国家“互联网+监管”系统
监管门户
应用接入规范

2019 年 08 月

修订历史记录

日期	版本	说明	编制人	审核人
<2018-9-10>	<1.0>	方案整理与编写工作	陈星	咸海成
<2019-05-15>	<2.0>	方案整理与编写工作	刘国钦	咸海成
<2019-08-15>	<2.1>	优化申请表和审核表	朱冬健	咸海成

目录

1 名称解释

PC 端：通过网页浏览器进行展示的终端。

移动端：通过手机等移动设备进行展示的终端，包括 APP 端，微信小程序和支付宝小程序。

2 接入概述

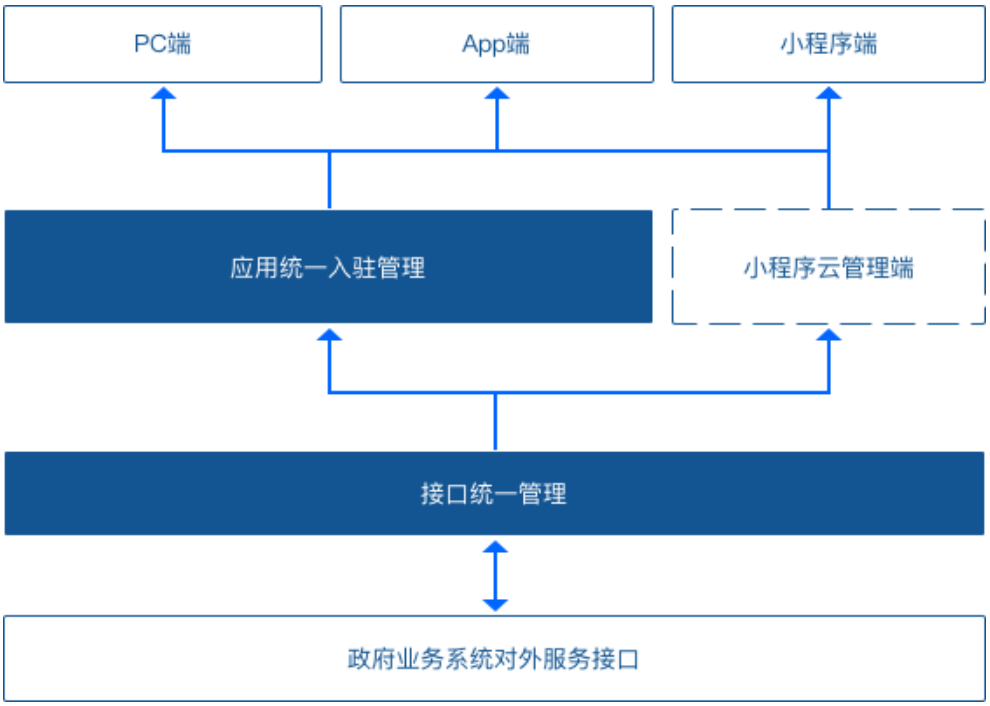
本标准规定了国家“互联网+监管”系统监管门户应用(包含 PC 端和移动端应用)的接入流程、对接模式、接入安全、数据规范和 UI 规范等。

国家“互联网+监管”系统监管门户应用接入的总原则是多端展现、接口统一。以便于统一数据、统一界面、统一使用。

本标准适用于国家“互联网+监管”系统监管门户应用的建设。

2.1 统一接入架构图

国家“互联网+监管”系统监管门户应用接入总体架构图如下图：



2.2 接入原则及要求

国家“互联网+监管”系统监管门户应用(包含 PC 端应用和移动端应用)接入，应遵循以下原则和要求：

1) 统一标准流程

接入国家“互联网+监管”系统监管门户的应用应统一接入流程和步骤，监管应用的页面和交互功能，确保数据接口规范、界面交互体验与国家“互联网+监管”系统要求一致、用户认证统一。

