、业务系统的可用性

各主机、数据库、应用服务器系统的安全运行同样十分关键，安全防护系统必须保证这些系统不会遭受来自网络的非法访问、恶意入侵和破坏。

3、访问的可控性

对关键网络、系统和数据的访问必须得到有效的控制，这要求系统能够可靠确认访问者的身份，谨慎授权，并对任何访问进行跟踪记录。

4、网络操作的可管理性

对于网络安全系统应具备审记和日志功能，对相关重要操作提供可靠而方便的可管理和维护功能。

5、网络行为的可控性

对内部人员和用户的网络行为进行有效监控，防止危险的网络操作对信息系统的破坏，规范网络行为，防止关键信息泄漏和访问发布不良信息。

6、安全体系的完整性

信息安全体系包括技术体系、运行体系和管理系统，只有完整的安全体系才能有效的防范安全风险，保证业务安全运行。

### 安全风险分析

信息安全风险是指在信息化[建设](https://baike.baidu.com/item/%E5%BB%BA%E8%AE%BE/32776" \t "_blank)中，各类应用系统及其赖以运行的基础网络、处理的数据和信息，由于其可能存在的软硬件缺陷、系统集成缺陷等，以及信息安全管理中潜在的薄弱环节，而导致的不同程度的安全风险。目前我的长沙-城市移动综合服务平台中可能存在的主要安全风险如下：

1、物理环境故障

由于断电、静电、灰尘、潮湿、温度、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害造成整个信息系统崩溃、数据丢失。

2、软硬件故障

由于设备硬件故障、通讯链路中断、系统本身或软件Bug导致对业务高效稳定运行的影响。

3、无作为或者操作失误

由于应该执行而没有执行相应的操作，或无意地执行了错误的操作，对系统造成影响。

4、管理不到位

安全管理不到位，造成安全管理不规范，或者管理混乱，从而破坏计算机系统正常有序运行。

5、恶意代码和病毒

计算机病毒泛滥，计算机系统一旦受到病毒的入侵，轻则运行效率下降，重则系统崩溃、重要数据丢失，甚至还有可能造成网络系统瘫痪。

6、黑客攻击技术

利用黑客工具和技术，例如侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对计算机系统进行攻击和入侵。黑客攻击越来越猖獗，网络安全问题也变得越来越严峻。

7、越权或滥用

通过采用一些措施，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏计算机系统的行为。譬如：

非法用户进入网络或系统进行非法操作；

冒充合法用户欺骗系统，占用合法用户资源；

合法用户以未授权方式进行非法操作；

合法用户不正常访问网络资源；

假冒网络控制程序，套取或修改使用权限、密钥等信息，越权使用网络的设备和资源。

8、物理攻击

物理接触、物理破坏、盗窃。

9、泄密、篡改

通过公网线路截获信息数据，造成数据泄密、数据被篡改。

通过篡改、删除、插入等手段改变用户信息数据，破坏数据完整性。

10、缺少审计机制

系统管理员、数据库管理员在关键服务器上的行为及用户对关键服务器的访问缺乏审计机制导致。

### 安全管理保障

#### 开放接口的安全防护

数据交换和信息共享是得以发挥作用乃至正常运转的核心能力。任何数据交换和信息共享过程都会对系统的安全性带来影响。应采取有针对性的安全措施，完善开放接口的安全防护能力，对数据交换和信息共享环节给予端到端的全过程监控，及时发现和解决问题隐患，以确保关键业务正常运转。

#### 重要数据的保障

加强平台中各类信息、个人隐私等重要数据的安全防护，建立数据安全规范。在系统后台对每类数据的安全属性进行必要的定义和设置，详细规定数据的开放范围和开放力度，并严格执行相应的权限管理。

#### 安全策略和管理制度

应制定完善的管理制度和完备的安全管理措施，定期对管理制度和管理措施进行评审修订，确保管理制度和管理措施持续符合相关安全要求。安全策略和管理制度具体内容和要求如下：

1、安全策略

制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

2、管理制度

（1）对安全管理活动中的各类管理内容建立安全管理制度；

（2） 要求管理人员或操作人员执行的日常管理操作建立操作规程；

（3）形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。

3、制定和发布

（1）指定或授权专门的部门或人员负责安全管理制度的制定；

（2）安全管理制度应通过正式、有效的方式发布，并进行版本控制。

4、评审和修订

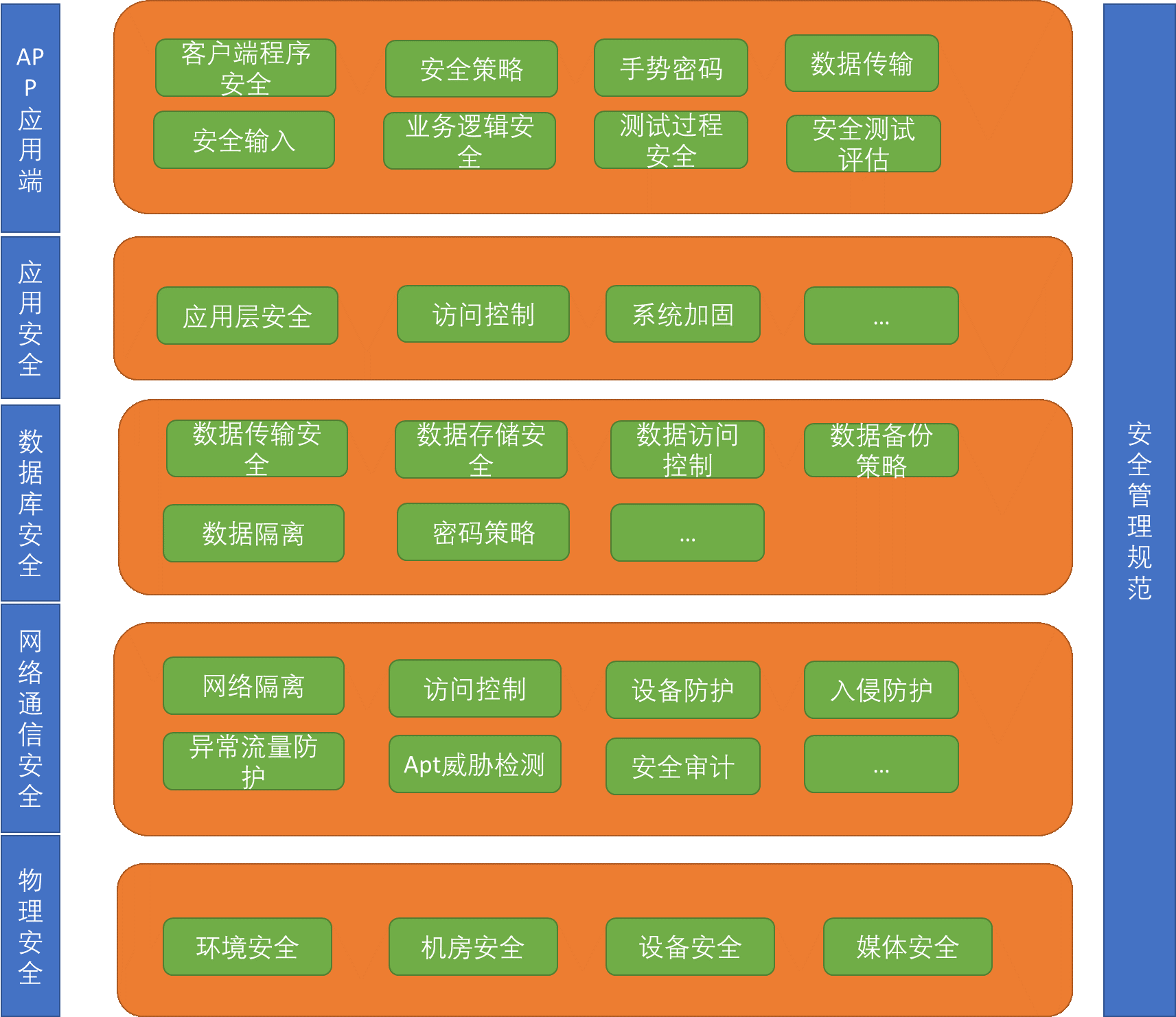
应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

