广西壮族自治区住房和城乡建设
信息化建设技术规范
(2024 年版)

目录

前言

本文件规定了广西壮族自治区住房和城乡建设信息化建设的整体要求。

本文件适用于参与广西壮族自治区住房和城乡建设信息化建设的软件开发厂商。

本文件由广西壮族自治区住房和城乡建设厅信息中心提出。

本文件起草单位：

本文件主要起草人：

引言

为规范广西壮族自治区住房和城乡建设信息化建设项目的建设，实现信息资源的整合与共享，推广、应用数字化城市建设、管理模式，提高城市管理和公共服务的水平与效率。为平台设计、建设、运营提供依据，拟由两个部分构成。

——第一部分： 技术规范主要目的在于建立广西壮族自治区住房和城乡建设信息化建设项目总体框架，也是明确数字住建信息化项目的功能要求、建设要求、接入要求、安全要求和管理要求的重要依据。主要构成：总体要求、总体架构、功能规范、接入规范、技术规范和安全规范。

——第二部分：技术使用手册主要目的在于指导各业务系统软件开发厂商及合作伙伴统一、安全、合理、规范的接入广西壮族自治区住房和城乡建设信息化建设项目。不限于平台接入手册、运维手册、技术管理手册、编码规范手册、二次开发手册等一系列操作使用文档。后续具体详细由运营方提供对应的手册供接入方进行对接。

1. 范围

本文件提出了广西壮族自治区住房和城乡建设信息化建设的总体架构，规定了其功能要求、技术要求、安全要求和接入要求。

本文件适用于参与广西壮族自治区住房和城乡建设信息化建设的软件开发厂商及合作伙伴。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅该日期对应的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB4943.1-2022音视频、信息技术和通信技术设备 第1部分:安全要求

GB/T20275-2021信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T20281-2020信息安全技术 防火墙安全技术要求和测试评价方法

GB/T20945-2023信息安全技术 信息系统安全审计产品技术要求和测试评价方法

GB/T22239-2019信息安全技术 网络安全等级保护基本要求

GB/T29245-2012信息安全技术 政府部门信息安全管理基本要求

GB/T32922-2023信息安全技术 IPSecVPN安全接入基本要求与实施指南

3. 术语和定义

下列术语和定义适用于本文件。

3.1. 数字住建基础支撑平台

广西壮族自治区住房和城乡建设厅数字住建信息化基础支撑平台是以建筑信息模型（BIM）、城市信息模型（CIM）、大数据、云计算、物联网、5G 移动通信、人工智能等前沿技术为依托，构建数据融合、应用支撑、业务协同等三大能力，打造服务、工作、决策、运维等四大门户，支撑住建主管部门实现全过程、全生命周期的一体化数字治理，是建设数字中国和新型智慧城市的重要信息基础设施。广西壮族自治区住房和城乡建设厅数字住建信息化基础支撑平台，包括技术中台、业务中台和数据中台。

3.2. 能力开放

能力开放是将自治区住房和城乡建设厅内部的业务和数据以能力服务的方式对外发布，供有权限的用户调用，同时提供完整的全生命周期管控服务能力和持续的运营能力。

3.3. 融合服务

融合服务是指基于自治区住房和城乡建设厅内部业务系统和业务流程，采用统一的技术栈，提炼出可复用的共性业务应用服务，并提供可支撑服务构建、发布、运行、运维、运营一体化的工具。

3.4. 业务中台

业务中台通过定义一套公共元业务标准，用以规范业务后台供应，以便更快的响应业务前台的需求。

3.5. 技术中台

技术中台定义一套元公共技术标准，用以规范技术开发框架、开发架构、接口定义等标准并提供给前端使用。

3.6. 数据中台

数据中台定义一套元公共数据标准，用以规范数据抽取、数据治理等动作并将数据封装成为一个公共的数据服务提供给前端使用。

3.7. 业务协同

业务协同是依托技术中台、业务中台、数据中台提供的公共服务，统一实现各类业务系统之间的申请、审批、会签、登记、操作等环节的管理，达到业务协同。

3.8. 统一组织

统一组织服务涵盖统一组织架构及用户管理负责所有用户信息的统一管理，创建统一的用户登录帐号，对于第三方接入的业务系统的用户帐号根据业务需求可以以不同的方式接入、导入后同统一平台的用户登录帐号进行绑定。实现厅内组织、用户的统一管理。

3.9. 统一身份认证

统一身份认证服务提供统一应用注册中心，业务系统注册应用并完成适配升级后，可实现一次登录，全系统登录；场景范围包含应用磁贴单点跳转、事项详情页面穿透跳转、消息详情页面穿透跳转。

3.10. 统一移动平台

统一移动平台是住建厅统一的公众移动办事入口，随时随地连接人与业务。打造集“统一入口、统一信息门户、移动化业务应用、轻应用开发平台”四位一体的移动平台。

3.11. 统一待办

统一待办是依托能力平台提供的公共服务，通过定义一套公共接口标准，统一的待办事项处理流程，包括待办、已办、已发等环节，处理来自不同业务的待办事项，实现待办事项的集中管理和统一处理。

3.12. 统一消息

统一消息是依托能力平台提供的公共服务，通过定义一套公共接口标准，与统一待办组合处理来自不同业务系统的办理事项消息通知，实现消息集中管理和统一处理。

3.13. 统一信息服务

统一信息服务是依托能力平台提供的公共服务，通过定义十四套公共接口标准，为业务系统提供统一的业务协同、能力共用、数据共享信息服务，实业务数据横向交换。

3.14. 管理方

广西壮族自治区住房和城乡建设信息化建设项目的主管方。对该平台拥有所有权、管理权和使用权，统一管理接入的服务事项，向运营方下达具体建设和运营工作任务。

3.15. 接入方

接入广西壮族自治区住房和城乡建设信息化建设项目的政府部门。负责组织业务系统的建设运营，提供政务事项的办理服务、信息发布和咨询投诉处理等。

3.16. 运营方

广西壮族自治区住房和城乡建设信息化建设项目的建设运营方。为管理方和接入方提供相关技术支持服务。

3.17. 缩略语

API 应用程序编程接口（Application Programming Interface）

PAAS 平台即服务（Platform as a Service）

IAAS 基础设施即服务（Infrastructure as a Service）

4. 总体要求

4.1. 通用性

应服务所有群体。保证残障人士、老年人、受教育程度较低的群体能方便地使用相关功能。

4.2. 可扩展性

应综合考虑广西壮族自治区住房和城乡建设信息化建设项目的架构设计，为建成后的运营、维护预留扩展空间。

4.3. 经济性

应统筹规划广西壮族自治区住房和城乡建设信息化建设，提高建设过程中各方协作效率，减少重复投入。

4.4. 人性化

应基于用户的真实需求、使用习惯、认知及操作能力进行设计，简化用户使用流程，减少材料提交数量。

5. 总体架构

5.1. 概述

数字住建信息化项目按照分层设计的架构分为“四层四体系”，“四层”分别是基础设施层、基础支撑层、应用服务层和用户展示层，“四体系”分别是安全管理体系、运维保障体系、研发管理体系、建设标准规范管理体系。