2) 统一接口规范

接入国家“互联网+监管”系统监管门户的服务应用应按照统一接口规范进行接口提交与审核，使用国家“互联网+监管”系统监管门户的域名统一输出标准接口地址进行应用开发。

3) 统一部署运维

接入国家“互联网+监管”系统的应用，需统一部署在国家“互联网+监管”系统监管门户应用开放平台，实现集中监测、统一运

维，并由国家“互联网+监管”系统统一网络配置并提供在线服务。

4）统一用户对接

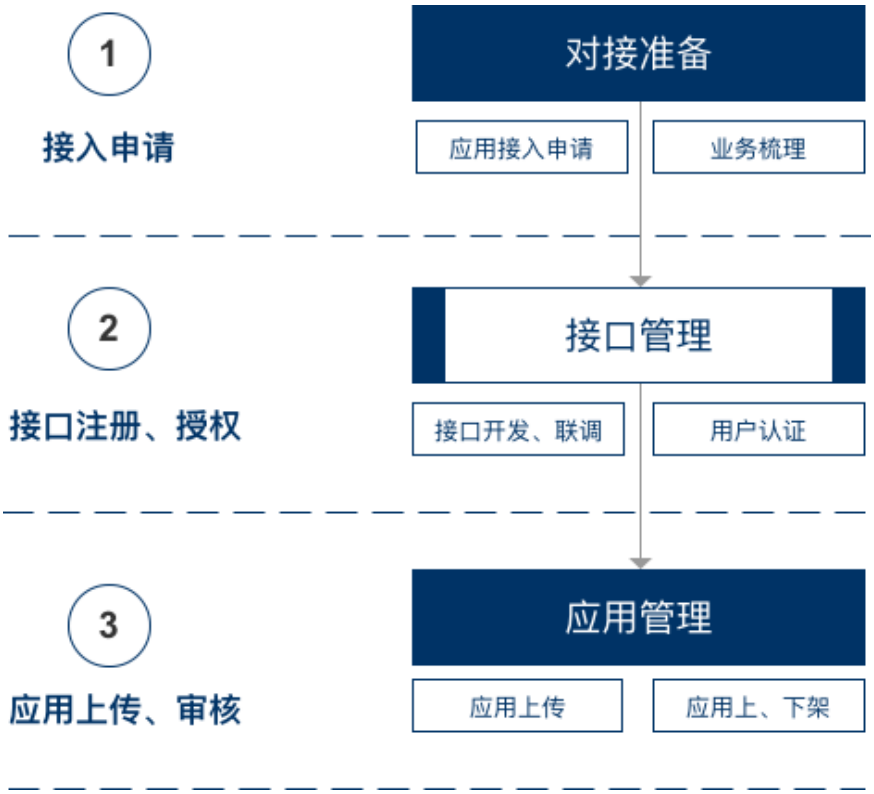
应用对接分为需身份认证应用与无需身份认证应用，无需身份认证应用不涉及用户信息的对接开发，可忽略。