#### 安全管理机构和人员

应当建立信息安全决策机构、执行机构，配备相应数量的安全管理人员，明确用户安全责任，且持续进行教育培训。在人员配备时，应当对关键事务岗位配备专职人员进行管理，专职安全管理员不可兼任。获得系统访问权限的外部人员应签署保密协议，不得进行非授权操作。

### 安全技术方案

我的长沙-城市移动综合服务平台存在被攻击、数据被损坏等潜在安全威胁，基础设施安全方案依托政务云实现，包括物理安全、设备和计算安全、网络和通信安全，应用安全方案由本项目设计，包括APP软件安全开发、应用安全设计和数据安全设计。针对行业及应用特点，通过对可能遇到的各种安全威胁和风险的分析，为保证信息的完整性、高可用性和抗抵赖性，需要建立一套完善的安全体系，确保该信息系统能够安全、稳定、可靠地运行。



安全防护体系图

#### APP软件安全开发

##### 客户端程序安全

针对移动客户端的安全检测，依据客户端安全测试规范为指导原则，对客户端进行有针对性的安全评估，发现客户端的安全缺陷并提出整改建议，保证客户端的安全性，防止敏感信息泄漏和其他安全问题。

1. 安装包签名

移动应用安装包进行正确签名，并且在安装应用时对签名进行校验，签名异常时禁止安装。

1. 完整性检测

移动应用安装时对安装包进行完整性校验，当检测到安装包被修改时禁止安装；移动应用启动时进行检测，当检测到移动应用自身遭到修改时，提示并退出。

1. 反编译保护

将代码进行混淆，使用技术手段对安装包进行保护，防止被反编译。

1. 运行环境检测

对于已root或越狱环境做出相应风险提示，必要时可退出运行。

1. 组件安全

严格控制对组件的访问、操作。

1. 系统日志

移动应用运行过程中涉及的敏感信息，不以明文或简单加密（单纯散列、哈希）形式出现在系统日志中。

##### 安全策略

1. 密码策略

密码策略设置为：长度至少8位，数字、大小写字母、符号至少四选二；密码强度在服务端做判断；修改密码、找回密码时对用户身份做校验。

1. 防暴力破解

移动应用严格设置限制策略，使其能防范暴力破解攻击。

1. 会话安全

移动应用在超过一定时间无操作后，提示退出登录状态或设置其他身份鉴别机制；移动应用在确保用户注销、登出后，会话被终止。

1. 敏感信息清除

在应用中填写的敏感信息，如果用户切出移动应用，清除填写的相关信息。

1. UI信息泄漏

移动应用对登录时错误的用户名、密码做出相同提示；移动应用中敏感信息部分做出隐藏或部分隐藏。

1. 图片验证码安全策略

移动应用在使用图形验证码时，验证码由服务器生成；具有有效时间并仅能使用一次。

1. 短信验证码安全策略

移动应用在使用短信验证码时，在服务端做校验；短信验证码至少设置6位，并设置有效时间；在服务端设置短信验证码获取频率、次数限制。

1. 登录限制

移动应用限制多终端同时登录，或在多终端同时登录时做出明显的风险提示。

##### 手势密码

移动应用使用手势密码时，手势密码至少包含四个点；

1、用户使用取消、修改、忘记手势密码功能时需要进行身份验证。

2、手势密码设置锁定策略。

3、手势密码不使用明文或简单加密（单纯做散列、哈希）存储在本地。

4、建议使用服务端验证。

##### 数据传输

1. 通讯加密

使用HTTPS加密传输，双向严格校验证书。

1. 数据保密性

移动应用在传输数据时，对敏感信息进行加密。

1. 版本更新

移动应用自动更新时，采取相关防护手段防止更新包被替换。

##### 安全输入

键盘使用随机键盘，重新激活输入框时对键盘重新随机化，禁止截屏。

##### 业务逻辑安全

1. 重放攻击

对敏感操作进行验证，防止数据包篡改、重放造成的攻击。

1. 越权操作

设置严格验证机制，防止通过修改参数造成的跨账户、跨权限操作。

##### 测试过程安全

不使用生产环境数据进行安全测试;，移动应用上线发布前，删除用于调试的代码。

##### 安全测试评估

测试分类 测试项目 测试内容。

客户端程序安全 安装包签名 测试客户端是否经过正确签名（正常情况下应用都应该是签名的，否则无法安装）。

反编译保护 测试客户端安装程序，判断是否能反编译为源代码，是否存在代码保护措施。

完整性检测 测试客户端程序是否在启动和更新时应进行真实性和完整性校验，防范客户端程序被篡改或替换。

敏感信息安全 文件权限检查 测试应用私有目录下的文件权限是否合理。

数据文件 检查数据文件中是否有敏感信息。

系统日志 检查客户端程序存储在手机中的日志。

安全策略 口令策略 测试客户端程序是否检查用户输入的密码强度，禁止用户设置弱口令。

帐号登录限制 测试一个帐号是否可以同时在多个设备上成功登录客户端，进行操作。

帐户锁定策略 测试客户端是否限制登录尝试次数。防止木马使用穷举法暴力破解用户密码。

会话安全设置 测试客户端是否在一段时间未操作后会话超时并要求重新登录，超时时间设置是否合理。

界面切换保护 检查客户端程序在切换到其他应用时，已经填写的账号密码等敏感信息是否会清空，防止用户敏感信息泄露。如果切换前处于已登录状态，切换后一定时间内是否会自动退出当前会话。

安全退出 测试客户端退出时是否正常终止会话。

密码修改验证 测试客户端在修改密码时是否验证旧密码正确性。

通信安全 通信加密 测试客户端和服务端通信是否采用https加密。

证书有效性检测 测试客户端程序和服务器端SSL通信是否严格检查服务器端证书有效性。避免手机银行用户受到SSL中间人攻击后，密码等敏感信息被嗅探到。

关键数据加密和校验 测试客户端程序提交数据给服务端时，密码、收款人信息等关键字段是否进行了加密，防止恶意用户嗅探到用户数据包中的密码等敏感信息。

业务功能测试 越权，重放等等 具体测试内容包括但不限于：篡改造成的越权操作（如跨帐户查询），交易篡改（如修改金额，转帐金额为负值），特殊数据提交（如各种注入问题），重放导致的多次交易，以及用户枚举和暴力密码破解等。

#### 应用安全设计

##### 应用层加密

对于应用层数据传输过程中的数据防护提供加密机制，保证敏感数据在传输过程中的机密性和完整性。同时，针对敏感分类以上的数据存储采用数据库字段级加密，保证数据在存储阶段的机密性。

