ICS 35.240.99
L 67

ZWFW

广 东 数 字 政 府 标 准 规 范

GDZW 0011-2019

广东省统一身份认证平台接入规范
（公众侧）

2019-08-20 发布　　2019-08-20 实施

广东省政务服务数据管理局　发布

目　　次

前　言

本标准按GB/T 1.1-2009给出的规则起草。

本标准由广东省政务服务数据管理局归口。

引　言

广东省统一身份认证平台（公众侧）为全省自然人和法人提供统一的注册、登录、核验等身份认证服务，实现“一个账号、一次登录、全省通用”。同时，已完成对接国家统一身份认证平台，支撑全国统一政务服务。

本规范文件按照全省政务服务工作的总体要求，基于标准统一、安全可靠、互联互通、应用方便的原则制定省统一身份认证平台（公众侧）的对接规范，规范相关对接流程和方法、服务接口、接口数据项，指导业务系统开展认证对接工作。

广东省统一身份认证平台接入规范（公众侧）

1 范围

本标准规定了广东省统一身份认证平台（公众侧）术语和定义、符号和缩略语、实名等级定级、数据字典、业务系统接入规范和用户信息同步规则。

本标准适用于地方和部门政务业务系统对接广东省统一身份认证平台（公众侧）。

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，仅注日期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。

GB/T 31072-2014 科技平台　统一身份认证

C 0131-2018 国家政务服务平台统一身份认证隐私保护要求

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

C 0110-2018 国家政务服务平台统一身份认证系统接入要求

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

C 0113-2018 国家政务服务平台统一信任服务平台接口要求

C 0114-2018 国家政务服务平台可信身份等级定级要求

C 0131-2018 国家政务服务平台统一身份认证隐私保护要求

3 术语和定义

3.1

身份 Identity

代指自然人或法人在政务服务中的身份标识，是政务服务授权的依据。

3.2

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。

3.3

业务系统 Business system

指政务服务应用系统。

3.4

身份认证 Identity authentication

包含实名核验和登录认证。实名核验是对自然人或法人身份进行实名核验时的认证。若无特指，本文中身份认证系指登录认证。

3.5

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。

3.6

信任传递 Trust transfer

实现用户、业务系统的强身份鉴别，跨地方和部门条件下的信任传递。

3.7

凭证 Credentials

系统生成一次性的验证信息，一种通讯安全保障机制。

3.8

统一身份认证 Unified identity Authentication

用户通过使用同一套认证凭证，可访问与该用户身份对应的授权政务应用。

3.9

申请方 ApplySquare

申请对接统一身份认证平台（公众侧）的业务系统的所有者。

3.10

受理方 Acceptance Unit

受理对接申请的机构，指统一身份认证平台（公众侧）的主管机构。

3.11

经办人 Operator

经办人是机构中某事项的处理者，是该事项的直接责任人。

4 符号和缩略语

下列符号和缩略语适用于本文件。

HTTP 超文本传输协议（HyperText Transfer Protocol）

HTTPS 基于安全通道的超文本传输协议(HyperText Transfer Protocol over Secure Socket Layer)

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）

5 实名等级定级

实名等级采用五级实名等级管理，等级逐级提升。自然人实名等级见表1。

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	a）身份证实名核验（公民身份号码、姓名、有效期限 ） b）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

6 数据字典

6.1 自然人用户数据字典

自然人用户关键信息如表2所示。

表 2 自然人用户信息表

编号	字段名称	字段名	字段类型	是否必填	说明
1	账户名	uid	varchar2(100)	是	
2	手机号	telephonenumber	varchar2(50)	是	隐私项
3	电子邮件	mail	varchar2(50)	否	
4	用户姓名	cn	varchar2(100)	是	
5	证件类型	idcardtype	varchar2(10)	是	
6	证件号码	idcardnumber	varchar2(50)	是	隐私项
7	证件地址	address	varchar2(200)	否	
8	用户类型	usertype	varchar2(1)	是	
9	所属地市	area	varchar2(20)	是	
10	法人账户（父账户）唯一标识	parent_uidcode	varchar2(32)	否	
11	用户来源	origin	varchar2(20)	是	
12	账户登录方式	accout_type	varchar2(1)	是	
13	用户唯一标识（UID）	useridcode	varchar2(32)	是	
14	用户信息更新时间	createtime	varchar2(30)	是	
15	用户信息版本	uversion	varchar2(4)	是	
16	性别	sex	varchar2(1)	否	
17	实名状态	is_real	varchar2(10)	是	
18	实名注册类型	real_type	varchar2(4)	否	
19	实名注册位置	authloc	varchar2(100)	否	
20	审核单位	entdep	varchar2(100)	否	
21	审核人名	authnam	varchar2(20)	否	
22	现场审核照片留存标记	authphoflag	varchar2(20)	否	
23	现场审核照片内容	authpho	varchar2(1000)	否	
24	数字证书内容	cert_data	varchar2(2000)	否	
25	数字证书发证机构	cert_ca	varchar2(100)	否	
26	数字证书有效期开始时间	cert_notbefore	varchar2(30)	否	
27	数字证书有效期结束时间	cert_notafter	varchar2(30)	否	
28	账户当前最高的可信等级	creditable_level_of_account	String	否	
29	账户可信级别以及核验方式字符串	creditable_level_of_account_way	String	否	