需身份认证应用接入国家“互联网+监管”系统时，需统一接入国家“互联网+监管”系统的统一用户中心，实现全国用户统一。

3 接入流程

3.1 流程总览

应用接入到国家“互联网+监管”系统分为三个步骤：1、接入申请，2、接口注册，3、应用上传三个步骤，如下图所示。



3.2 接入申请

3.2.1 步骤说明

接入单位在对接应用前，需要向国家“互联网+监管”系统提交接入申请单，由国家“互联网+监管”系统统一回复结果。

3.2.2 申请准备

接入单位需自行梳理业务服务场景，根据梳理情况填写《监管应用接入申请表-单位名称-日期》（见附件 1），填表后需加盖接入单位公章。

3.2.3 提交方式

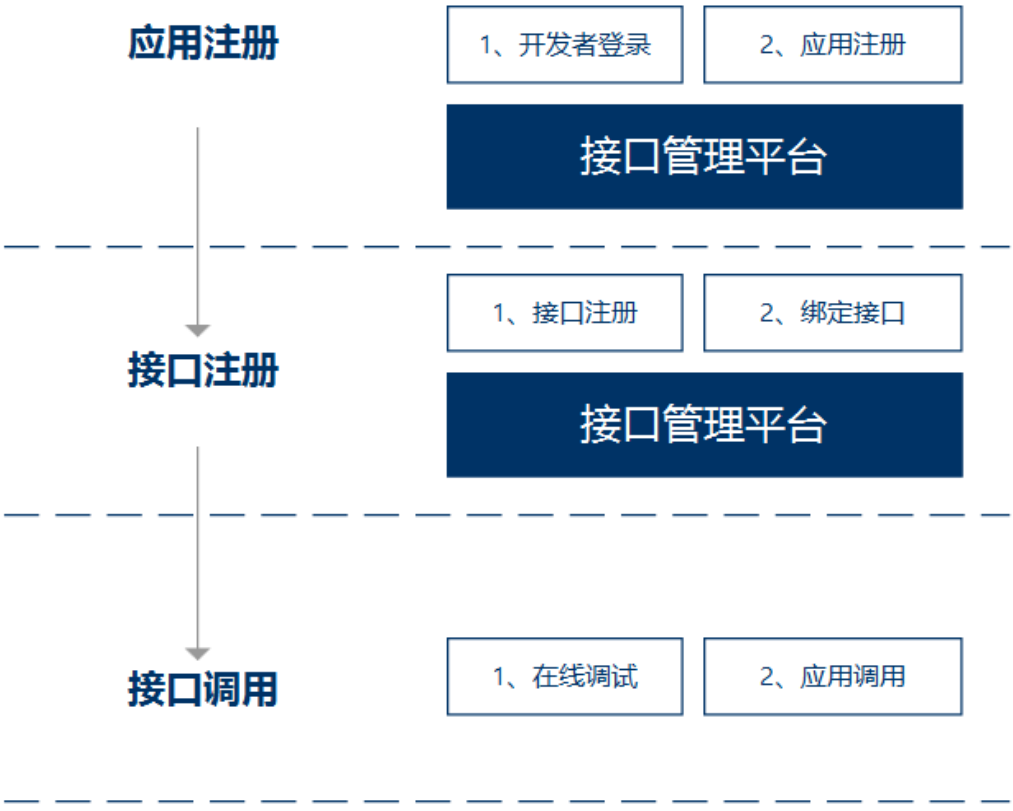
接入单位以发送邮件形式将应用接入申请表发送至国家“互联网+监管”系统邮箱 a16@cegn.gov.cn，国家“互联网+监管”系统管理员在接收到接入申请表单后，将在 24 小时内完成审核工作，并以邮件形式回复审核结果。

3.2.4 账号分配

国家“互联网+监管”系统管理员在审核同时，需给接入单位分配接口管理平台账号和应用入驻平台账号，并将平台地址、账号密码、接入指南以及相关帮助文档一并在邮件中回复给接入单位。

3.3 接口统一管理

3.3.1 流程图



3.3.2 应用注册

接入单位使用分配的账号登录国家“互联网+监管”系统接口管理平台注册应用。注册应用时需创建应用唯一标识，详见 3.5.6 章节。

3.3.3 接口注册

接入单位需要将开发应用所需接口注册至国家“互联网+监管”系统接口管理平台中，注册参数如下图，包括接口地址、请求方式，以及相关请求参数与返回结果示例

接口地址。	https://*********/query。
返回格式。	JSON。
请求方式。	get 或 post。
接口协议。	https。
接口备注。	***接口。

请求参数。

名称。	必填。	类型。	说明。
region。	是。	string。	行政区划代码，见 C 0109.1-2018 的 4.3。
pf。	是。	string。	可兼容的访问渠道。 如：gov - 中国政务服务。 all - 全端支持。
auth_code。	是 。	string。	业务代码，作为请求唯一标识。
name。	是。	string。	用户姓名。
code。	是。	string。	***编码。