1、远程指令传输加密/解密。

2、采集数据文件经过加密后存储在磁盘上。

##### 应用层访问控制

对应用层访问采用统一的身份认证管理机制，防止未授权的访问。同时，对应用层的访问采取了WEB应用安全管控和敏感信息检测等机制。

针对来自互联网居民的访问，采用用户名、口令等形式的访问控制规则，并对访问数据做日志和审计记录。

针对客服人员、运维人员可采用数字证书加密形式，使用统一的身份认证管理机制，充分保障了用户在访问过程中的安全性，提供可供审计的日志。

##### 系统安全加固

政府门户网站系统本身也需要进行一系列安全加固措施，主要包括：

1、对登录用户进行身份标识和鉴别，且保证用户名的唯一性。

2、根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用3种以上字符、长度不少于8位并定期更。

3、启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

#### 数据安全设计

数据安全是保障云平台安全的重点。为了保证保障用户的数据安全，我的长沙-城市移动综合服务平台从数据隔离、访问控制等多个方面采取措施。同时我的长沙-城市移动综合服务平台制订了数据保密性安全规范用于保障业务平台重要业务数据的安全传递与处理应用，确保数据能够被安全、方便、透明的使用。为此，业务平台应采用加密等安全措施开展数据保密性工作：

1、采用加密效措施实现重要业务数据传输保密性。

2、采用加密实现重要业务数据存储保密性。

通过对敏感数据进行加密处理和安全存储，保障用户数据的私密性和安全性。并通过身份认证和权限管理，对使用云服务数据的用户进行严格的身份审核，实现用户数据的安全数据存取和安全数据交换。

##### 数据传输安全

在对数据进行传输、风险评估的基础上采用合理的加密技术，选择和应用加密技术时，符合以下基线：

1、必须符合国家有关加密技术的法律法规。

2、根据风险评估确定保护级别，并以此确定加密算法的类型、属性，以及所用密钥的长度。

3、根据专家的建议，确定合适的保护级别，选择能够提供所需保护的合适的工具。

4、敏感数据的传输过程中必须使用数字签名以确保信息的不可否认性，使用数字签名时应符合以下规范。

5、充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名。

6、采取保护公钥完整性的安全措施，例如使用公钥证书。

7、确定签名算法的类型、属性以及所用密钥长度。

8、用于数字签名的密钥应不同于用来加密内容的密钥。

我的长沙-城市移动综合服务平台在与远端网络通讯时采用VPN的方式加密传输数据，用来保障通讯过程中的机密性、完整性和可用性。VPN被定义为通过一个公用网络（通常是互联网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定隧道。使用这条隧道可以对数据进行加密达到安全使用互联网的目的。

我的长沙-城市移动综合服务平台针对应用层的数据通信采用TLS 加密技术，用来保证应用层安全，以达到保障数据安全的目的。

采用TLS传输加密技术的优势在于：

1、通信双方所有信息均为加密传输，第三方无法窃听。

2、通信过程中具有校验机制，一旦被篡改，通信双方立刻发现。

3、通信前校验身份证书的有效性，防止身份被冒充。

##### 数据存储安全

我的长沙-城市移动综合服务平台对于存储介质的管理采用包含重要、敏感或关键数据的移动式存储介质由专人保管，任何存储媒介入库或出库均经过授权，并保留相应记录，方便审计跟踪。

我的长沙-城市移动综合服务平台数据安全存储为满足数据安全的需要，采用以下安全基线：

1、包含重要、敏感或关键数据的移动式存储介质由专人承担管理职责。

2、数据入库或出库需经过授权，并保留相应记录，方便审计跟踪。

1、数据分级

我的长沙-城市移动综合服务平台针对具有敏感信息的数据，采取加密存储的机制，在保证密钥安全的情况下，采用对称、非对称加密技术对敏感信息做加密处理，即使数据库管理员也无法查看到任何明文的敏感数据，数据只有在使用前通过应用程序调用自动完成解密操作，以保证敏感信息安全性。

我的长沙-城市移动综合服务平台针对信息的分类原则依照：敏感、公开级别划分。

（1）敏感：业务推广过程中的相对隐私的数据文件，如用户个人隐私，身份信息等，一旦泄漏会产生一定的不良影响，对组织或用户照成形象受损。例如我的长沙-城市移动综合服务平台中的个人身份标识、家庭住址等信息

（2）公开：可对公众发布的非敏感类信息，不会对企业或用户照成不良影响。

我的长沙-城市移动综合服务平台针对敏感分类以上数据，全部采用数据库字段级存储方式，保障数据机密性，并对数据针对列进行分类分级，并通过标签对数据进行标记，对于不同密级数据进行不同的处理。

2、数据库安全防护

我的长沙-城市移动综合服务平台针对数据库层面充分采用数据库安全机制。

（1）采用复杂数据库密码口令策略

我的长沙-城市移动综合服务平台对于数据库管理员账户严格遵循复杂密码安全策略，同时设置定期强制修改密码等安全策略。

（2）安全的帐号使用策略

我的长沙-城市移动综合服务平台对于数据库帐号采用严格的职责划分和使用策略。

（3）数据库日志

我的长沙-城市移动综合服务平台针对数据库登录事件的“失败和成功”审核机制，详细记录所有账号的登录事件。请定期针对数据库日志做检查是否有可疑的登录事件发生，或者大批量查询、删除等日志。

##### 数据访问控制

访问控制的主要功能包括：保证合法用户访问受权保护的网络资源，防止非法的主体进入受保护的网络资源，或防止合法用户对受保护的网络资源进行非授权的访问。访问控制首先需要对用户身份的合法性进行验证，同时利用控制策略进行选用和管理工作。当用户身份和访问权限验证之后，还需要对越权操作进行监控。因此，访问控制的内容包括认证、控制策略实现和安全审计。

1、认证。包括主体对客体的识别及客体对主体的检验确认。

基于角色的访问控制

角色（Role）是一定数量的权限的集合。指完成一项任务必须访问的资源及相应操作权限的集合。角色作为一个用户与权限的代理层，表示为权限和用户的关系，所有的授权应该给予角色而不是直接给用户或用户组。

基于角色的访问控制（Role-Based Access Control，RBAC）是通过对角色的访问所进行的控制。使权限与角色相关联，用户通过成为适当角色的成员而得到其角色的权限。可极大地简化权限管理。为了完成某项工作创建角色，用户可依其责任和资格分派相应的角色，角色可依新需求和系统合并赋予新权限，而权限也可根据需要从某角色中收回。减小了授权管理的复杂性，降低管理开销，提高企业安全策略的灵活性。

2、控制策略。通过合理地设定控制规则集合，确保用户对信息资源在授权范围内的合法使用。既要确保授权用户的合理使用，又要防止非法用户侵权进入系统，使重要信息资源泄露。同时对合法用户，也不能越权行使权限以外的功能及访问范围。

在访问控制实现方面，实现的安全策略包括5个方面：数据资源目录、数据申请安全防护、数据隐私防护、数据监控及异常管理、数据权限管理。

##### 数据备份策略

在系统运行过程中，可能会出现一些特殊情况而造成数据丢失。通过系统数据的安全备份进行数据的安全管理，处理应急事故。建立比较完善可靠的数据存储容灾备份系统，对系统数据进行实时或定时的复制，以达到数据备份的目的，在出现问题时可以以最短的时间保证快速恢复数据。