6.2 法人用户数据字典

法人用户关键信息如表3所示。

表 3　法人用户信息表

编号	字段名称	字段名	字段类型	是否必填	说明
1	用户名	uid	varchar2(100)	是	
2	联系人手机号	telephonenumber	varchar2(50)	是	隐私项
3	联系人电子邮箱	mail	varchar2(50)	否	
4	法人名称	cn	varchar2(100)	是	
5	法人证件类型	idcardtype	varchar2(10)	是	
6	法人证件号码	idcardnumber	varchar2(50)		
7	联系人姓名	link_person_name	varchar2(20)		
8	联系人证件类型	link_person_type	varchar2(10)		
9	联系人证件号码	link_person_code	varchar2(50)		隐私项
10	法人地址	address	varchar2(200)		
11	用户类型	usertype	varchar2(1)		
12	所属地市	area	varchar2(20)		
13	法定代表人姓名	legal_person	varchar2(20)		
14	法定代表人证件类型	legal_id_type	varchar2(10)		
15	法定代表人证件号码	legal_code	varchar2(50)	是	隐私项
16	法人账户（父账户）唯一标识	parent_uidcode	varchar2(32)	否	
17	用户来源	origin	varchar2(20)	是	
18	账号类型	accout_type	varchar2(1)	是	
19	用户唯一标识（UID）	useridcode	varchar2(32)	是	
20	用户信息更新时间	createtime	varchar2(30)	是	
21	用户信息版本	uversion	varchar2(4)	是	
22	实名状态	isreal	varchar2(10)	是	
23	实名注册类型	realtype	varchar2(4)	否	
24	实名注册位置	authloc	varchar2(100)	否	
25	审核单位	entdep	varchar2(100)	否	

26	审核人名	authnam	varchar2(20)	否	
27	场审核照片留存标记	authphoflag	varchar2(20)	否	
28	现场审核照片内容	authpho	varchar2(1000)	否	
29	数字证书内容	cert_data	varchar2(2000)	否	
30	数字证书发证机构	cert_ca	varchar2(100)	否	
31	数字证书有效期开始时间	cert_notbefore	varchar2(30)	否	
32	数字证书有效期结束时间	cert_notafter	varchar2(30)	否	
33	账户当前最高的可信等级	creditable_level_of_account	String	是	
34	账户可信级别以及核验方式字符串	creditable_level_of_account_way	String	是	

7 业务系统接入规范

7.1 概述

省统一身份认证平台（公众侧）分为网页版和小程序两种服务形式，申请方根据自身业务系统的场景，选择对接统一身份认证平台网页版或者小程序。

7.2 接入流程

a) 申请方提交接入申请，受理方分配测试环境参数；
b) 申请方根据受理方提供的参数配置测试环境，完成接入后，提供测试地址供受理方进行验证；
c) 受理方检查接入功能是否正常，若正常，并收到正式申请后，分配正式环境参数；
d) 申请方对正式环境进行配置，完成后进行单点登录、用户信息同步等功能的检测。