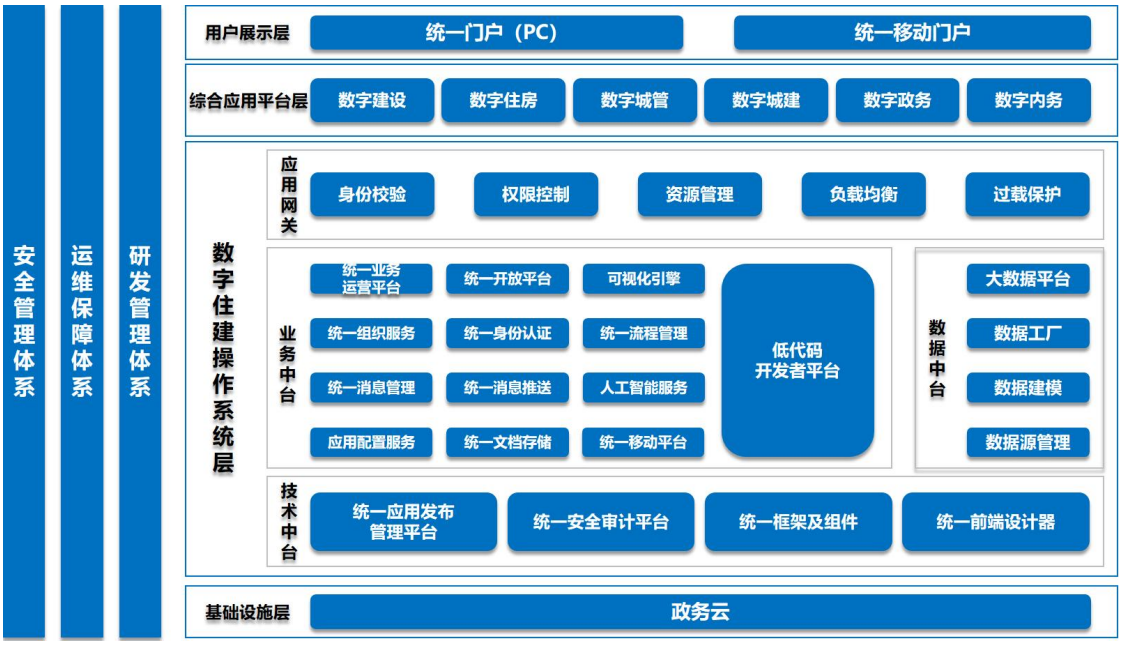


图 5-1-1 数字住建信息化项目总体框架

5.2. 用户展示层

用户展示层提供统一两个门户入口：统一门户主要为网页终端用户提供网页应用登录的统一入口；统一移动端门户主要为公众用户办事提供移动端统一入口。

5.3. 应用服务层

应用服务层是基于数字住建基础支撑平台提供的业务服务、数据服务和标准规范，改造、迁移、建设各类业务应用。当前规划主要包括：数字建设、数字住房、数字城管、数字城建、数字政务和数字内务。后续业务可接入或新建其他应用系统。

5.4. 基础支撑层

基础支撑层包括技术中台、业务中台、数据中台，为业务应用服务层提供具有可复用价值、可扩展的业务服务、数据服务。

5.5. 基础设施层

基础层是政务云，为数字住建信息化系统提供一体化云计算资源承载及网络支持。

5.6. 安全管理体系

安全管理体系基于政务云平台安全管理基础，提供等级保护服务和相关应用安全保护措施。

5.7. 运维保障体系

运维保障体系为各应用系统的云服务运行环境和应用运行提供上线维护、性能监控、异常告警、运营分析服务，为运维工作提供管理规范的相关保障。

5.8. 研发管理体系

研发管理体系为各应用研发工作提供管理规范、工具手册、研发协作的全方位保障。

5.9. 建设标准规范管理体系

标准规范体系定义了资源与基础支撑平台、各应用子系统的建设标准和规范，包括接口规范、业务标准、数据标准定义，开发规范等内容。标准规范体系是保证平台各系统能够持续演进，不断升级迭代的基础。

6. 功能规范

6.1. 功能建设要求

避免重复建设的要求。在广西壮族自治区住房和城乡建设厅信息化项目中台能力清单中已经提供的相同或类似的功能，不允许合作伙伴及开发厂商重复建设。广西壮族自治区

住房和城乡建设厅信息化项目包含如 6-2-1表 广西壮族自治区住房和城乡建设厅信息化项目中台能力，对于“使用要求”定义为“强制”的，合作伙伴及开发厂商建设业务系统时必须按照信息化项目对接要求接入；对于“使用要求”定义为“可选”的，无需要可不用，如需使用相应场景功能时，必须调用中台对应能力，不允许合作伙伴及开发厂商另行建设。

6.2. 平台中台能力清单

分类	主题	中台能力	使用要求	应用
融合业务基础服务	基础信息管理	企业信息管理	强制	提供企业基本信息接口调用，为业务系统提供查询企业的相关基本信息。
		个人信息管理	强制	提供个人基本信息接口调用，为业务系统提供查询个人的相关基本信息。
		行政编码管理	强制	提供行政编码信息接口调用，为业务系统提供查询行政编码的相关信息。
	工程项目管理中心	项目基本管理	强制	提供项目基本信息接口调用，为业务系统提供查询项目的相关基本信息。
		施工许可管理	强制	提供施工许可信息接口调用，为业务系统提供查询施工许可的相关信息。
		施工图审信息管理	强制	提供施工图审信息接口调用，为业务系统提供查询施工图审的相关信息。
		招投标信息管理	强制	提供招投标信息接口调用，为业务系统提供招投标的相关信息。
		竣工验收信息管理	强制	提供竣工验收信息接口调用，为业务系统提供查询竣工验收的相关信息。
	诚信评分管理	企业信用管理	可选	为各业务系统办理记录企业获奖、企业表彰、企业质量安全事故、行政处罚、通报批评、企业黑名单等信用信息、加减诚信分基础数据信息，并对该信息进行管理。
		个人信用管理	可选	为各业务系统提供个人信用良好行为、个人不良行为、个人黑名单等个人信用信息的服务能力。
		信用评分管理	可选	为业务系统计算诚信分值提供评判规则、对各种信用评判规则与相关业务系统中的评分信息进行管理功能。
		信用发布管理	可选	为各业务系统提供企业获奖、企业表彰、企业质量安全事故、行政处罚、通报批评、企业黑名单等信

分类	主题	中台能力	使用要求	应用

				息、个人执业信用、注册信用、其他良好信用、信用变更、信用发布等服务能力。
		信用查询管理	可选	为各业务系统提供查询企业获奖、企业表彰、企业质量安全事故、行政处罚、通报批评、企业黑名单等信息、个人执业良好信用、注册良好信用、其他良好信用变更信息、个人黑名单、个人执业不良信用、注册不良信用、其他不良信用信息等各类信用信息的查询服务。
		信用变更管理	可选	为各系统中的信息提供企业获奖、企业表彰、企业质量安全事故、行政处罚、通报批评、企业黑名单等信息、个人执业良好信用、注册良好信用、其他良好信用信息、个人黑名单、个人执业不良信用、注册不良信用、其他不良信用信息进行变更的服务能力。
	设备管理中心	设备基本信息	可选	为各业务提供设备基本信息，供设备管理及相关监督系统开展报备业务、应用审 批业务。
		设备厂商管理	可选	为各业务系统提供设备生产备案、产权备案、应用备案及事故追责业务的服务能力。
		设备入场管理	可选	为企业项目进行设备应用、设备监督提供备案及审批验收服务能力。
		设备保养管理	可选	为监督管理系统提供报备信息、保养超期预警、事故追责信息。
		设备拆装管理	可选	为各系统提供设备应用环节合法性监管服务能力、为安全监测信息系统提供位置信息、安装数量信息。
		设备状态管理	可选	为各业务厅提供人员驾驶设备履历信息、为监测信息系统提供设备应用状态信息。
	住房及公积金管理中心	房屋基本信息	可选	为各业务提供房产项目基本信息，供各系统开展房产销售备案、交易业务、公积金办理业务能力。
		住房信息管理	可选	为各业务系统办理住房登记、住房交易、住房贷款、产权证明提供数据信息。
		公积金缴存管理	可选	为企业及个人用户提供公积金缴存、查询业务。
		公积金申请服务	可选	为个人用户提供公积金提取、状态信息查询服务能力。
		公积金贷款管理	可选	为相关系统提供公积金贷款办理，贷款涉及房产信息、个人信息服务能力。
	专家信息管理	专家基本信息	可选	为组织专家入库、专家资格评审等提供专家基础信息，为后续参加项目评审、验收等工作提供基础信息支撑。