存储备份系统中的存储设备中保存着最重要的资源“数据”，由于用户数据具有的完整性、唯一性、独特性，一旦出现数据损坏要么不可恢复，要么恢复工作量巨大。存储备份系统的安全性和可靠性是最优先考虑的因素，其次存储备份设备的容量要满足应用要求。

本项目备份系统设计包括：依托于长沙市电子政务云平台的存储备份系统，为我的长沙-城市移动综合服务平台信息资源中心分配存储资源，构建存储备份机制。备份策略的选择如下：

1、备份策略三种类型

全量备份：每次备份定义的所有数据，优点是恢复快，缺点是备份数据量大，数据多时可能做一次全备份需很长时间；

增量备份：备份自上一次备份以来更新的所有数据，其优点是每次备份的数据量少，缺点是恢复时需要全备份及多份增量备份；

差分备份：备份自上一次全备份以来更新的所有数据，其优缺点介于上两者之间；

在备份类型选择时，一般的规则是：

对于操作系统和应用程序代码，可在每次系统更新或安装新软件和做一次全备份；对于一些日常数据更新量大，但总体数据量不是非常大的关键应用数据，可每天在用户使用量较小的时候安排全备份；对于日常更新量相对于总体数据量较小，而总体数据量非常大的关键应用数据，可每隔一个月或一周安排一次全备份，在此基础上，每隔一个较短的时间间隔做增量备份。

2、备份策略分析

完全备份所需时间最长，但恢复时间最短，操作最方便，在备份窗口允许时尽量多的采用全备份，其它时间采用所用时间更少的增量备份或采用介于两者之间的差分备份。各种备份的数据量不同：全备份>差分备份>增量备份。

在恢复数据时需要的备份介质数量也不一样：如果使用全备份方式，只需最近一次的全备份数据就可以恢复所有数据；如果使用全备份和增量备份相结合的方式，则需要一次全备份数据和若干次增量备份数据才能恢复所有数据；如果使用全备份和差分备份相结合的方式，只需上次的全备份数据和最近的差分备份数据就可以恢复所有数据。

3、数据备份策略

项目需要对系统已有数据，包括市民个人数据及系统所产生的业务数据进行增量及全量备份。（1）增量备份，对每日生成的新数据进行备份，用于灾后快速恢复。（2）全量备份，对市民的所有个人信息数据及系统业务数据进行每日全量备份，防止由于不可抗因素或系统宕机导致的数据丢失。

我的长沙-城市移动综合服务平台项目的备份策略为，增量数据每日进行备份，并且保留最近30天的数据，全量数据每日进行备份，备份完成后删除前日数据。备份数据采用对象存储。

##### 用户数据隔离防护

用户端到我的长沙-城市移动综合服务平台之间的用户数据传输涉及数据隔离措施；新上线应用和已有应用提供数据层隔离；避免来自同一宿主机上的其他虚拟机破坏数据完整性；不同安全域及部门专属业务域之间既要实现应用数据隔离，也要保障业务的关联性和一致性；设计统一的密钥管理机制。

采用分离设备驱动模型实现I/O的虚拟化。虚拟机所有的I/O 操作都会被截获处理；保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。

密码安全

密码的使用遵循以下原则：

1、不能将密码写下来，不能通过电子邮件传输。

2、不能使用缺省设置的密码。

3、不能将密码告诉别人。

4、系统的密码泄漏，必须立即更改。

5、 密码以加密形式保存，加密算法强度要高，加密算法不可逆。；

6、系统强制指定密码的策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等。

7、需要特殊用户的口令（比如说UNIX下的Oracle），禁止通过该用户进行交互式登录。

8、在要求较高的情况下使用强度更高的认证机制，例如：双因素认证。

9、要定时运行密码检查器检查口令强度，系统每月检查一次。

#### 网络和通信安全

##### 网络隔离

通过政务云平台安全组服务实现组内和组间的访问控制，加强虚拟机的安全保护，实现VPC内部的网络隔离。

##### 访问控制

通过政务云平台虚拟防火墙服务为我的长沙-城市移动综合服务平台提供南北向流量的访问控制，控制VPN与外网间流量的互访，VPN之间东西向流量也用虚拟防火墙隔开。

##### 网络设备防护

政务云平台提供虚拟堡垒机服务为网络设备提供运维操作全程审计，建立面向用户的集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求。

通过基于唯一身份标识的集中账号与访问控制策略，与网络设备、安全设备等无缝连接，实现网络设备的身份鉴别、二次鉴权、登录控制、口令复杂点等管控。

##### 网络入侵防护

通过政务云平台互联网出口部署IPS设备，阻断各类入侵攻击。IPS应具备攻击事件检测、阻击、记录、报警功能。IPS日志数据可集中提交给安全管理平台、安全事件管理平台实现安全事件集中溯源、审计。

两路直通是入侵防护设备高可用性的一种部署方式，主设备与从设备都有两对直通口连接两端的网络设备，两台设备之间各通过一个管理口（作为心跳口）相连。

##### 异常流量防护

网络异常流量防护从系统设计上需要实现以下关键目标：

1、提供高效安全能力：安全威胁实时发现能力，全网高效协同能力，快速安全响应/恢复能力。

2、支持异构多源数据：多源信息安全分析能力，流量智能识别检测控制能力，多元网络安全策略协同能力。

3、提供高价值决策：全面安全感知能力，动态、精确的安全策略自适应能力，富价值的安全决策能力。

4、服务能力可视化：安全威胁可视化，资产可视化，安全风险可视化，安全态势可视化。

电子政务云互联网出口DDOS防护采用清洗、检测的方式进行防护，能够保证大型数据中心异常攻击流量细颗粒检测、并且迅速对出口交换机进行流量牵引。

##### Apt威胁检测

高级可持续攻击监测系统通常部署在互联网接入口，检测进出网络的流量，发现企图进入内网的恶意软件，以及试图出局的木马连接等，实现的方式可分为：

威胁分析检测设备（安全探针）：用来在漏洞利用阶段发现恶意软件，并且可以跟踪恶意软件后续的下载、回连等活动过程。

入侵防御系统：IPS接收信誉库数据，检测或阻截带有攻击的数据流量，并控制其后续的数据窃取及持续渗透活动。

在部署方面，高级可持续攻击监测系统通过端口镜像方式对应用流量进行持续监测，IPS设备与检测设备进行对接，IPS将可疑文件发送给分析检测系统进行检测，一旦测试发现危害结果，将测试结果反馈给IPS设备，由IPS设备进行及时拦截。

##### 安全审计

在云平台互联网出口区部署网络审计以及数据库审计设备，用于网络流量、用户行为进行审计，在云平台安全管理区部署集中日志审计系统，开启网络设备日志发送功能，将各网络设备的日志统一发送到集中日志审计系统，实现设备状态等集中审计。

##### 物理安全

依托政务云实现物理安全保护，物理安全是保护计算机网络设备、设施以及其它媒体免遭环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。在网络环境中，涉及到的物理安全主要包括四个方面：

1、环境安全：对系统所在环境的安全保护，如区域保护和灾难保护。

2、机房安全：对系统核心设备所位于的中心机房的安全系统设计、实施和运行监控。

3、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。

4、媒体安全：包括媒体数据的安全及媒体本身的安全。为保证信息网络系统的物理安全，除网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。

