ICS 35.240.99
CCS L67

DB 44

广　东　省　地　方　标　准

DB 44/T XXXX—XXXX

公众统一身份认证子平台接入规范

Access interface specification of Unified Identification Authentication System for the public

（送审稿）

（本草案完成时间：2021 年　月　日）

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并归口。

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：

公众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从Web端接入广东省公众统一身份认证平台（以下简称“省公众认证平台”）时，对接过程的总体接入架构、接入流程、技术对接、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业务系统通过Web端与省公众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

可信身份认证 trusted identity authentication

在网络空间中，网络实体通过其持有的认证凭据经过认证鉴别后与其现实社会的真实身份建立绑定关系的过程。

3.2

自然人 natural person

基于出生而取得民事主体资格的人，其外延包括本国公民（大陆居民、港澳台居民）、外国公民和无国籍人等。

3.3

法人 legeal person

具有民事权利能力和民事行为能力，依法独立享有民事权利和承担民事义务的组织。

3.4

身份信息 identity information

自然人或法人身份的属性信息，自然人身份信息包括姓名、公民身份号码、手机号等，法人身份信息包括法人名称、法定代表人、统一社会信用代码等。

3.5

登录认证 login authentication

自然人或法人账号登录时，对其进行身份鉴别的过程。登录认证方式包括但不限于如账号口令、生物特征、数字证书登录认证等。

3.6

单点登录 single sign on

当用户访问多个应用系统时，只需提交一次认证信息就可访问多个应用系统。

3.7

政务部门 administrative organization

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。

3.8

业务系统 the business system

政务部门的政务应用系统。

3.9

接入方 accessor

需要向省公众认证平台申请业务系统对接的政务部门。

3.10

运营方 operator

负责省公众认证平台日常运营的机构。

3.11

管理方 administrator

省公众认证平台的主管方，即政务服务数据管理部门。

3.12

粤基座平台 yuejizuo platform

广东省数字政府建设公共资源管理平台。

3.13

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 缩略语

下列缩略语适用于本文件。

APP 应用程序（Application）

JSON JavaScript 对象标记语言（JavaScript Object Notation）

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

API 应用程序接口（Application Programming Interface）

5 总体接入架构

5.1 综述

省公众认证平台构建全省自然人和法人账号库，具备统一的用户注册、登录认证、身份核验等基础能力，支持公安部可信身份认证和国家市场监督管理总局电子营业执照核验，支持多家CA数字证书和网银证书核验，支持港澳居民出入境证件身份认证核验和港澳台居民居住证身份信息核验。业务系统通过OAuth2.0协议对接省公众认证平台，可依托平台能力实现用户在业务系统的统一登录、统一登出、二次核验等功能。总体接入架构如图1所示。

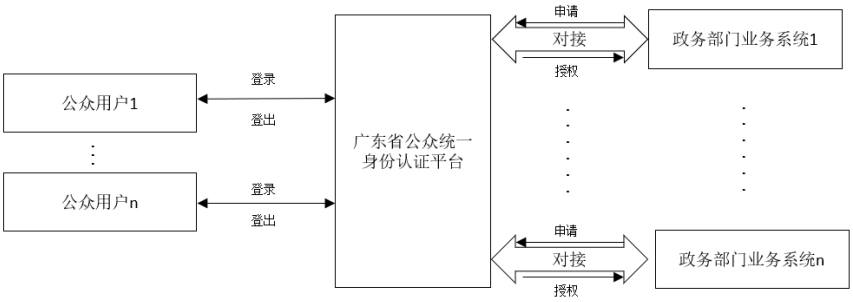

图1　总体接入架构

5.2　统一登录

用户在业务系统登录时，使用省公众认证平台支持的登录方式进行统一登录，通过省公众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。

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，并调用省公众认证平台登出能力，完成用户登出。

5.4　二次校验

业务系统可结合自身业务需要，根据用户当前登录认证方式、实名等级、业务场景，在进行重要业务操作时可发起二次校验请求，对当前登录用户身份进行即时性检验，返回结果为成功或失败。二次校验只对当前请求一次性有效，不修改用户当前实名等级，不更改登录信息中的用户实名等级。业务场景需确认本人操作，则二次校验可使用以下认证方式中的一种或组合：

a)　自然人刷脸认证；
b)　法人电子营业执照认证；
c)　数字证书认证。

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），接入方应遵从省公众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公众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公众认证平台相关服务。

6.7 系统对接

接入方获取参数接入授权后，可在运营方处获取相关操作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 用户登录流程