分类	主题	中台能力	使用要求	应用
	中心	专家单位管理	可选	是对于符合资格的专家建立在线专家个人档案补充，管理专家的职业道德、工作成绩等指标。
		专家履历管理	可选	对该专家的专业理论水平、实际工作能力、职业道德、工作成绩、沟通能力、技术能力进行在线记录用于线下评审该专家是否符合任职资格。
		专家抽取管理	可选	为质量安全监督管理、施工图纸审查、消防设计审批提供专家评审，通过系统自动进行专家抽取、自动通知实现专家管理的自动化，摆脱人为因素，实现项目论证的公平透明性。
统一门户管理服务	门户管理中心	对外门户管理	强制	对外部人员或单位提供登录查询、业务办理等服务能力。
		对内门户管理	强制	使自治区住房和城乡建设厅上下有一个完全共享的信息空间、交流空间。
		个人门户管理	强制	把个人日常工作、新闻公告、文档以及其他关联资源等统一展示，提供充分的信息资源整合。
		集成资源管理	可选	系统将集成的发起和接收相关内外事件和接口，以资源形式进行统一语义化注册，为统一管理和配置化集成提供基础支持。
门户公共信息服务	用户管理中心	用户注册服务	可选	为各个系统提供统一的用户注册服务能力，实现一次注册，全部通用业务赋能。
		用户登录服务	可选	为各个系统提供统一的用户登入登出的服务能力。
		组织同步服务	强制	为各个系统提供组织数据同步的服务能力。
		组织机构管理	可选	为各个系统提供统一的组织机构管理维护与信息权限管理调用的服务能力。
统一身份认证服务	统一认证中心	应用导航管理	强制	提供统一的登录入口、应用访问入口及应用导航、访问控制的功能。
		单点登录管理	强制	提供各系统的单点登录接入服务，支持PC端和移动端，移动端通过H5页面接入。
		门户权限管理	强制	提供各系统接入门户后，其相应的权限分配或功能模块的禁用开启的服务。
		身份认证管理	可选	为各个系统提供统一的身份认证服务能力，包含多种认证类型，短信认证、人脸认证，打款认证，自然人要素，企业要素等。
统一流程管理服务	统一流程中心	流程设计	强制	为各系统提供系统内外协同办公、过程审批等流程服务能力。
		开发节点	可选	开发节点可以执行一些特定的动作，定制工作流开发节点，实现自定义动作如解锁账号、创建邮箱、

分类	主题	中台能力	使用要求	应用
				发送邮件等、跨单位调动人员等。
		事件管理	强制	为各系统流程深度集成提供节点事件开发，基于工作流的节点的不同的处理事件，调用外部第三方系统。
		流程接口	可选	提供系统内置常见的业务场景需要的，BPM接口提供第其他系统调用服务。
统一待办管理服务	统一待办中心	应用接入管理	强制	提供各外部系统提供应用注册、接入配置、应用注销等应用统一待办接入门户的服务能力。
		用户绑定管理	强制	提供各系统调用的用户绑定接口，完成两个系统之间的用户关系绑定，达到点对点的效果。
		待办信息管理	强制	为了各个系统提供统一待办信息生成、路由、转发、处理、更新状态的服务能力。
		检验穿透服务	强制	提供各系统接入待办中心，流程审批的穿透处理服务。
统一消息管理服务	消息管理中心	消息配置管理	强制	为各系统提供消息类型、消息模板、消息规则等等服务能力。
		消息组装服务	强制	为各系统提供消息的组装服务能力。
		消息分发服务	强制	为各系统提供分发消息的服务能力。
		消息发送服务	强制	为各系统提供发送消息的服务能力。
AI人工智能服务	AI应用中心	人脸识别	强制	为各系统提供实人身份认证的服务能力。
统一日志管理服务	统一日志管理中心	日志采集管理	强制	为各个系统提供日志名称、日志路径、存储目标等信息维护的服务能力。
		日志处理服务	强制	为各个系统提供日志拆解、日志合并等日志预处理的服务能力。
		日志分析管理	强制	为各个系统提供日志类型、分类统计等日志分析的服务能力。
		日志信息查询	强制	为各个系统提供归属应用，产生时间， 日志内容，日志级别等日志信息查询的服务能力。
监控管理服务	监控管理中心	问题跟踪处理	可选	为各系统的日常问题提供流程化工单闭环能力，包括事件工单、问题工单等。
		基础资源管理	可选	为各系统基础资源提供统一录入管理的能力，包括主机资源、CPU，内存，硬盘等。

分类	主题	中台能力	使用要求	应用
		监控应用端口	可选	为各系统提供应用端口监测的服务能力。
		监控应用URL	可选	为各系统提供应用URL监测的服务能力。
		监控应用服务	可选	为各系统的应用服务提供服务存活探测、服务进程名称、进程标识、进程启动时间、进程持续运行时间等指标的监测能力。
		监控容器服务	可选	为各系统提供容器名称、容器状态、容器资源等信息监测的服务能力。
		监控硬件指标	可选	为各个系统提供硬件资源使用信息监测的服务能力。
		监控业务指标	可选	为各个系统提供业务调用信息监测的服务能力。
统一安全审计服务	统一审计管理中心	认证管理	强制	为运维人员提供统一身份认证，实现统一的密码策略，并且增强动态口令等强认证模式，实现用户身份有效的鉴别机制。
		单点登录	强制	统一运维人员登录入口，实现运维人员登录统一来源管理，为用户实现SSO功能，可托管服务器用户名口令，不需要运维人员知道高账号口令即可登录运维。
		授权管理	强制	对运维人员进行最严格权限管控，可为每个运维人员设置可登录来源IP、可登录时间、可运维的主机系统、可使用的操作系统账号、可运行的操作命令，最大降低系统操作风险。
		审计管理	强制	运维人员操作过程进行录像审计，可对运维人员操作进行实现监控，可断开进行的高危操作，可分析出运维人员执行的操作命令。
		应用管理	强制	可为运维人员发布B/S及C/S程序，指定运维人员可登录的URL地址和C/S客户端可登录的对象，并且运维人员对应用的操作可实现录屏审计。
应用配置管理服务	配置管理中心	配置统一管理	可选	为基础支撑平台提供统一界面来管理不同集群，环境以及命名空间的配置，并且支持多个不同应用共享同一份配置的能力。
		配置发布管理	可选	为基础支撑平台提供配置项，配置值、配置发布历史记录的服务能力。
		配置信息管理	可选	为基础支撑平台的各应用提供统一的业务配置、应用配置、网络配置、数据库配置等其他配置信息设置的服务能力。
		配置分类管理	可选	为基础支撑平台提供业务配置、应用配置、网络配置、数据库配置等不同类型配置分类管理的能力。