返回参数。

名称。	必填。	类型。	说明。
result_code。	是。	string。	结果状态码。 如：100 - 处理成功。 102 - 处理失败。 103 - 处理中。
error_code。	是。	string。	结果状态码为 102 时，接入单位接口返回自定义的错误码。
error_msg。	是。	string。	结果状态码为 102 时，接入单位接口返回自定义的错误消息。
date。	是。	string。	当前操作日期 YYYY-MM-DD。

JSON 返回。

```
{。
   "process_response": {。
   "result_code": "100",。
   "date": "2018-04-25",。
   "items": [。
                {。
                    "id": "15485",。
                    "name": "**丹",。
                    "ctime": "2018-04-25 12:04:23",。
                    "desc": "**********"。
                }。
            ]。
  }。
```

注意：

1、地方和部门要对接口自行进行封装，注册到接口管理系统的地址

请求方式支持 get、post 和 webservice 方式，参数支持 string 和

integer 类型。

2、接口需要通过高并发的处理，要求并发数达到 1000+，响应时长不超过 2s。

3、接口需要通过安全性的处理，涉及敏感信息应进行加密或脱敏处理。脱敏规则详见 3.5.4 章节。

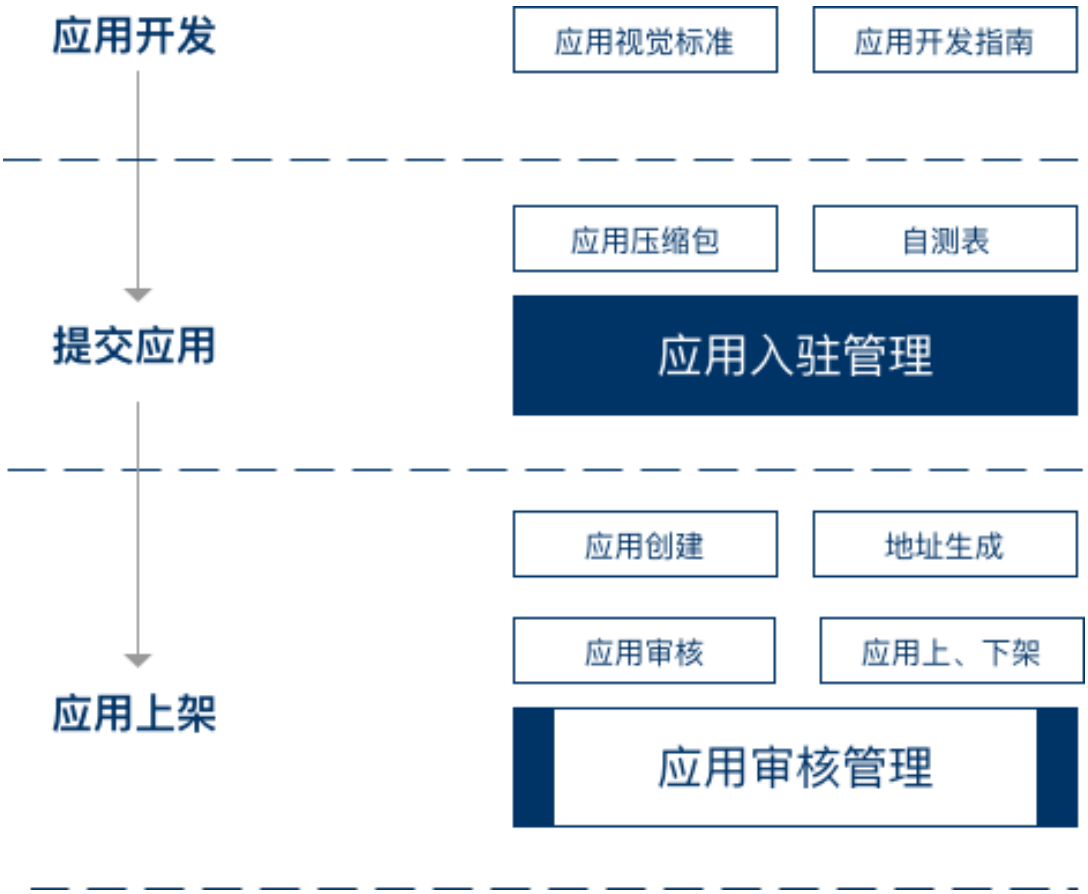
4、应用开发需使用接口平台返回的接口地址和 key 码，在应用审核的时候，会进行匹配审核。