我的长沙-城市移动综合服务平台部署于政务云平台上，根据政务云平台项目的计划和安排，机房租用运营商的机房，机房的建设满足国家A级电子信息系统机房设计规范（GB50174-2008）的安全要求。在机房建设及改造过程中，充分考虑了机房环境、机房管理、机房设备与介质安全等问题，满足国家标准《信息安全技术 信息安全安全等级保护基本要求》中规定第三级物理安全防护要求。

## 用户界面需求

用户界面是程序中用户能看见并与之交互作用的部分,设计一个好的用户界面是非常重要的,本设计将为用户提供美观,大方,直观,操作简单的具备windows风格的用户界面。

用户界面的整体标准包括以下四个方面：

1、规范性

2、合理性

3、一致性

4、界面定制性

### GUI设计的规范

遵循一致的准则，确立标准并遵循，是软件界面设计中必不可必的环节。确立界面标准的好处：

1、便于用户操作：户使用起来能够建立起精确的心里模型，使用熟练了一个界面后，切换到另外一个界面能够很轻松的推测出各种功能。

2、使用户感觉到统一、规范，在使用软件的过程中愉快轻松的完成操作，提高对软件的认知

3、降低培训、支持成本，不必花费较多的人力对客户进行逐个指导

### GUI布局的合理性

界面的合理性是指界面是否与软件功能相融洽，界面的颜色和布局是否协调等。例如：

1、界面布局

a.屏幕不能拥挤

Mayhew在1992年的试验结果表明屏幕总体覆盖度不应该超过40％，而分组覆盖度不应该超过62％；

整个项目，采用统一的控件间距，通过调整窗体大小达到一致，即使在窗体大小不变的情况下，宁可留空部分区域，也不要破坏控件间的行间距。

b.控件按区域排列

一行控件纵向中对齐, 控件间距基本保持一致，行与行之间间距相同，靠窗体的控件距窗体边缘的距离应大于行间距；

当屏幕有多个编辑区域，要以视觉效果和效率来组织这些区域。

c.有效组合

逻辑上相关联的控件应当加以组合以表示其关联性，反之，任何不相关的项目应当分隔开。在项目集合间用间隔对其进行分组，或者使用方框划分各自区域。

d.窗口缩放时，控件位置、布局

固定窗口大小，不允许改变尺寸；

改变尺寸的窗口，在窗口尺寸发生变化时控件的位置、大小做出相应的改变；

改变尺寸的窗口，在窗口改变尺寸时增加相应在的纵向、横向滚动条，以方便用户使用窗体上的控件。

2、界面颜色搭配

使用恰当的颜色，可以使软件的界面看起来更加规范：

a.统一色调

针对软件类型以及用户工作环境选择恰当色调，如：安全软件，根据工业标准，可以选取黄色。绿色体现环保，蓝色表现时尚清新、紫色表现浪漫等等，淡色可以使人舒适，暗色做背景使人不觉得累等。

b.与操作系统统一，读取系统标准色表。

c.遵循对比原则

在浅色背景上使用深色文字，深色背景上使用浅色文字，如蓝色文字以白色背景容易识别，而在红色背景则不易分辨。除非特殊场合，杜绝使用对比强烈，让人产生憎恶感的颜色。

d.整个界面色彩尽量少的使用类别不同的颜色。

e.颜色方案也许会因为显示器、显卡、操作系统等原因显示出不同的色彩。

f.针对色盲、色弱用户，可以使用特殊指示符。

e.颜色方案也许会因为显示器、显卡、操作系统等原因显示出不同的色彩。

f.针对色盲、色弱用户，可以使用特殊指示符。

### GUI风格的一致性

界面的一致性既包括使用标准的控件，也指相同的信息表现方法，如在字体、标签风格、颜色、术语、显示错误信息等方面确保一致。

1、在不同分辨率下的美观程度

软件界面要有一个默认的分辨率，而在其他分辨率下也可以运行，分别在1024×768，1280×768，1280×1024，1200×1600分辨率下的大字体、小字体下的界面表现。

2、界面布局要一致

如所有窗口按钮的位置和对齐方式要保持一致。

3、界面的外观要一致

如控件的大小、颜色、背景和显示信息等属性要一致，一些需要特殊处理或有特殊要求的地方除外。

4、界面所用颜色要一致

颜色的前后一致会使整个应用软件有同样的观感，反之会让用户觉得所操作的软件杂乱无章，没有规则或言。

5、操作方法要一致

如双击其中的项，触发某事件，那么双击任何其他列表框中的项，都应该有同样的事件发生。

6、控件风格、控件功能要专一

a.不错误的使用控件

例如使用Button样式做Table的功能，拿主菜单条显示版权信息等   b.一个控件只做单一功能，不复用

如果在特殊情况下出现复用的时候，可采用以下两种方法解决：

分组，使用双份控件；

使用Table页，给用户很明显的视觉变化。

7、标签和讯息的措词要一致

如在提示、菜单和帮助中产生相同的术语。

8、标签中文字信息的对齐方式要一致

如某类描述信息的标题行定为居中，那么其他类似的功能也应该与此一致。

9、快捷键在各个配置项上语义保持一致

如Tab键的习惯用法是阅读顺序从左到右，从上到下。在定义软件快捷键时也可以将现有一些快捷键的属性作为参考，如表1-3-1（见附件）列出了常用的快捷键及其功能。

## 软硬件环境需求

### 硬件技术需求

本章节主要描述我的长沙-城市移动综合服务平台对对基础设施（IAAS）和应用支撑（PAAS）的需求设计，不属于本项目的建设范畴。政务云提供的CPU主频为2.2GHZ。根据2.3章节的需求分析，本项目对基础设施（IAAS）和应用支撑（PAAS）的需求设计如下。

#### 基础设施资源需求清单

（根据实际情况，弹性调整）。

##### 弹性计算主机服务

结合计算资源设计所需CPU资源总量为400核，需要800GB内存（ CPU核数与内存比例为1:2）。根据实际情况，弹性调整。设计计算主机服务需求清单如下（后续如有扩容需求，以实际扩容后资源为准）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 云主机服务备注（云硬盘作为启动盘） | | | | | |
| 编码 | 主机服务名称 | CPU（核） | 内存（G） | 系统盘（G） | 备注（共400核） |
| ZJ03 | 8核16G云主机服务 | 8 | 16 | 100 | 50套 |

##### 主机服务配置表

##### 云硬盘服务

针对存储资源服务需求清单如下（后续如有扩容需求，以实际扩容后资源为准）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编码 | 产品大类 | 产品小类 | 型号 | 描述 | 备注 |
| YP03 | 存储 | 云硬盘存储 | 大容量文件共享存储服务 | 开放NFS（linux）和CIFS（Windows）接口，按需使用，容量单位为TB。 | 16TB（包括操作系统存储） |

云硬盘服务配置表

##### 操作系统

针对操作系统需求清单如下（后续如有扩容需求，以实际扩容后资源为准）：

| 部署应用 | 操作系统 | 物理区域 |
| --- | --- | --- |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 内部数据中心 |
| 数据库集群 | Centos 7.5\_x86\_64 | 业务数据库区 |
| 数据库集群 | Centos 7.5\_x86\_64 | 业务数据库区 |
| 数据库集群 | Centos 7.5\_x86\_64 | 业务数据库区 |
| 数据库集群 | Centos 7.5\_x86\_64 | 业务数据库区 |
| 数据库集群 | Centos 7.5\_x86\_64 | 业务数据库区 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |
| 应用集群 | Centos 7.5\_x86\_64 | 外部数据中心 |