分类	主题	中台能力	使用要求	应用
		配置导入导出	可选	为基础支撑平台提供配置信息批量导入导出的服务能力，方便系统迁移。
统一文档存储服务	文件管理中心	文件空间管理	强制	为各个系统提供存储对象容器的服务能力。
		文件上传服务	强制	为各系统提供非结构化文件统一上传的服务能力。
		文件下载服务	强制	为各系统提供非结构化文件统一下载的服务能力。
		文件删除服务	强制	为各系统提供非结构化文件统一删除的服务能力。
		文件元信息服务	可选	为各系统提供文件元信息查询的服务能力。
数据共享开放	数据交换中心	元数据信息	强制	为各业务系统查看数据的描述信息。
		数据资产目录	强制	为各系统提供目录分类查询、关键字查询等方式检索查看已经发布成资产的资产目录，可查看表信息、使用说明、字段说明、进行数据预览等。
能力共享开放平台	能力共享开放平台	能力上架	强制	为各系统提供系统上线申请，上线审批，上线发布的服务。
		能力下架	强制	为各系统提供系统下线申请，下线审批，下线处理的服务。
		调用统计	强制	为各个业务提供系统服务使用情况统计分析。
		能力申请	强制	为各个系统申请使用平台功能提供申请审批、颁发系统接入信息的服务。
		用户中心	强制	提供门户用户中心的信息获取、信息同步、管理等服务。
		组织架构	强制	提供门户组织架构的获取、同步、子应用的组织架构管理等服务。
		短信服务	可选	为应用提供短信发送、短信验证码校验等服务。
		文件库能力	可选	为应用提供文件、文件夹的上传、下载以及管理等服务。
		应用配置服务	可选	为应用提供统一的配置数据，包括业务数据、行政编码、节假日等。
		企业基本信息查询	可选	提供基于企业名称、统一社会信用代码的精确查询服务，其中企业名称和统一社会信用代码至少输入一项，返回结果为企业记名所需的企业基本

				信息（含省局节点号）。
		国家人口身份核验	可选	通过公民身份号码、姓名，在国家人口库中确认是否存在该人信息，反馈核查结果和死亡标识。
		企业基本信息验证	可选	提供企业照面信息比对验证服务，通过输入企业照面相关信息，其中企业名称和统一社会信用代码至少输入一项，其他比对字段可选。比对结果包括输入条件、比对企业登记状态、比对结果、比对差异详细等内容。
		企业开办四要素核验	可选	提供基于统一社会信用代码的精确查询服务，输入统一社会信用代码，返回结果为企业开办需要的四要素。查询结果为一条，返回单条结果。
低代码开发平台	低代码开发平台	业务建模	可选	各业务系统可以通过拖拉拽使用业务建模做对应业务的字段以及字段的类型。
		表单建模	可选	各业务系统可以通过拖拉拽使用表单建模做业务表单页面，提供给用户进行业务表单新建，编辑，查看等。
		列表页面建模	可选	各业务系统可以通过拖拉拽使用列表页面建模做对应的业务操作界面，如：列表、搜索栏、操作按钮等等，让用户拥有非常友好的使用界面。
		流程建模	可选	各业务系统可以通过拖拉拽使用流程建模做符合业务的工作流程，任务流程，审核流程等。
		报表BI建模	可选	各业务系统可以通过拖拉拽使用报表BI建模做数据可视化分析，形成对应的报表，自助分析，大屏可视化等。

