ICS 35.240.99
CCS L67

DB44

广　东　省　地　方　标　准

DB44/T XXXX—2023

政务人员统一身份认证子平台接入规范

Access interface specification of Unified Identification Authentication System for the Administrative staff

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由广东省政务服务数据管理局提出及归口。

本文件起草单位：数字广东网络建设有限公司、广东省标准化研究院。

本文件主要起草人：

本文件为首次发布。

政务人员统一身份认证子平台接入规范

1 范围

本文件规定了各级政务部门业务系统接入广东省政务人员统一身份认证子平台（以下简称“省政务认证平台”）时，对接过程的总体要求、接入流程、技术对接要求、管理要求等内容。

本文件适用于广东“数字政府”框架下的各级政务部门的政务业务系统与省政务认证平台对接的过程。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

身份 identity

代指政府工作人员在政务服务中的身份标识，是政务服务授权的依据。

3.2

政务部门 administrative organization

指依一定的宪法和法律程序建立的、行使国家行政权力、管理社会公共事务的政府组织机构实体。

3.3

业务系统 the business system

指政务部门的政务应用系统。

3.4

接入方 accessor

指需要向省政务认证平台申请业务系统对接的政务部门

3.5

运营方 operator

负责省政务认证平台日常运营的机构。

3.6

管理方 administrator

省政务认证平台的主管方，即政务服务数据管理部门。

3.7

粤基座平台 yuejizuo platform

广东省数字政府建设公共资源管理平台。

3.8

系统承建单位 system construction unit

负责承建政务部门业务系统的单位。

4 符号和缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application programming interface）

ID：标识号码（Identity Document）

OAuth2.0：开放授权标准2.0（The Open standard for Authorization 2.0）

5 总体接入架构

5.1 综述

省政务认证平台构建全省政务人员账号信息库，提供政务人员账号管理、登录、登出等身份认证标准服务，支持账号密码登录、扫码登录、数字证书登录等登录方式。业务系统通过OAuth2.0协议对接省政务认证平台，可依托平台服务实现账号登录和登出。总体接入架构如图1所示。

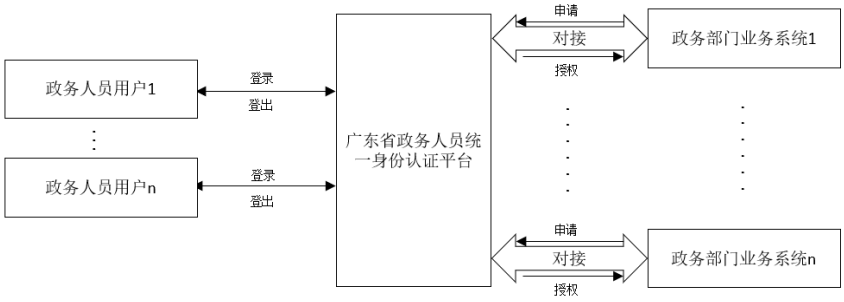

图1 总体接入架构

5.2 统一登录

用户在登录业务系统时使用省政务认证平台登录，跳转到省政务认证平台登录首页，通过省政务认证平台登录认证后登入业务系统，业务系统可为该用户创建本地登录会话。业务系统可建立本地用户中心，可保存省政务认证平台认证后的登录用户信息，并对用户在本系统的使用进行权限管控。

5.3 统一登出

用户在业务系统请求统一登出时，由业务系统注销该用户的本地登录会话，并按省政务认证平台登出要求调用省政务认证平台登出功能。

6 接入流程

6.1 综述

接入工作流程主要包括系统改造、接入准备、接入申请、申请审批、分配授权的接入参数、系统对接、上线确认、完成接入等过程。

6.2 系统改造

接入申请前或者分配授权的接入参数后（见6.6），接入方应遵从省政务认证平台相关操作指引及国家有关信息安全的要求完成业务系统改造。

6.3 接入准备

接入方应提前了解省政务认证平台相关接入要求，明确申请流程和申请材料，约定接入各方的工作职责后方提出接入申请。

6.4 接入申请

接入方通过粤基座平台提出接入申请，按要求填写申请信息和上传附件（申请表内容如附录A所示），接入方应确保所填信息准确无误。

6.5 申请审批

平台管理方对接入申请进行审核，确认信息无误后予以批准并通知运营方配合接入方实施接入。

6.6 分配授权的接入参数

审批完成后，运营方应授权业务系统接入，分配测试/正式参数，返回client_id、client_secret等配置信息，业务系统使用这些信息对接省政务认证平台相关服务。