3.3.4 接口调用

成功注册的接口，会经过国家“互联网+监管”系统接口管理平台进行域名转换，生成统一的国家平台域名的接口地址：https://国家“互联网+监管”系统接口管理平台主域名/link.do。开发者可自行测试、用于开发对接。

3.4 应用统一部署

3.4.1 流程图



3.4.2 应用自测

应用开发工作完成后进行应用功能测试。PC 端应用应使用带有调试模式的浏览器(谷歌浏览器)进行应用功能测试、移动端应用应使用“调试助手”进行应用功能测试。

3.4.3 应用提交

应用代码需封装成压缩包（.zip），压缩包命名规则按照 3.5.6 章节执行。使用分配的国家“互联网+监管”系统应用入驻平台账号登录平台，将应用压缩包和审核规范表（两者缺一不可）按流程提交至后台即可。

3.4.4 应用审核

应用审核员使用调试工具进行应用测试，严格把关质量，对不符合要求的应用进行沟通处理，审核通过后方可上架提供服务。

3.4.5 应用上下架

应用上下线管理包含监管应用兼容性、可用性、安全性及压力测试，审核通过后上线到相应接入单位的监管应用站点，并对上线的监管应用进行统一监控，对监管应用不稳定、安全风险大、并发性能差的应用予以通知整改，情况严重的应用需进行下架处理。

3.5 技术规范

3.5.1 HTTPS 支持

随着当前网络环境用户信息泄密越来越严重，全网 HTTPS 已成为一种强需求，接入单位在开发应用服务时需保证页面加载的所有资源协议支持 HTTPS 访问协议。

3.5.2 用户信息获取

因为用户交互进行更加严格的安全改造，不支持以 HTTPS 方式请求 token 的通道，只保留 webservice 请求通道。各接入单位如需获取用户信息，需通过业务后台与统一用户中心进行交互。标准交互流程图如下：

3.5.3 接口鉴权

各单位提供的应用是用于进行互联网交互的应用，需进行接口访问安全性进行设计，建议使用两种鉴权模式：

安全鉴权：请求签名机制，签名算法采用 SM2，双方以安全方式存储通讯密钥。

白名单鉴权：接口白名单，接口的开放针对国家“互联网+监管”系统加入白名单。

3.5.4 数据脱敏

接入单位应根据实际业务情况，对输出的数据进行脱敏处理后向用户展示，脱敏范围应不少于 50%，常见用户隐私信息脱敏规则如下。

- 中文姓名脱敏 李** 保留第一位，后面以*替换；
- 公民身份号码脱敏 **********5762 保留后 4 位；

- 固定电话脱敏 ****1234 保留后 4 位；
- 手机号码脱敏 1******34 保留第一位，后面保留 2 位；
- 地址脱敏 北京市海淀区**** 保留前 6 位；
- 电子邮箱脱敏 g**@163.com ***@后面的部分；
- 银行卡号脱敏 622260**********1234 保留前 6 位后 4 位；
- 公司开户银行联号脱敏 12******** 保留前 2 位；
- 时间类的处理，建议脱敏规则为：入参 yyyymmdd(没有下划线，中划线)****1234 保留后 4 位，可根据不同业务需求场景自行判断是否脱敏。

3.5.5 数据缓存

为保障应用的并发能力和承载国家“互联网+监管”系统监管门户的高访问量，要求应用的 server 端接口都加上接口缓存。缓存数据仍然要求通过脱敏（同 3.5.4）处理。