6-2-1 表 广西壮族自治区住房和城乡建设厅信息化项目中台能力

7. 接入规范

7.1. 接入要求

对接入方要求如下：

（1）接入方应按照广西壮族自治区住房和城乡建设信息化建设项目运营方的要求配合开发应用程序。

（2）入驻广西壮族自治区住房和城乡建设厅数字住建信息化基础支撑平台的应用及子系统由平台运营方统一发布和更新。

（3）接入方应配合平台运营方的安全检测，填写调查信息，修补安全漏洞。

（4）接入方应配合平台运营方的功能和压力测试团队，在上线前完成功能和压力测试。

7.2. 接入流程

7.2.1. 整体流程

接入流程包含接入方登入平台、查找能力、申请能力、申请审核，管理方授权，接入方查看申请能力列表，查看能力使用详情，根据需求调用能力，整体流程参见图7-2-1。

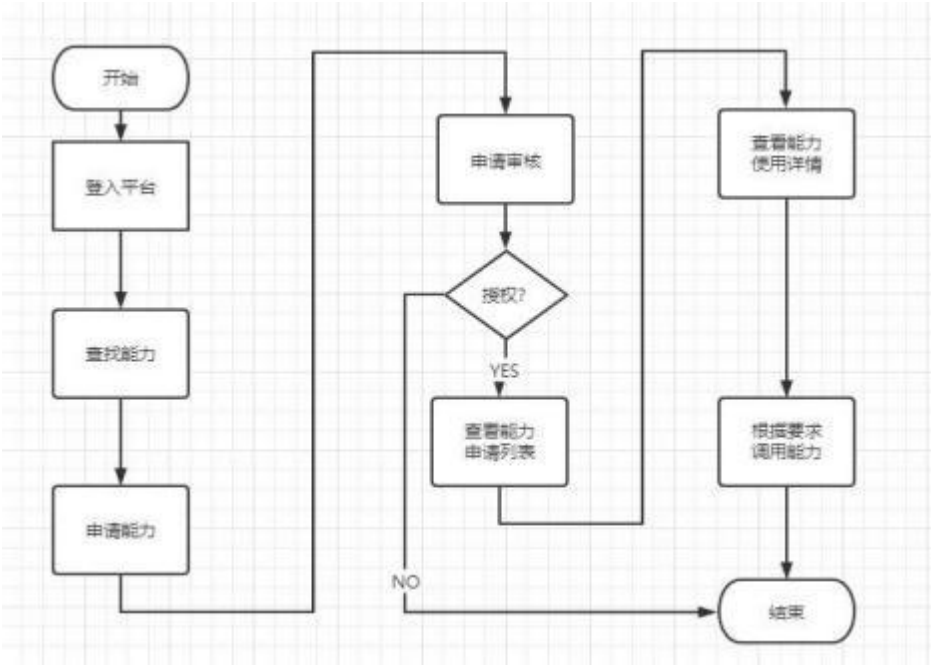


图 7-2-1应用接入基础支撑平台流程

7.2.2. 登入平台

接入方确认需求后，向管理方申请基础支撑平台帐号和密码，并登入平台。

7.2.3. 查找能力

接入方根据关键字在平台中查找相应的业务能力或者向运营方技术人员咨询相关能力。

7.2.4. 申请能力

接入方根据业务需要申请相应的业务能力。

7.2.5. 申请审核

管理方对接入方的申请进行审核，审核通过则给接入方授权，审核不通过则流程结束，并标注不通过原因。

7.2.6. 查看能力申请列表

接入方查看能力申请列表，查阅自己所申请的能力。

7.2.7. 查看能力使用详情

接入方查看能力使用的详情信息，获取接入详细信息。

7.2.8. 根据要求使用能力

接入方根据能力使用要求，在应用中配置相应的 appid 和 key，调用能力。

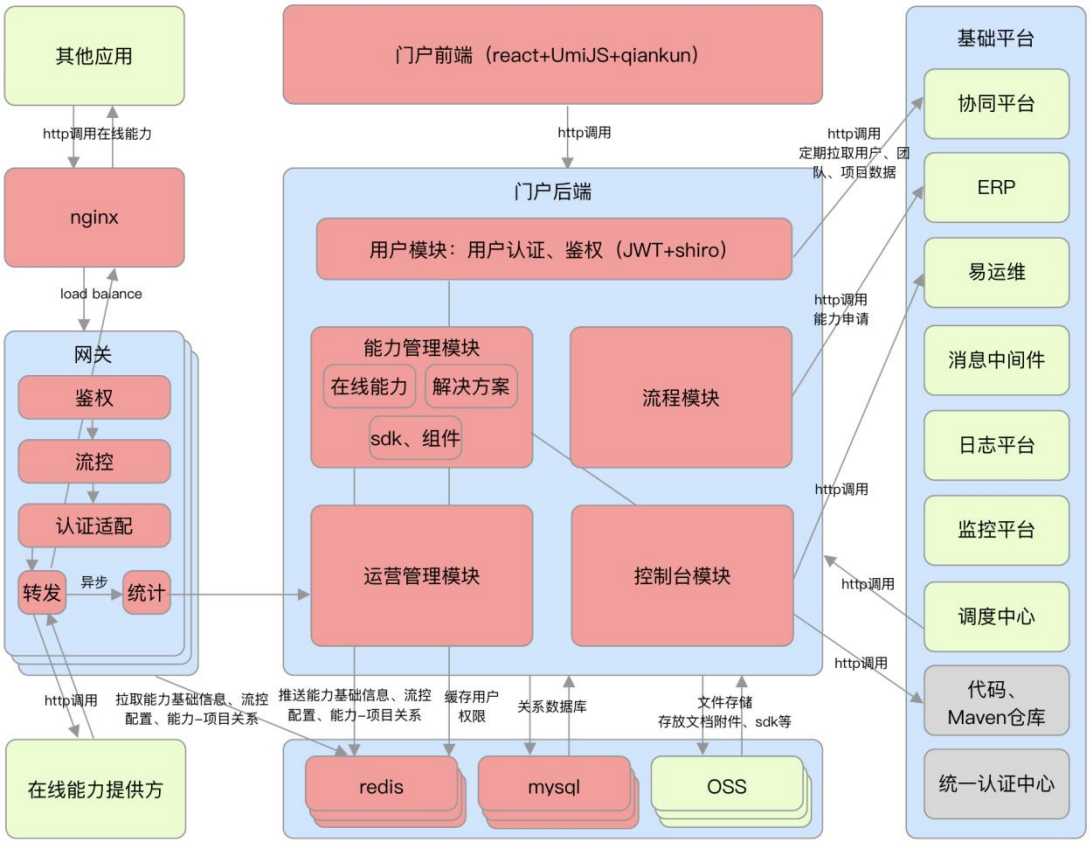
7.3. 接入技术要求

7.3.1. 接口集成

各业务系统应开放接口，汇聚能力到基础支撑平台。各业务系统的接口应按照支撑平台的接入规范与基础支撑平台对接。业务系统应提供 HTTP/HTTPS RESTful 接口，报文应使用 JSON 格式。公共能力以标准 API 对外提供服务。

7.3.2. 能力注册与发布

各业务系统接入基础支撑平台或调用支撑平台上的服务前，应先向管理方申请创建应用，通过应用对服务进行提供和调用操作。具体设计如下所示



门户前端实现主应用中接入各类使用不同技术栈子应用模式，实现前后端可独立开发，部署完成后主框架自动完成同步更新。

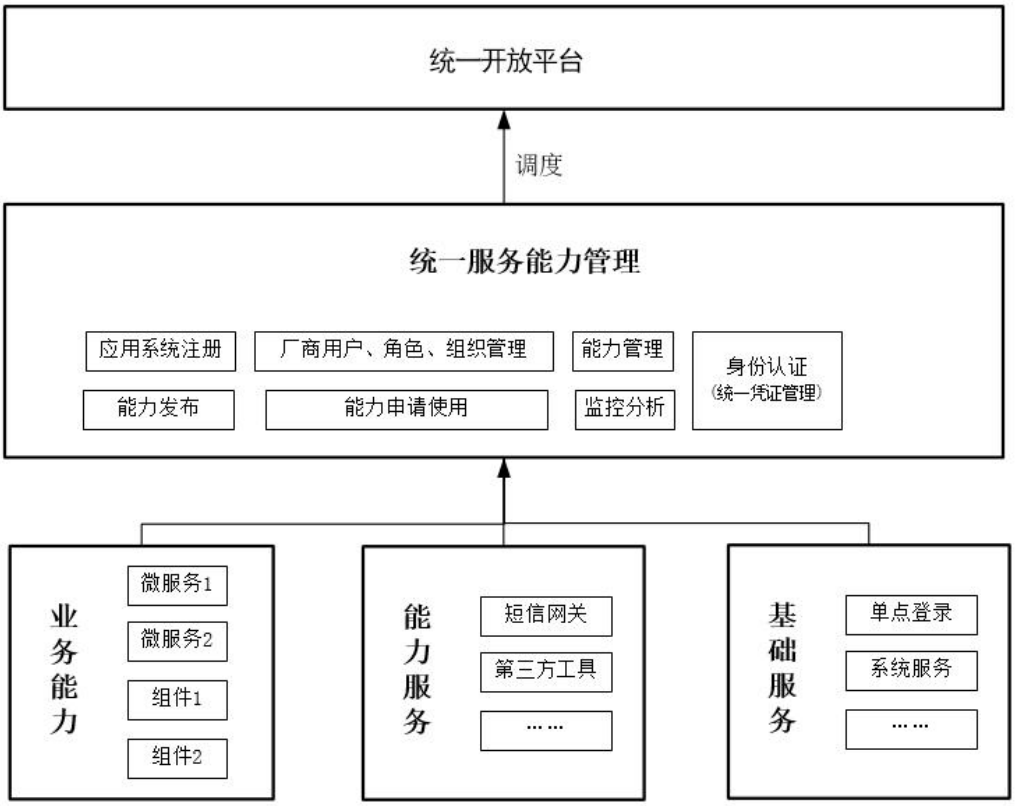
门户后端包括用户模块、能力管理模块、流程模块、运营管理模块以及控制台模块。使用统一的用户模块实现用户认证、鉴权等功能。实现统一能力管理中心，提供微服务及组件服务的托管服务，涵盖能力的创建、发布、管理、使用的全生命周期管理。流程模块实现开放平台流程的管理、设计以及监控等功能。运营管理模块实现平台数据的统计分析、用户权限分配、应用管理等功能。