6.7 系统对接

接入方获取参数接入授权后，可在运营方处获取对接指引并由接入方指定技术人员进行对接联调，运营方提供技术支持。

6.8 上线确认

完成生产环境对接联调之后，接入方应提交上线报告（格式见附录B）给运营方确认，确认内容主要包括生产环境功能是否正常、对接工作是否已完成。

6.9 完成接入

运营方审核上线报告，确认接入工作已完成后，进行归档备案。

7 技术对接

7.1 业务系统对接内容

7.1.1 综述

省政务认证平台采用OAuth2.0协议对接，一共分四步，分别通过调平台四个接口来实现：

a) 请求认证授权码：在前端通过省统一认证登录请求认证授权码 code；
b) 获取访问令牌：将前端请求到的 code 传到后端获取访问令牌 token；
c) 获取登录账号信息：在后端使用获取的 token 获取当前登录账号信息；
d) 账号登出：前端调退出接口清除浏览器登录 cookie(退出接口调用成功即清除省统一认证登录态)。

7.1.2 登录流程

业务系统完成接入后，使用省政务认证平台登录流程如图2所示。

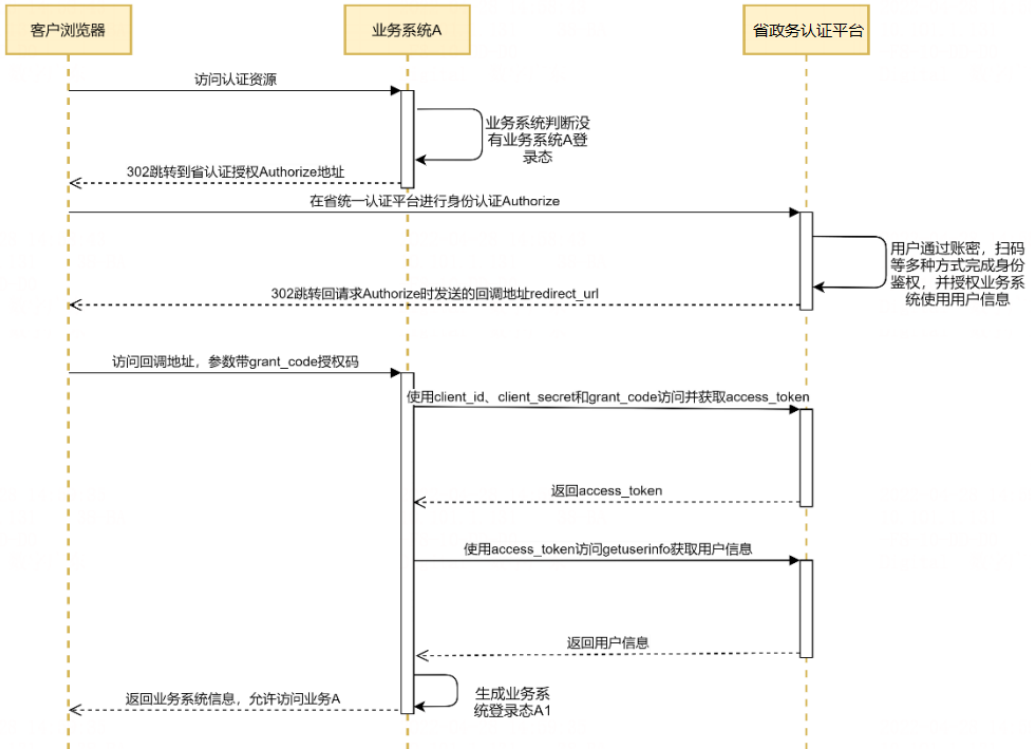

图2　使用省政务认证平台服务登录业务系统的流程图

登录流程具体如下：

a) 用户访问业务系统需要认证的资源时，业务系统 A 将请求跳转到省政务认证平台的 Authorize 页面，同时带上回调地址 redirect_url；

b) 用户在省统一认证平台选择各种核验方式进行身份核验，登录成功后，省政务认证平台发起请求访问回调地址，并带上 code 参数；

c) 业务系统应用服务接收到省认证回调的请求后，应在服务端使用该 code 和 client_id、client_secret 访问省认证平台的获取访问令牌接口，获取 access_token 信息；