##### 操作系统配置表

##### 安全资源

针对安全资源需求清单如下（后续如有扩容需求，以实际扩容后资源为准）：

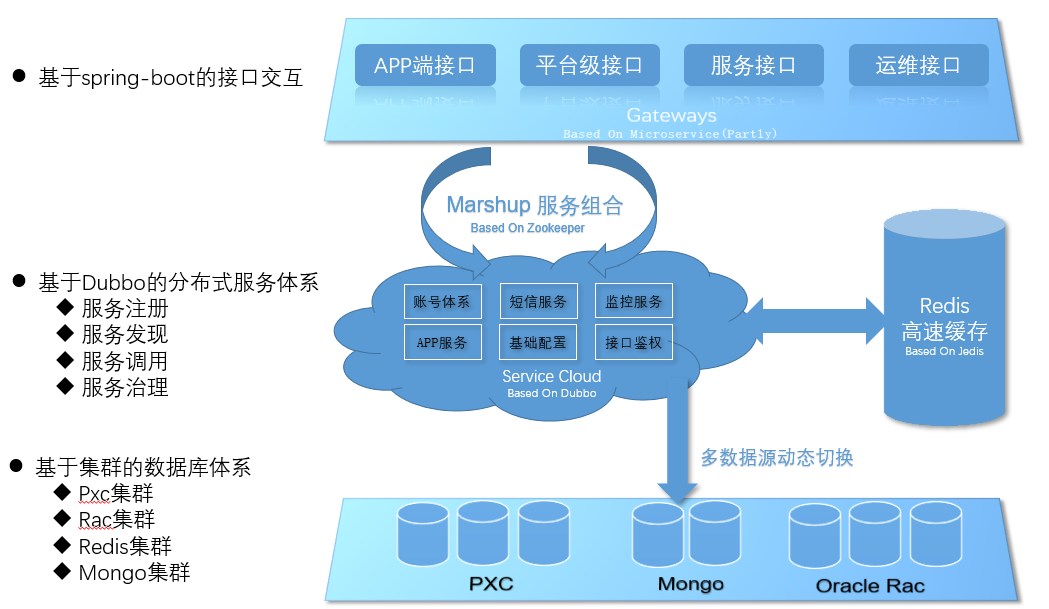
| 序号 | 目录 | 简要描述 | 数量 |
| --- | --- | --- | --- |
| 1 | 边界防火墙 | 边界安全防护、网络防病毒 | IAAS云平台提供 |
| 2 | 入侵防御系统 | 网络入侵防护及检测 | 购买服务，租户安全资源池提供 |
| 3 | 主机安全防护系统 | 主机安全防护 | 购买服务，租户安全资源池提供 |
| 4 | WEB防护系统 | WEB安全防护 | 购买服务，租户安全资源池提供 |
| 5 | 运维安全审计系统 | 运维安全审计 | 购买服务，租户安全资源池提供 |
| 6 | 数据安全审计系统 | 数据库审计、脱敏 | 购买服务，租户安全资源池提供 |
| 7 | 日志审计系统 | 日志安全审计 | 购买服务，租户安全资源池提供 |
| 8 | 渗透测试服务 | 通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。 | 20人天，预计40万 |
| 9 | 应急响应服务 | 一年两次应急响应服务或结合实际业务模拟一次应急演练 | 15人天，预计30万 |
| 10 | 漏洞扫描系统 | 漏洞检测 | 购买服务，租户安全资源池提供 |
| 11 | 网络安全审计系统 | 网络安全审计 | IAAS云平台提供 |
| 12 | 安全巡检服务 | 一年两次安全策略、安全基线、漏洞扫描等服务。 | 一年2次，预计10万 |
| 13 | 合规咨询服务 | 提供匹配等级保护、分级保护及主管部门等要求的安全管理体系、技术体系最佳实践咨询服务。 | 一次，预计10万 |
| 14 | 安全培训服务 | 根据需求提供不大于一次安全意识一次安全技术培训的讲师与课件 | 一次，预计10万 |
| 15 | 专项检查服务 | 根据实际需求提供主管机构或自发需求的专项检查服务。 | 一次 |
| 16 | 安全情报与通告 | 提供威胁情报与重大安全事件通告及预警服务 | 一年 |

安全资源表

### 软件技术需求

#### 技术需求框架

系统采用分布式架构，实现服务的自动注册、发现，实现数据库的高可用集群。



服务组件图

系统分层技术描述：

|  |  |
| --- | --- |
| 负载层 | 为APP端和网站端访问提供外网访问及服务负载均衡配置 |
| 应用层 | 为各个独立子系统提供前端服务 |
| 展现层 | APP或者网站采用的数据交互方式及展现形式 |
| 服务层 | 为应用层提供后端服务支撑和基础服务框架封装 |
| 数据层 | 提供底层数据访问、数据映射及数据库集群 |
| 基础设施 | 提供虚拟或实体服务器 |
| 监控运维 | 为每层提供独立监控功能 |