网关服务在对接其他应用时起到鉴权、流量控制、认证适配以及转发等作用。

数据持久化存储层包括redis、mysql、oss分别用于缓存、数据存储以及文件存储等功能。

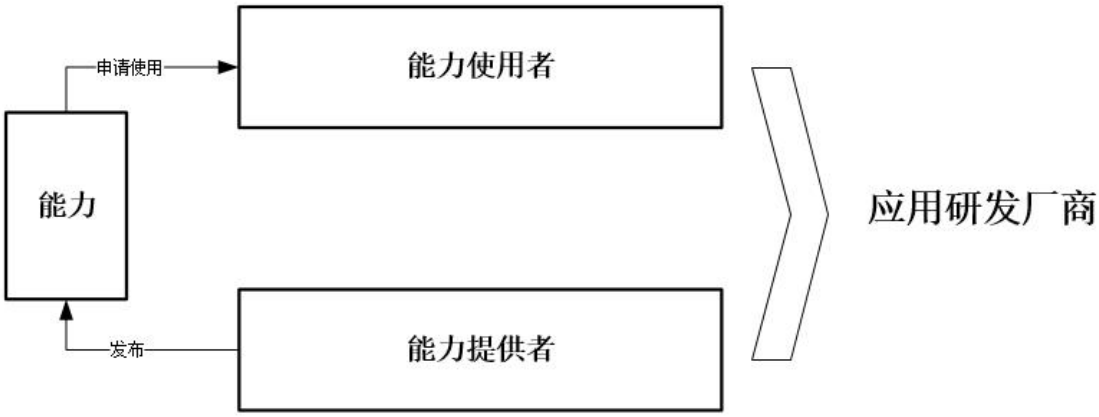
能力提供

服务提供方在提供给接入方各业务系统调用前，应在基础支撑平台以应用的身份发布服务，填写接口、文档等信息，并通过运营方审核后上架该能力。上架能力后，平台提供统一能力管理中心，实现微服务及组件服务的托管服务，涵盖能力的创建、发布、管理、使用的全生命周期管理，方便资源统一管理和运用。辅助用户简单、快速、低成本、低风险的实现微服务聚合、前后端分离、系统集成，向各个业务系统承建单位开放功能和数据。示意图如下：

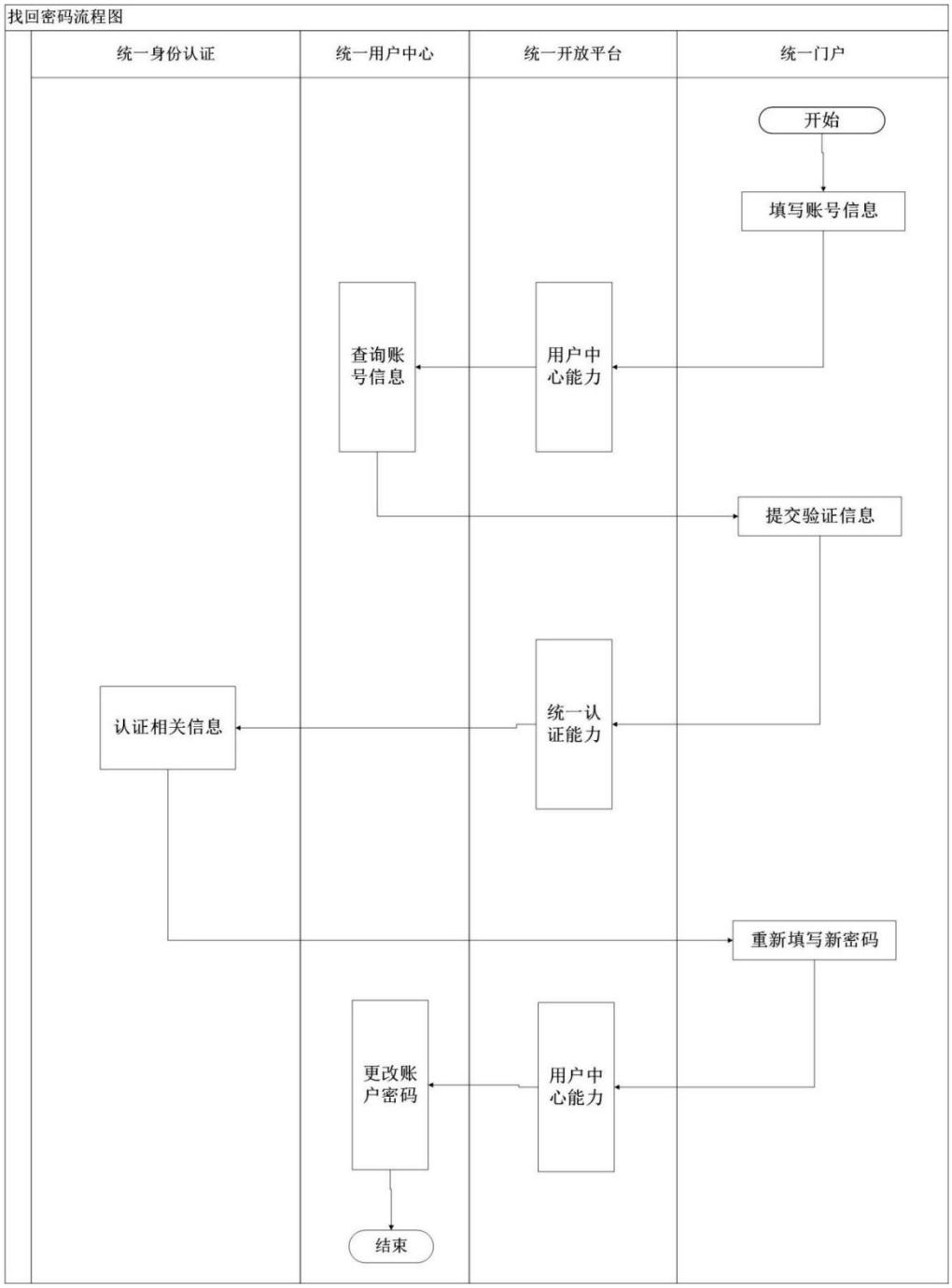


能力调用

调用能力方在使用能力前，向基础支撑平台以应用的身份申请使用能力，通过审批后，通过创建应用时获取的appKey 和 appSecret作为凭证对能力进行调用。



服务提供及调用流程示例如下所示：



统一门户填写找回密码的账号信息后，通过开放平台挂载的用户中心能力对账户的真实性进行查询，如存在该账户则在统一门户中跳转至填写验证信息，用户填写完验证信息后通过开放平台挂载的认证能力对信息进行验证，如果验证通过则返回统一门户，让用户进行新密码的设置，设置提交后通过开放平台对用户中心相应的账户进行更新密码操作。

7.3.3. 能力调用样例

所有的接口应使用 HTTP 或 HTTPS 协议、JSON 数据格式、UTF8 编码。

7.3.3.1. SDK 使用说明

在调用能力时可以通过 SDK 封装的方法自动生成。在项目中通过引用 SDK 的 jar 包和提供调用能力的方法封装，通过父类-AbstractHttpServiceAdapter 中的 httpPostJson 方法实现请求。

7.3.3.2. 移动端接入说明

接入的厂商如需实现移动端，必须提供标准的 H5 页面支持。移动端的加密方式、安全握手和 PC 端保持一致。

7.3.3.3. 能力参数说明

服务基本属性包含但不限于表 7.3.3-1

序号	属性	说明	取值说明
1	ID	项目的唯一标识	
2	项目名称	项目中文名称	
3	appKey	应用关键字，系统自动分配	
4	appSecret	应用秘钥，系统自动分配	点“显示”展示明文。
5	操作	重置	重置appSecret

接口基本属性包含但不限于表 7.3.3-2

序号	属性	说明	取值说明
1	ID	能力的唯一标识	
2	能力描述	能力功能简明扼要描述	
3	联系人	能力提供者	
4	联系电话	能力提供者的电话	
5	能力状态	能力上架、下架状态	上架、下架

请求消息头 Header 基本属性包含但不限于表 7.3.3-3

序号	属性	说明	取值说明
1	appKey	项目标识	
2	apiCapKey	接口标识/能力标识	
3	x-ca-nonce	参数加签随机串	
4	x-ca-timestamp	时间戳	
5	x-ca-signature-headers	x-ca-timestamp， x-ca-nonce， x-ca-signature-method	参数加签项固定值

6	x-ca-signature-method	HmacSHA256	参数加签加密算法固定值,使用SHA-256生成哈希值的HMAC算法
7	x-ca-Signature	参数加签结果	根据加签算法计算结果