d) 省政务认证平台返回 access_token 相关信息（包括过期时间等字段信息）给业务系统应用服务；

e) 业务系统应用服务再次发起请求到省政务认证平台的 getuserinfodetail 接口，使用 access_token 参数换取账号信息；

f) 业务系统应用服务将获得账号信息生成业务系统自身的登录态，用于业务资源的访问控制。

g) 业务系统应用服务返回到客户浏览器，完成用户账号在业务系统 A 的登录过程。

7.1.3　登出流程

用户在业务系统使用省政务认证平台账号登录后，在业务系统点击退出，业务系统需要调用省政务认证平台的账号登出接口。下次登录时，需要重新走登录流程。

7.2　接口及参数说明

7.2.1　总体要求

具体如下：

a) 业务系统需通过粤基座认证中心域名进行接口调用；
b) 业务系统调用接口时回调地址(redirect_uri)需要进行编码；
c) 账号登录省政务认证平台后，访问其它接入省政务认证平台的业务系统时，会直接返回授权码code给业务系统，业务系统通过code获取账号信息后，实现登录。

7.2.2 API调用说明

业务系统需要调用省政务认证平台相关接口时,应先申请获取授权Client_ID和Client_Secret等信息，以及登记Redirect_Uri（见6.6）。相关接口见表1所示。

表1 接口表

接口名称	接口功能
authorize	请求认证授权码（code）
token	获取访问令牌
getuserinfodetail	获取登录账号详细信息
manage/userinfo	账号管理页
logout	账号登出

平台管理方应针对以上接口制定详细的接口参数指引指导接入方实施系统改造及接入。

7.2.3 错误信息说明

错误信息说明表2。

表2 错误信息说明

场景	错误信息	说明
请求认证授权码	Invalid redirect	非法回调地址，/oauth/authorize的redirect_uri入参必须与申请表一致
	Bad client credentials	非法client_id，/oauth/authorize的client_id入参必须以省统一认证平台分配信息为准
获取访问令牌	Invalid authorization code	非法授权码，授权码一次核验则失效
	Bad credentials	参数错误，非法的client_id或非法的Client_secret
	Redirect URI mismatch	非法回调地址，redirect_uri入参必须与申请表一致
	Missing grant type	参数grant_type缺失
	Unsupported grant type	非法grant_type参数
	Invalid refresh token	非法refresh_token参数

8 管理要求

8.1 责任分工

平台管理方应对接入过程责任分工予以明确规定，接入过程各相关方应充分了解接入过程职责分工和要求。

8.2 沟通反馈

平台管理方应建立沟通反馈机制，保障接入过程的信息和问题得到有效沟通和及时处理。

8.3 人员建设

接入过程各相关方应做好专业人员队伍建设，为业务系统正常接入提供组织和人员保障。

8.4 制度建设

平台管理方应针对业务系统接入制定管理制度和技术操作文件，为接入工作提供规范和指引。

8.5 安全管理要求

安全管理要求如下：

a) 接入过程各相关方应根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规要求，严格执行 GB 17859-1999、GB/T 22239-2019 等网络安全等级保护制度，保障省政务认证平台和业务系统免受干扰、破坏，防止数据泄露或者被窃取、篡改等，加强系统安全防护与管理。

b) 接入过程各相关方应遵守国家信息安全条例和保密法规定，不得利用省政务认证平台进行危害国家安全，侵犯国家、社会和集体利益，保障公民合法权益，不得在省政务认证平台上传输、存储和处理涉密信息。

c) 管理方应组织对接入省政务认证平台的业务系统开展安全监督和安全检查，定期发布安全公告，督促运营方和接入方开展安全风险整改加固工作。

d) 接入方应建立健全业务系统相应的运行、维护、管理机制，采取安全防护措施，保障业务系统安全。

e) 接入方应规范接入省政务认证平台的业务系统对用户隐私数据的使用，坚持最小化原则，涉及隐私数据的收集和使用应符合业务需要，明确责权，贯彻知情原则。

f) 接入方应履行个人信息和数据安全保护责任，建立健全接入省政务认证平台的业务系统中的个人信息和数据安全保护制度。

g) 与省政务认证平台对接的业务系统应具备完善的信息安全防护措施，符至少应合计算机信息系统安全等级保护三级要求以上。业务系统须提供等保三级测评报告或具备安全测评资质的第三方测评公司的系统安全测评报告

h) 系统用户应按省政务认证平台要求设置密码并定期更新，不得向第三方组织或个人共享账号和系统数据，因泄露密码或共享账号及数据造成的一切后果由用户本人承担。

i) 不支持涉密系统接入省政务认证平台，不支持 APP 端接入省政务认证平台。

j) 省政务认证平台不提供批量获取用户信息的相关接口，业务系统可根据登录用户的最新信息建立本地用户中心，实现用户的权限管控。对于留存在本地用户中心的个人信息，应按相关规定做好安全防护，避免个人隐私泄露。