3.5.6 命名规范要求

应用中文名称命名规则：

应用中文名称应简单明了，说明应用用途，建议长度不超过 8 个字，便于理解和记忆。

省级部门应用标识命名规则：

应用标识 = [部门简称汉语拼音首字母]+ [应用名称汉语拼音

首字母]

举例：

[人社部]“职业资格证书查询”,命名为“rsbzyzgzscx”。

地方应用命名规则：

应用名称 = [地区名称汉语拼音首字母]+[应用名称汉语拼音首字母]

举例：

[江苏]“中考查询”,命名为“jszkcx”。

命名重复排除规则：

应用名称 = 应用名称+[提报时间戳]（具体到分钟）

地方如“[江苏]个税计算器”,命名为“jsgsjsq”,如果出现一个应用名称为“[江苏]个税计时器”,命名为“jsgsjsq201809060800”,如果还有出现一个应用如“[江苏]个税计数器”,命名为“jsgsjsq201809061800”。

3.5.7 底部统一标识

移动端服务应用的所有页面底部都需注明“本服务由某某单位提供”该标语，具体样式要求见移动端UI规范。建议将该部分独立成公共模块，在每个页面引入方便后期维护。

3.5.8 兼容性规范

移动端应用对系统支持要求，推荐兼容iOS 9+、Android 4.0+系统，确保开发的应用可适配大部分主流尺寸的屏幕，给予用户良好的体验。

3.5.9 图形验证码使用

接入服务应用涉及到表单提交时，建议加入验证码，尤其不要求用户登录的服务应用必须在提交表单时加入图形验证码。使用验证码的目的是为了阻止攻击者使用自动工具和程序连续恶意提交表单尝试登录、查询等行为，从而降低被暴力查询获取大批量接入单位业务数据的可能。若验证码影响用户体验，接入单位可以自行决定多少次提交表单后再显示验证码。对于图形验证码的技术要求建议如下：

验证码在设计上必须要考虑到一些安全因素，以免能被轻易地破解，常见的方式是增加背景干扰元素；验证码在一次使用后要求立即失效，新的请求需要重新生成验证码，防止验证码多次有效。

3.5.10 表单输入校验

接入单位开发服务应用时必须对用户产生的输入内容进行校验，不能完全依赖于客户端校验，必须使用服务端代码对输入数据进行最终校验。客户端的校验只能作为辅助手段，减少客户端和服务端的信息交互次数。一旦发现数据不合法，应该告知用户输入非法并且建议用户纠正输入。一方面是为了提升用户体验，另一方面是为了防止攻击者通过输入进行 SQL 注入、XSS 攻击等恶意行为。

3.6 其他

3.6.1 外部资源调用

禁止应用前端直接调用外部服务资源，包括但不限于应用提供单位开放的外网应用系统数据接口，降低应用提供单位原始接口暴

露的风险，同时要求保障接口调用和数据传输的安全。除特殊情况下，不建议应用服务直接调用外部服务。

对于应用服务页面内容引用的静态资源（JS 文件、CSS 文件、图片等），建议这部分资源尽量随应用服务部署在互联网区，不使用外链资源，防止因外链资源失效导致影响应用服务使用的情况发生。个别必须使用外链的第三方服务资源，可按实际情况引用。

4 附件

通过申请回复的相关文档包括：

附件 1：《国家“互联网+监管”系统应用接入申请表-单位名称-日期》

附件 2：《国家“互联网+监管”系统应用开发用户对接指南》

附件 3：《国家“互联网+监管”系统应用 JS-API 接入指南》

附件 4：《国家“互联网+监管”系统应用接入审核规范》

附件 5：《国家“互联网+监管”系统应用审核规范》

附件 6：《国家“互联网+监管”系统 PC 端应用界面视觉要求》

附件 7：《国家“互联网+监管”系统移动端应用界面视觉要求》