用户直接访问政务部门业务系统，使用省公众认证平台账号登录流程如图2所示。

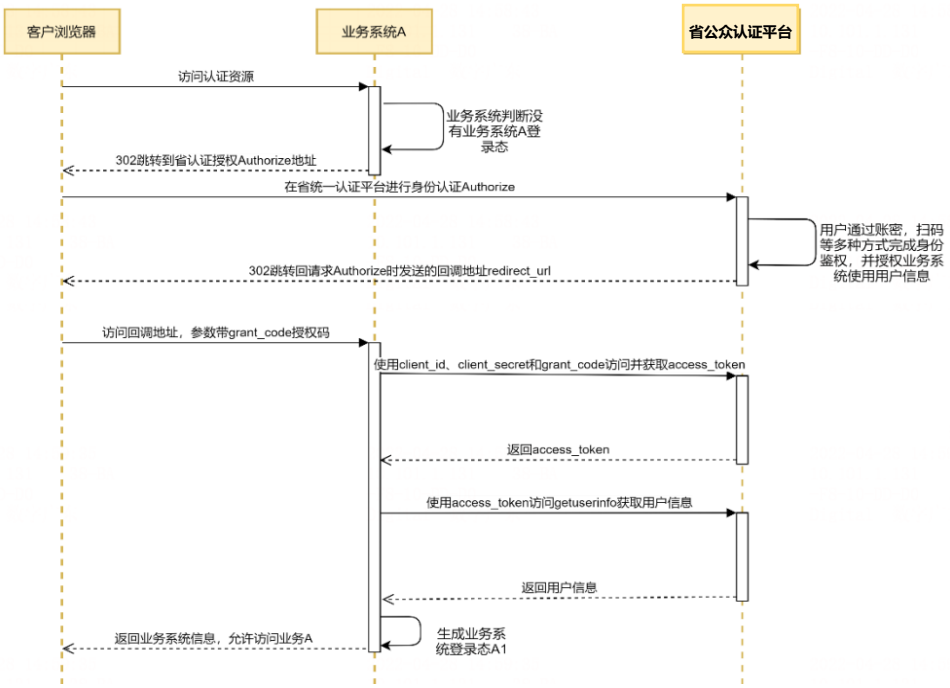

图2　使用省公众认证平台服务登录业务系统流程

登录流程说明如下：

a) 用户访问业务系统需要认证的资源时,业务系统将请求跳转到省公众认证平台的 Authorize 页面，同时带上回调地址 redirect_uri；
b) 用户在省公众认证平台登录成功后，带上 grant_code 参数，重定向到业务系统回调地址；
c) 业务系统应用服务接收到请求后，使用该 grant_code 参数，后端调用省公众认证平台的 access_token 接口；
d) 省公众认证平台在响应体 JSON 返回 access_token 值到业务系统应用服务；
e) 业务系统应用服务使用上一步获取的 access_token 发起请求到省公众认证平台的 tokeninfo 接口，换取用户信息；
f) 业务系统应用服务对用户信息进行处理，提示用户登录成功。

7.1.2　使用省公众认证平台账号登录业务系统

业务系统应在用户点击现有的系统入口或事项的“在线申办”链接时，跳转到省公众认证平台登录认证页面（Authorize页面），用户进行登录。省公众认证平台验证用户登录通过后，返回用户基本信息给业务系统。