接口请求参数基本属性包含但不限于表 7.3.3-4

序号	属性	说明	取值说明
1	名称	服务名称	
2	apiCapKey	接口标识	系统分配
3	URL	调用该接口的URL	
4	请求协议	可选HTTP、HTTPS协议	
5	请求方法	调用该接口的调用请求方法	参数加签项固定值
6	请求头	进行接口进行概述调用时的请求头	参数加签加密算法固定值,使用SHA-256生成哈希值的HMAC算法
7	超时时间	调用该接口的超时时间（单位ms）	根据加签算法计算结果
8	QPS配置	QPS限流值	不同接口不一样
9	限流策略	直接拒绝	达到限流值直接拒绝
10	QPS开关	启用QPS参数	ON/OFF
11	描述	对该接口进行概述	

接口入参基本属性包含但不限于表 7.3.3-5

序号	属性	属性位置	属性类型	必填属性	描述
1	eventInfo	Body	String	是	事件描述
2	eventIp	Body	String	是	IP地址
3	eventTime	Body	String	是	事件时间
4	eventType	Body	String	是	事件类型
5	remark	Body	String	是	备注

接口出参基本属性包含但不限于表 7.3.3-6

序号	属性	属性位置	属性类型	必填属性	描述
1	data	Body	String	是	接口返回体： {"data":{ "id":"b1976831be5c4619be"}}
2	success	Body	String	否	true/false
2	code	Body	String	是	参考具体接口描述
3	message	Body	String	是	参考具体接口描述
4	operate	Body	String	是	操作描述如： 审计日志保存
5	page	Body	String	否	分页信息

7.3.3.4.能力入参样例

```
{
    "eventInfo": "事件描述",
    "eventIp": "IP地址",
    "eventTime": "事件时间",
    "eventType": "事件类型",
    "remark": "备注"
}
```

7.3.3.5. 能力出参样例

```
{
    "data": { "id":"b1976831be5c4619be"},
    "code":100,
    "message":"成功",
    "operate":"审计日志保存",
    "page":null
}
```

7.3.3.6. 接口的返回码

接口返回码 code 基本信息描述包含但不限于表 7.3.6-1

code	**描述(message)**	**推荐解决办法**
100	调用成功	
101	能力或项目不存在	检查appKey和apiCapKey参数是否正确
103	无访问能力权限	检查appKey和apiCapKey参

		数是否正确
105	系统异常	联系管理员
121	下游能力连接失败	稍后再试或者联系管理员
123	调用下游能力失败,认证异常	联系管理员
125	调用下游能力失败,客户端异常	联系管理员
127	调用下游能力失败,服务器异常	联系管理员
129	未知返回码	联系管理员

7.4. 系统要求

7.4.1. 安全要求

各业务系统接入基础支撑平台的安全要求参见“安全规范”说明。

7.4.2. 性能要求

为保证数字住建信息化项目用户体验，接入的业务系统性能应达到普通等级，宜达到优秀等级。性能通过 TPS、响应时间、请求成功率衡量，等级划分如下：

（1） TPS 等级见表 1。

表 1 TPS 等级

TPS	>500	100-500	<100
等级	优秀	普通	待改进

（2）响应时间指系统对请求作出响应的时间，其等级见表 2。

表 2 响应时间等级

响应时间	0-1 秒	1-3 秒	>3 秒
等级	优秀	普通	待改进

（3）请求成功率指成功返回结果的请求数占总请求数比例，其等级见表 3。

表 3 请求成功率等级

请求成功率	95%-100%	90%-95%	<90%
等级	优秀	普通	待改进

8. 技术规范

8.1. 技术中台技术要求

技术中台要求接入数字住建基础支撑平台的业务系统应满足在容器、微服务、数据

库及消息中间件等进行的技术规范。

8.2. 容器技术要求

容器技术包括集群管理、应用管理、运维管理、镜像管理、容器云平台兼容、容器编排、容器调度功能。

8.2.1. 应支持容器集群管理

（1）应支持跨区域容器集群统一管理，提供跨区域灾备、业务流量分担。

（2）应提供功能全面的图形化控制台对容器集群资源进行可视化管理。

8.2.2. 应支持容器应用管理

（1）应支持无状态、有状态、任务、定时任务、DaemonSet 等工作负载对象部署，并支持应用模板和配置项(ConfigMap)的管理。

（2）应支持工作负载的自动弹性伸缩。

8.2.3. 应支持容器运维管理

（1）应支持对容器集群、应用资源监控。

（2）应支持告警和容器内日志采集。

8.2.4. 应支持容器镜像管理

（1）应提供 Web 控制台界面、命令行工具或 Docker Registry API 方式管理容器镜像生命周期。

（2）可支持镜像自动同步，将最新推送的镜像自动同步到其他区域镜像仓库内，兼容并维护不同 CPU 架构下的容器镜像。

（3）可支持容器云兼容不同云平台。

8.2.5. 容器编排

（1）应提供对容器化的应用程序进行规划、部署、管理和扩展的功能。

8.2.6. 容器调度

（1）应根据资源的可用性、负载情况等因素动态地分配和管理容器。

8.3. 微服务技术要求

（1）可具备微服务开发架构。

（2）可支持应用能够独立部署、更新、重启、水平扩容等功能。

（3）可支持应用间同步、异步通信方式，如 RESTful、RPC、消息中间件等方式。

（4）可具备服务限流和降级的功能。

（5）可具备熔断功能。

（6）可支持微服务健康度检查，出现问题的时候可快速定位问题。

8.4. 数据库技术要求

（1）应支持关系型数据库及非关系型数据库。

（2）应提供多个品牌和版本数据库服务，如支持人大金仓/达梦。

（3）应支持查询及监控数据库服务使用的资源情况。

（4）应支持关系型数据库及非关系型数据库高可用，可伸缩。

（5）应支持信创数据库。

（6）应支持数据库审计功能，包括报表功能，性能监控等。

8.5. 消息中间件技术要求

（1）应支持创建、配置、更新、启动、停止各种类型的消息中间件。

（2）应支持信创中间件产品。

（3）应支持分布式消息中间件，如 kafka 等开源产品。

9. 安全规范

9.1. 概述

接入广西壮族自治区住房和城乡建设信息化建设项目的各业务系统软件开发厂商及合作伙伴应满足在物理安全、网络安全、数据安全、系统安全、应用安全和安全管理等的规范要求。最终要求以各个系统的等级保护和密码应用安全性评估为准。

9.2. 物理安全

（1）机房物理环境安全应合理设计机房、配电、冷却、安防、防雷、消防等场地设施，同时应按容错系统配置，在电子信息系统运行期间，场地设施不应因操作失误、设备故障、外部电源中断、维护和检修而导致电子信息系统运行中断。

（2）进入机房的硬件设备，应符合GB4943.1-2022的相关要求。

9.3. 网络安全

9.3.1. 网络安全构架与风险分析

广西壮族自治区住房和城乡建设信息化建设项目运营商提供基础信息服务。企事业单位用户可通过电子政务外网方式接入基础支撑平台；为了保证传输速度，基础支撑平台的音频视频等大数据可以通过政府机构机关各部门各单位及其他关联指挥或运营中心专网接入基础支撑平台；同时基础支撑平台为公众用户提供无线APP的接入方式。