系统分层技术表

具体软件描述

MySQL，数据库，版本需求5.7.22，数量一套；

Mongo，文档数据库，版本需求3.4，数量一套；

Redis,缓存数据库，版本需求4.11，数量一套；

Dubbo，服务注册发现组件，版本需求2.4，数量一套。

### 移动端运行环境需求

#### 安卓运行环境需求

CPU：双核2GHz及以上；

机身内存：4G以上

屏幕分辨率：1920x1080及以上；

操作系统：Android 5.0及以上版本。

#### 苹果运行环境需求

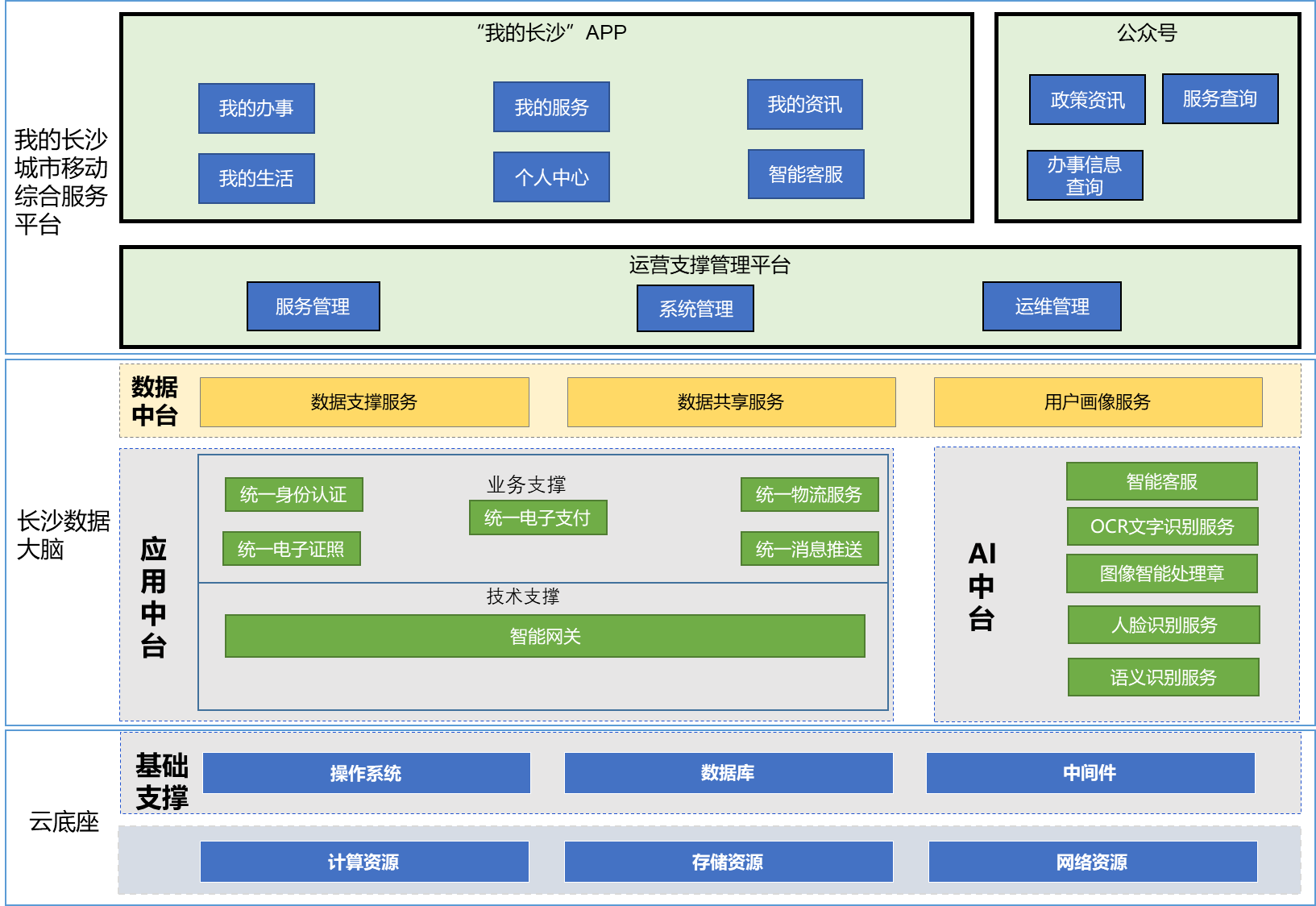
iPhone机型：iPhone5及以上版本；

机身内存：16G以上；

操作系统：iOS 9.0及以上版本。

## 扩展性需求

本项目对应用支撑层（PAAS）的需求，由长沙数据大脑提供基础的支持能力，包含数据大脑提供的数据中台、应用中台和AI中台的相关服务，具体包括以下部分。（本章节不属于本项目的建设范畴）



长沙数据大脑与我的长沙-城市移动综合服务平台关系图

本项目与长沙数据大脑（又称三中台）的关系如上图所示，我的长沙-城市移动综合服务平台需要数据大脑提供能力支撑，我的长沙用户相关数据将会沉淀至数据大脑。

### 应用中台需求表

| **序号** | **应用中台服务** | **应用场景** | **需求** |
| --- | --- | --- | --- |
| 1 | 应用服务平台 | 我的长沙-城市移动综合服务平台统一使用中台能力，中台能力以服务的方式通过数据大脑应用中台的智能网关发布，利用智能网关实现服务的注册、传输服务、提供位置透明的路由和定位服务、提供多种消息传递形式、支持广泛使用的传输协议、多服务集成、服务和事件管理支持等功能。 | √ |
| 2 | 应用接入平台 | 我的长沙-城市移动综合服务平台需要对接多个省级、市级局委办业务系体接口，接口以服务的方式通过数据大脑应用中台的智能网关发布，利用智能网关实现服务的注册、传输服务、提供位置透明的路由和定位服务、提供多种消息传递形式、支持广泛使用的传输协议、多服务集成、服务和事件管理支持等功能。 | √ |
| 3 | 应用运营平台 | 我的长沙-城市移动综合服务平台的持续运营效果也需要借助运营平台实现用户的留存拉新，功能的完善迭代。 | √ |
| 4 | 电子证照服务 | 我的长沙-城市移动综合服务平台为了实现少填少报，最多跑一次的业务目标， 需要利用电子证照服务进行证照的在线获取、共享 | √ |
| 5 | 统一物流服务 | 为了实现“最多跑一次”的业务目标，需要利用快递服务实现收件和送件的服务，以避免多跑。利用物流公司管理、物流信息查询、业务接入、打印管理等管理功能，提供获取邮件号、新增订单、变更订单等公共服务，实现与第三方物流平台无缝连接提供支撑 | √ |
| 6 | 统一支付服务 | 在非税缴费方面，一体化平台利用统一支付服务，实现与第三方支付平台的统一对接，并实现与财政非税支付平台的对接，实现整体业务的对账与支付功能。 | √ |
| 7 | 统一消息服务 | 为实现办理过程和办理结果实时在线可查，通知及时送达，需要利用统一消息服务实现及时的信息推送 | √ |
| 8 | 统一身份认证服务 | “政务一体化平台”涉及民众的办事服务需要进行实人认证，利用统一身份认证提供的移动端提供多种身份认证方式，如个人认证、法人认证等，并集成统短信,验证码接口服务。 | √ |
| 9 | 表单引擎 | 调用电子表单工具，能依靠表单引擎的输出灵活配置前端的页面展示信息 | √ |
| 10 | 微服务平台 | 针对服务的入驻提供一整套的流程管理，如注册、申请、审核、发布等 | √ |

应用中台需求表

### 统一支付能力需求

1、统一支付平台的功能性需求为：

（1）建设先进的、规范的、安全的统一支付平台，提供和包支付、微信、支付宝、银联等支付渠道。

（2） 建立统一的数据规范和技术规范，为用户提供统一支付方式，为各业务提供统一支付接口及组件，支持多种类型的支付服务调用，支持包括H5、SDK，进一步支持业务机构之间的必要对账需求和相应服务的报表管理。

（3）汇聚腾讯优势资源，整合公共服务中水电煤、电视缴费等服务提供给我的长沙APP。

根据业务需求，统一支付平台需满足长沙市互联网+政务一体化、我的长沙APP、小程序等平台需求，为政务服务、公共服务、生活服务提供支付能力输出。

2、非功能性要求

（1）统一性

支付平台采用统一的支付界面，界面应简洁明了，布局合理，美观大方。支付界面的风格、要素和布局应保持一致。

（2）易用性

所有人机界面均要求简洁、易操作，在线帮助便捷、准确，对于固定可选的输入选项应提供列表选择。

（3）可靠性

支付平台在设计时按照：核心功能与外围功能的分离；系统架构和模块层次关系设计与具体业务开发的分离；支付平台与第三方接入系统接口的分离原则，在系统架构上保证了系统的可靠性。

系统性能要求

按服务人口800万规模估算，注册用户数30%~40%，约300万注册用户，根据同类APP日活5%的结果估算，涉及支付类业务约占总量5%，初步估算日处理300\*5%\*5%，约10万笔交易左右；峰值按照均值的5倍计算，约50万笔/天。