7.1.3　广东政务服务网单点登录到业务系统

用户登录广东政务服务网后，点击市、县、省直部门窗口或事项列表中的“在线申报”等链接时，可直接进入相应业务系统。

7.1.4　业务系统单点登录到广东政务服务网或其他业务系统

公众用户使用省公众认证平台账号登录业务系统后，点击该业务系统上关联的其他已接入省公众认证平台的业务系统链接时，可直接进入相应业务系统。

7.1.5　用户信息修改

用户使用省公众认证平台账号在业务系统登录后，如需修改用户基本信息，则由业务系统按照省公众认证平台的相关操作指引，返回省公众认证平台完成用户信息的修改操作。

7.1.6　账户关联关系

帐户、帐户登录名、法人、自然人、父子帐号的关系如图3所示，建议系统间关联字段：uid。

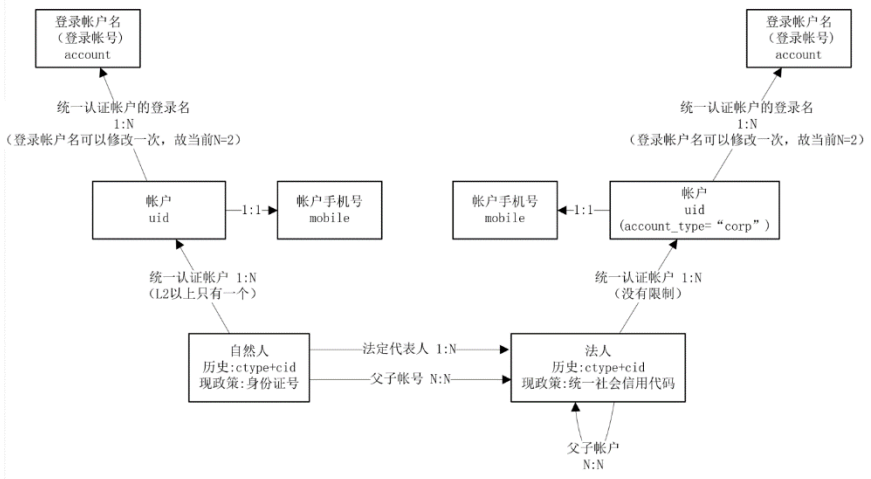

图3　账户关联关系

7.2　接口参数

对接接口包括请求认证授权码服务接口、获取访问令牌服务接口、获取登录账号信息服务接口以及账号登出服务接口。平台管理方应制定详细的接口参数指引，指导接入方实施系统改造和接入。

7.3　接入方要求

7.3.1　入口要求

业务系统应留有省公众认证平台登录方式，用户可通过省公众认证平台账号进行登录。如系统存在多种登录方式，省公众认证平台登录入口按钮宜统一命名为“广东省统一身份认证平台登录”。

7.3.2　账户实名等级判断要求

公众用户通过省公众认证平台登录成功后，业务系统应对返回的用户账户的账户等级进行判断，敏感信息查看及业务实名办理要求用户账户等级应达到表1规定四级及以上。

表1　自然人实名等级

等级	实名核验方式
一级	邮箱，账号口令
二级	手机号，短信码
三级	1、身份证实名核验（公民身份号码、姓名、有效期限 ） 2、社保核验（公民身份号码、姓名、社保卡发卡地行政区划代码、社会保障号码） 以上两种方式中任意一种均可
四级	在三级基础上进行实人核验，使用人脸或其它生物特征进行核验
五级	在四级基础上，使用身份证专用识别设备或具有射频功能的手机配合专用 APP 进行实证核验

7.3.3　用户基本信息管理要求

用户通过省公众认证平台登录业务系统后，如需修改用户基本信息或者提升账户等级，需跳转至省公众认证平台的账户管理页面进行办理。修改后，需退出业务系统，重新登录，以便获取更新后账户信息。

7.3.4　自然人用户隐私保护要求

接入省公众认证平台的业务系统、发布于广东政务服务网的政务服务事项应对自然人二级以上隐私数据（见表2）进行脱敏，查看需进行二次认证。

表2　隐私数据定级表

隐私数据等级	定义
一级数据	不能对应到自然人实体身份信息的数据。
二级数据	可用于标识自然人实体的身份信息，且较公开的数据。如登录账号、姓名、手机号等，统一身份认证隐私数据定级见附录C。
三级数据	可用于标识自然人实体的身份信息，且具有较高隐私性的数据。如证件编号、户籍地址、工作单位等，统一身份认证隐私数据定级见附录C。

7.3.5 用户信息安全要求

接入方在申请对接时应审核业务系统的服务情况，以及业务系统的等保三级测评报告或由具备安全测评资质的第三方测评公司出具的系统安全测评报告。接入方应承担业务系统获取用户账户信息后的信息安全责任。

7.3.6 安全访问及传输要求

接入省公众认证平台的所有业务系统访问、调用省公众认证平台应采用HTTPS协议。

7.3.7 系统退出时同步退出要求

业务系统在退出时，应调用省公众认证平台退出接口。

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，接入过程各相关应充分了解接入过程职责分工和要求。平台运营方提供必要的对接技术指导，保障应用接入工作符合相关标准规范要求

8.2 沟通反馈

平台管理方应建立沟通反馈机制并加强接入情况监督管理。推动运营方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》、《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 等信息安全等级保护制度，保障省公众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，不得利用省公众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，不得在省公众认证平台上传输、存储和处理涉密信息。
c) 管理方应组织对接入省公众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公众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，建立健全接入省公众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) 与省公众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，应至少符合信息安全等级保护三级要求及以上。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。业务系统在申请对接时暂未能提供三级等保报告或者第三方安全测评报告的，须承诺在申请对接之日起，180 天内提供级等保报告或者第三方安全测评报告。