附 录 A
（规范性）
接入申请表格式

业务系统接入申请表格式见表A.1。

表A.1 广东省政务人员统一身份认证子平台接入申请表

申请单位信息(申请单位填写)			
业务系统名称	填写业务系统名称		
业务单位名称 （盖章）	业务单位填写盖章处		
单位联系人		申请时间	
单位联系人电话		单位联系人邮箱	
业务系统信息(系统承建单位填写)			
系统概述及业务应用场景描述	业务系统应用省统一身份认证的业务场景		
业务系统首页地址	测试环境：		
	生产环境：		
业务系统回调地址	测试环境：		
	生产环境：		
系统开发商			
开发商联系人		联系电话	
备注			

填表说明：

1） 填写的申请单位名称（全称）应与单位公章所使用的名称完全一致，不得使用简称、缩写等。
2） 业务系统回调地址：填写业务系统完成认证后重定向的地址。
3） 单位及开发商联系人、联系人电话、邮箱须填写正确，用于后续对接沟通。

附 录 B
（规范性）
上线报告格式

业务系统上线报告格式见表B.1。

表B.1 接入广东省政务人员统一身份认证子平台上线报告

<table>
<tr><td colspan="2">接入系统</td><td colspan="3">广东省政务人员统一身份认证子平台</td></tr>
<tr><td colspan="2">接入单位</td><td colspan="3"></td></tr>
<tr><td colspan="2">业务系统</td><td colspan="3"></td></tr>
<tr><td>序号</td><td>功能</td><td>验证内容</td><td>验证结果</td><td>备注</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">登录功能</td><td>使用省政务认证平台账号登录，业务系统能正常接收到省认证平台返回的用户信息。</td><td>正常</td><td></td></tr>
<tr><td>业务系统使用 https 访问省政务认证平台，前端页面禁止传输或显示 client_secret/paastoken 等密钥信息。</td><td>正常</td><td></td></tr>
<tr><td>2</td><td>账号绑定</td><td>使用省政务认证平台账号登录业务系统，可以主动绑定业务系统账号，实现用户信息统一。</td><td>正常</td><td></td></tr>
<tr><td>3</td><td>退出功能</td><td>业务系统有退出功能，当用户退出业务系统之后，需要同步退出省政务认证平台账号。</td><td>正常</td><td></td></tr>
<tr><td colspan="2">结论</td><td colspan="3">各项功能正常，系统已完成对接及上线。

业务单位（盖章）
年 月 日</td></tr>
</table>

参 考 文 献

[1] C 0110-2018 国家政务服务平台统一身份认证系统接入要求
[2] C 0111-2018 国家政务服务平台统一身份认证系统身份认证技术要求
[3] C 0112-2018 国家政务服务平台统一身份认证系统信任传递要求
[4] C 0113-2018 国家政务服务平台统一信任服务平台接口要求
[5] C 0114-2018 国家政务服务平台可信身份等级定级要求
[6] GDZW 0011-2019 广东省统一身份认证平台接入规范（公众侧）
[7] GDZW 0010-2019 广东省统一身份认证平台接入规范（政务侧）
[8] 中华人民共和国主席令（2010年第二十八号）中华人民共和国保守国家秘密法
[9] 中华人民共和国主席令（2017年第五十三号）中华人民共和国网络安全法
[10] 中华人民共和国主席令（2021 年第八十四号）中华人民共和国数据安全法
[11] 中华人民共和国主席令（2021年第九十一号）中华人民共和国个人信息保护法
[12] 国务院令第716号 国务院关于在线政务服务的若干规定
[13] 国办发〔2020〕35号 国务院办公厅关于加快推进政务服务“跨省通办”的指导意见
[14] 国办发〔2018〕45号 国务院办公厅关于进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案的通知
[15] 国办发〔2017〕39号 国务院办公厅关于印发政务信息系统整合共享实施方案的通知
[16] 粤府〔2021〕44号 广东省人民政府关于印发广东省数字政府改革建设“十四五”规划的通知
[17] 粤办函〔2021〕44号 广东省人民政府办公厅关于印发广东省数字政府改革建设2021年工作要点的通知
[18] 粤办函〔2022〕24号 广东省人民政府办公厅关于印发广东省数字政府改革建设2022年工作要点的通知