（1）平均日处理笔数10万。

（2）峰值日处理笔数50万。

（3）交易成功信息页面速度：用户提交验证信息后，在平均20秒、最多70秒完整显示交易成功信息页面。

4、安全需求

统一支付系统由于涉及资金并连接金融网络，因此对系统数据的稳定和安全要求非常高。具体要求包括：

（1）保证系统稳定持续，尽量不间断运行。。

（2）保证敏感数据的安全和相关数据库服务器的安全以及互联网数据传送的安全性、机密性和完整性。

（3）保证与联网金融系统的连接安全。

（4）使用备份机制，服务器及数据库要能够在短时间内恢复。

### 统一身份认证能力需求

涉及民众的办事服务需要进行实人认证，利用统一身份认证提供的移动端提供多种方式、多个层级的个人身份认证。功能需求如下：

1、多层级用户

个人用户包括游客用户、注册用户、实名认证用户、带人脸信息的用户。

2、多种实名认证方式

为保证用户全覆盖，APP上需提供多种渠道的实名认证方式，包括微信小程序、手持身份证、银联、支付宝等，供用户自由选择。

### 统一物流能力需求

为了实现“最多跑一次”的业务目标，需要利用快递服务实现收件和送件的服务，以避免多跑。利用物流公司管理、物流信息查询、业务接入、打印管理等管理功能，提供获取邮件号、新增订单、变更订单等公共服务，实现与第三方物流平台无缝连接提供支撑。

### 数据中台需求表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 数据中台服务 | 应用场景 | 需求 |
| 1 | 业务数据库服务 | 我的长沙-城市移动综合服务平台将使用业务数据库服务中的分布式数据库服务实现数据持久化，通过文档数据库服务实现非结构化数据的持久化，内存数据库用于高并发高性能的数据访问服务。 | √ |
| 2 | 主题库服务 | 为了实现政务服务少填少报，最多跑一次，将利用主题库的基础库能力实现基础共享数据的自动填写 | √ |
| 3 | 数据开放运营服务 | 为了实现政务服务少填少报，最多跑一次的业务目标，需要数据共享的支持，数据开放运营服务将提供以数据资产为维度的数据共享服务。 | √ |

数据中台需求表

##### 用户画像需求

需数据中台对用户行为进行分析，利用算法技术，对用户行为数据进行分析解读，打上标签，将用户的画像提供给APP。APP根据用户画像，将受众感兴趣的内容推送给用户，实现“千人千面”的服务、资讯。

### AI中台需求表

| 序号 | AI中台服务 | | 需求 |
| --- | --- | --- | --- |
| 1 | AI原子能力服务 | 图像服务 | √ |
| 语义服务 | √ |
| 语音服务 | √ |
| 2 | AI工作室 | AI模板 | √ |
| 3 | 算法中心 | 数据服务 | √ |
| 模型服务 | √ |
| 4 | 接入中心 | 算法适配器 | √ |
| 数据适配器 | √ |

AI中台需求表

##### 人脸核身能力需求

AI中台提供配套SDK、接口及授权，APP端集成SDK。在身份认证的过程中，若需要进行实人认证，则需要进行“人脸核身”的技术应用场景，在人脸核身的过程中将使用AI中台的“图像识别”原子能力，通过识别人脸图像特征并进行数据的比对，实现APP端内刷脸认证。这里涉及AI中台的AI原子能力服务、AI工作室服务能力。

##### 在线客服能力需求

智能客服是政务服务的标配能力，民众通过线上机器人客服则可以实现咨询、投诉、查询、问询等操作，后台无需人工干预。期间应用技术包括语义识别、语音服务、机器学习、语音合成等能力，涉及AI中台的AI原子能力服务、AI工作室、算法中心、接入中心服务能力。

在线客服性能需求

(1)数据量分析

1、小数据量压测

小数据量且开启faiss情况下，挂载不同类型的子bot，性能差异不大：

qps平均为:38.7/sec 耗时平均为：387/ms。

2、中等数据量压测

中等数据量且开启faiss情况下，挂载不同类型的子bot，部分性能存在差异:

（1） 挂载子bot为faq+寒暄时：qps平均为:38.5/sec 耗时平均为：389/ms。

（2） 挂载子bot为faq+任务型时：qps平均为:37.4/sec 耗时平均为：400/ms。

（3） 挂载子bot为faq+资料库时：qps平均为:35.8/sec 耗时平均为：418/ms。

（4） 挂载子bot为faq+知识图谱时：qps平均为:39.5/sec 耗时平均为：379/ms。

（5） 挂载子bot为faq+寒暄+资料库时：qps平均为:32.2/sec 耗时平均为：466/ms。

（6） 挂载子bot为faq+寒暄+任务型时：qps平均为:36.4/sec 耗时平均为：412/ms。

（7） 挂载子bot为faq+寒暄+知识图谱时：qps平均为:38.2/sec 耗时平均为：391/ms。

（8） 挂载子bot为faq+寒暄+资料库+任务型时：qps平均为:30.7/sec 耗时平均为：487/ms。

（9） 挂载子bot为faq+寒暄+资料库+知识图谱时：qps平均为:34.8/sec 耗时平均为：430/ms。

（10） 挂载子bot为faq+寒暄+资料库+任务型+知识图谱时：qps平均为：25.7/sec 耗时平均为：582/ms。

3、大数据量压测

大数据量业务在挂载faq，寒暄，资料库，任务型 并且开启faiss，但不开启缓存的情况下：qps平均为：9.8/sec 平均耗时为：507/ms。

(2)服务器资源消耗分析

1、离线训练组件

（1）压测过程中（无离线模型训练），单台离线训练组件所在服务器cpu使用在20%左右，内存消耗持续上升，达到19G左右后趋于稳定。

（2）压测停止后，cpu下降到7%左右，内存维持在19G左右。

（3）中小数据量业务压测数据样本数总计约133万（单日），即单日会话数在130万左右时，统计服务可以正常落日志，且实时访问产品系统的服务总览等日志查询页面无异常。

2、在线计算组件

（1）压测过程中，在线计算组件单机所在服务器的cpu使用在60%内，单机内存消耗在58G左右。

（2）压测停止后，cpu下降到在3-5%，内存使用维持在50G左右。

## 可维护性需求

通过统一支撑管理平台记录操作log,在考虑需求可行性,准确性等的同时,以保障软件可维护性。

1、易分析性：与为诊断缺陷或者失效原因及为判定待修改的部分所需努力有关的软件属性。如日志记录系统等。

2、易改变性：与进行修改排除错误或者适应环境变化所需努力有关的软件属性。

3、稳定性：与修改所造成的未预料结果的风险有关的软件属性。

4、易测试性：与确认已修改软件所需的努力有关的软件属性。

5、源代码标准化:

（1）制定编码标准规范，包括前端工程编码规范、后端工程编码规范;

（2）编码标准规范细则包括命名标准规范、注释标准规范、异常处理标准、代码格式标准、数据库命名标准等;

（3）制定开发人员源代码管理制度，对源代码的提交审核做初审、核定、合并流程控制;

（4）源代码的代码库做最小粒度权限控制;

（5）对源代码的review要求做到常态化;

（6）要求源代码的说明文档格式规范统一，便于识别维护。

6、文档标准化

（1）遵从超脑文档管理标准规范;

（2）制定文档标准目录，要求涵盖项目的整个生命周期;

（3）编制文档标准模板，每个项目周期的文档内容框架及格式做严格限定;

（4）每个文档编制完成，都要求做多方评审，做评审记录;

（5）文档归集、使用要求有标准的审核流程、权限控制流程。