h) 系统用户应按省公众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。

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 广东省公众统一身份认证平台接入申请表（WEB 端）

<table>
<tr><td colspan="6">申请单位信息(申请单位填写)</td></tr>
<tr><td colspan="2">业务系统名称</td><td colspan="4">填写业务系统名称（移动端填写 APP/小程序名称）</td></tr>
<tr><td colspan="2">业务单位名称
（盖章）</td><td colspan="4">业务单位填写盖章处</td></tr>
<tr><td colspan="2">单位联系人</td><td></td><td>申请时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">单位联系人电话</td><td></td><td>单位联系人邮箱</td><td colspan="2"></td></tr>
<tr><td colspan="6">业务系统信息(系统承建单位填写)</td></tr>
<tr><td colspan="2">系统概述及业务
应用场景描述</td><td colspan="4">业务系统应用省统一身份认证的业务场景</td></tr>
<tr><td colspan="2">认证登录次数预估
（万次/年）</td><td colspan="4">____万次/年</td></tr>
<tr><td rowspan="5">□Web 端</td><td>业务系统
终端分类</td><td colspan="4">□PC 端 □公众号</td></tr>
<tr><td rowspan="2">业务系统
首页地址</td><td colspan="4">测试环境：</td></tr>
<tr><td colspan="4">生产环境：</td></tr>
<tr><td rowspan="2">业务系统
回调地址</td><td colspan="4">测试环境：</td></tr>
<tr><td colspan="4">生产环境：</td></tr>
<tr><td colspan="2">系统开发商</td><td colspan="4"></td></tr>
<tr><td colspan="2">开发商联系人</td><td></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td colspan="2">备注</td><td colspan="4"></td></tr>
<tr><td colspan="6">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、邮箱应填写正确，用于后续对接沟通。</td></tr>
</table>

附 录 B
（规范性）
上线报告格式

业务系统Web端接入上线报告格式见表B.1。

表B.1 接入广东省公众统一身份认证平台上线报告（WEB端）

接入系统	广东省公众统一身份认证平台（公众侧）WEB端			
接入单位				
业务系统				
序号	功能	验证内容	验证结果	备注
1	注册登录功能	业务系统首页有广东省公众统一身份认证平台登录入口。	正常	
		使用广东省公众统一身份认证平台账号登录，由广东省公众统一身份认证平台返回用户基本信息到业务系统，业务系统需要显示、自动完善用户的基本信息（如名称、证件号码等）。	正常	
		用户登录广东省公众统一身份认证平台之后，可单点登录直接进入其他已对接广东省公众统一身份认证平台的业务系统办理业务，无需再次登录或出现二次账号登录页面。	正常	
		业务系统使用 https 访问广东省公众统一身份认证平台，前端页面禁止传输或显示client_secret/paastoken等密钥信息。	正常	
2	账号绑定	使用广东省公众统一身份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。	正常	
3	用户信息管理功能	用户使用广东省公众统一身份认证平台登录业务系统后，如需修改用户基本信息或者提升等级，需跳转到广东省公众统一身份认证平台账户管理页面或实名核验页面进行用户信息修改或提升等级操作。	正常	
4	退出功能	业务系统有退出功能，当用户退出业务系统之后，需要同步退出广东省公众统一身份认证平台账号。	正常	
5	业务系统账号应用场景特殊情况说明	无。		
结论		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		

附 录 C
（规范性）
自然人身份信息隐私判定说明

表 C.1 规定了自然人身份信息隐私数据级别定级。

表 C.1 自然人身份信息隐私判定表

信息	隐私级别
自然人姓名	二级数据
自然人登录账号	二级数据
自然人证件类型	一级数据
自然人证件编号	三级数据
证件散列码	一级数据
自然人手机号	二级数据
自然人实名等级	一级数据
证件有效日期	二级数据
证件失效日期	二级数据
自然人实名核验日期	一级数据
社保卡号	三级数据
发卡地	二级数据
用户邮箱	二级数据
注册时间	二级数据
用户生日	二级数据
用户性别	一级数据
用户学历	二级数据
用户支付宝号	二级数据
用户微信号	二级数据
用户户籍地址	三级数据
用户居住地址	三级数据
用户工作单位	二级数据
用户类型	一级数据
用户民族	一级数据
用户国籍	一级数据
用户第二手机号	二级数据
用户第三手机号	二级数据

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] C 0131-2018 国家政务服务平台统一身份认证隐私保护要求
[7] GDZW 0011-2019 广东省统一身份认证平台接入规范（公众侧）
[8] GDZW 0010-2019 广东省统一身份认证平台接入规范（政务侧）
[9] 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
[10] 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
[11] 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
[12] 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
[13] 国务院令第716号 国务院关于在线政务服务的若干规定
[14] 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
[15] 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
[16] 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
[17] 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
[18] 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
[19] 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