9.3.2. 边界安全

接入广西壮族自治区住房和城乡建设信息化建设项目的各业务系统软件开发厂商及合作伙伴在边界安全上应符合以下要求。

（1）专网边界能实现各业务系统和专网的物理边界隔离。隔离包括采用传统的安全设备，且应具有数据智能，能感知未知威胁；能实现联动智能，对网络进行协同防御。

（2）对于建在政务云上的业务系统，应实现和公共信息平台的虚拟化网络边界隔离，包括虚拟化网络内部隔离和虚拟机内部隔离。

（3）国家电子政务外网及公共信息平台的边界接入安全，应坚持分级部署原则和属地化接入原则，能实现统一入口、VPN网关集群、统一认证和鉴别、管理与审计、安全防护等安全要求。

（4）部署的VPN产品应符合GB/T32922-2016的相关要求。

（5）专网的边界接入安全应满足边界可控、数据交换可控、对接入用户可管理、对终端、网络、应用和数据有安全保护措施的要求。

（6）确保智能移动终端硬件安全、操作系统安全、外围接口安全、应用层安全和用户数据保护安全的要求。

9.3.3. 访问控制

访问控制应符合以下要求：

（1）应对非涉密政府信息中敏感信息和一般信息，及政府业务类型中一般业务、重要业务和关键业务定义不同的访问控制策略。

（2）应具有对政府用户、企业用户、公众用户、运维用户等不同的身份鉴别机制，能限制用户对数据信息的访问能力及范围，确保信息资源不被非法使用和访问。

（3）应在不同等级的网络区域边界和虚拟化网络边界部署访问控制设备，设置访问控制规则，依据安全策略控制虚拟机间的访问。

（4）信息系统的访问控制应符合GB/T22239-2019中的相关要求，部署的访问控制设备，例如防火墙等应符合GB/T20281-2020或相关设备要求。

9.3.4. 入侵检测

各业务系统入侵检测应符合以下要求：

（1）对常见攻击行为，包括端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等，能检测、记录并告警。

（2）对恶意代码，应能检测和清除，对恶意代码库应保持升级和更新。

（3）采用云平台建设的业务系统，对虚拟机或对宿主机资源的异常访问、虚拟机之间的资源隔离失效、非授权新建虚拟机或者重新启用虚拟机、恶意代码感染以及在虚拟机间蔓延的情况，能检测、记录并告警。

（4）应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击（例如基于行为特征对0-day漏洞、APT攻击等）的检测分析，并采取防御措施。

（5）对DDOS攻击应具有检测能力，并采取防御措施。

（6）部署的入侵检测系统应符合GB/T20275-2013中的相关要求。

9.3.5. 安全审计

各业务系统的安全审计应符合以下要求：

（1）审计系统应包括日志审计、数据库审计、审计分析等不同的审计功能，审计过程中用户无法中断审计进程，无法删除、修改或覆盖审计记录，同时能及时对安全事件进行预警，并展示安全趋势。

（2） 日志审计的范围应包括通讯日志、访问日志、内容日志等； 日志审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，具有对审计记录数据进行统计、查询、分析及生成审计报表的功能。

（3）安全审计系统可提供相应API，将日志提供给用户，用户可根据日志信息自行审计或接入第三方审计系统进行相关审计。

（4）应对运维人员的全部操作记录进行安全审计。

9.3.6. 可用性保证

各业务系统的可用性保证应满足以下要求：

（1）应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。

（2）应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

9.4. 数据安全

各业务系统的数据安全应符合以下要求：

（1）用于业务运行和数据处理及存储的物理设备应位于中国境内。

（2）应符合GB/T22239-2019中二级的相关要求，通过数据加密、数据销毁、数据防泄漏、数据备份等技术手段，确保数据全生存周期中数据产生、访问、传输、存储到销毁各环节数据安全能力。

（3）各业务系统中涉及的公共基础数据库及各主体数据库，应具有对数据库安全的防护能力，能满足数据库的数据独立性、数据安全性、数据完整性、并发控制、故障恢复的要求，并提供数据库审计功能。

（4）数据访问日志记录，对于所有涉及到数据文件、数据库记录的操作均应有日志，对所有的数据库操作应设置有日志审计记录。数据库的更新操作应通过数据库事务日志记录，并传到专用的数据库日志服务器，防止数据库文件被破坏导致用户数据丢失

或泄漏。系统应记录用户访问系统、办理业务过程中的系统日志，供系统审计使用。系统应记录业务逻辑的关键路径以及出错信息，方便线上排错。如需记录用户身份信息，应对用户身份信息脱敏后再进行日志记录。

9.5. 系统安全

各业务系统的系统安全应符合GB/T22239-2019中相关要求，并应符合以下要求：

（1）服务器、主机及数据库系统的账户管理应具备身份鉴别、访问控制、安全审计能力。

（2）服务器、主机及数据库系统应具有入侵防范和恶意代码防范能力。

（3）操作系统和数据库系统所在的存储空间，在被释放或再分配前，应完全清除。

（4）操作系统优选国产化操作系统，并实施内核等安全加固措施。

（5）数据库系统应具备数据备份和恢复能力。

（6）部署的数据库系统等宜优选国产化产品。

9.6. 应用安全

各业务系统的应用安全应符合GB/T22239-2019中的相关要求，并应符合以下要求：

（1）应用系统应建立统一的账号、认证、授权和审计系统，实施身份管理、安全认证与访问权限控制，提供用户访问记录，访问可溯。

（2）应用系统应采取安全最小化原则，关闭未使用的服务组件和端口。

（3）应用系统应加强内存管理，防止驻留在内存中的剩余信息被他人非授权获取。

（4）应用系统应具有通信完整性及通信保密性。

（5）应用系统应具有抗抵赖、软件容错、资源控制的能力。

（6）全球广域网(WEB)安全防护能防护各类常见的web应用攻击。

9.7. 安全管理

9.7.1. 网络安全等级保护制度执行

接入方应根据《中华人民共和国网络安全法》等法律法规要求，严格执行网络安全等级保护制度，保障广西壮族自治区住房和城乡建设信息化建设项目的业务系统免受干扰、破坏；应加强内、外部人员管理，开展安全意识培训，防止数据泄露或者被窃取、篡改。

9.7.2. 平台建设管理

9.7.2.1. 平台安全测评

广西壮族自治区住房和城乡建设信息化建设项目的业务系统在上线前，接入方应开展第三方安全测评。

9.7.2.2. 应用接入

各业务系统接入广西壮族自治区住房和城乡建设信息化建设项目时，其接口应满足以下条件，包括但不限于：

（1）业务系统对接广西壮族自治区住房和城乡建设厅数字住建信息化基础支撑平台的接口目录。

（2）业务系统应严格按照网关开发文档开发，区分用户业务接口和后端业务接口，不应将后端业务接口发布到用户业务接口上。

（3）各个接口不应存在 SQL 注入漏洞，宜使用参数化查询。

（4）各个接口应对用户鉴权，禁止用户创建、更新、读取、删除其他用户的信息。

（5）文件上传模块应禁止任意文件上传，应通过白名单限制上传格式。

（6）敏感接口（如：短信接口、邮件接口）应做频率限制：60 秒一次，验证码长度应为 6 位，有效期 5 分钟。

（7）需验证码校验的事项，校验成功后应返回 token 值，并传递到下个页面接口再次校验 token 有效性。

（8）个人办理事项，不应从用户端获取用户身份，应从智能网关的请求的 header 头获取。

（9）业务系统返回个人信息类的数据时应对用户敏感信息进行掩码处理，不应返回明文。

（10）接入的事项应对业务系统合理配置错误页面（403、404、405、500、503、504 等），禁止泄露中间件错误页面。

（11）若无特殊需要，应使用 GET、POST 两种 HTTP/HTTPS 方法。