7.3 网页版接入规范

7.3.1 接入安全规范

业务系统不直接对接统一身份认证平台，使用OAuth2.0协议对接智能网关，进而间接对接统一身份认证平台，其中智能网关对业务系统透明。

7.3.2 接口调用时序

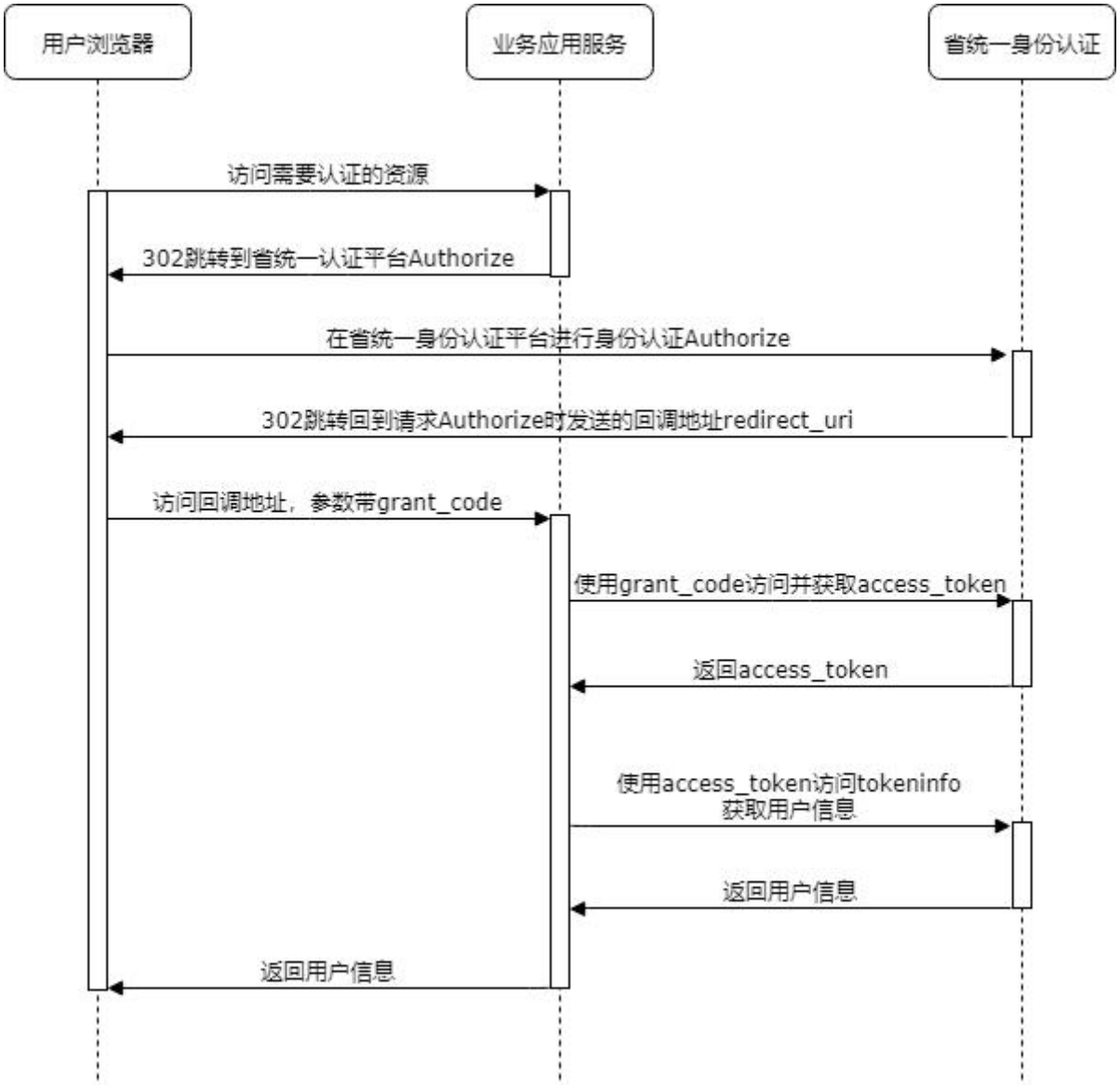

图 1 接口调用时序

图 1 接口调用时序如下所述：

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统一身份认证平台页面，同时带上回调地址；

b) 用户在省统一身份认证平台登录成功后，浏览器自动发起请求访问回调地址，并附带授权码参数；

c) 业务系统应用服务接收到请求后，应使用授权码参数访问省统一身份认证平台的获取令牌接口；

d) 省统一身份认证平台在响应体返回令牌值到业务系统应用服务；

e) 业务系统应用服务再次发起请求到省统一身份认证平台的获取用户信息接口，并使用令牌参数换取用户信息；

f) 业务系统应用服务将获得用户信息返回给用户。

7.3.3 接口说明

7.3.3.1 接口概述

业务系统对接网页版统一身份认证平台需调用获取授权码、获取令牌、获取用户信息、退出登录等四个接口。

7.3.3.2 获取授权码

表 4　获取授权码接口说明表

a） 请求示例：

接口功能	获取授权码
url	待提交接入申请表并批准后告知
参数	client_id ：业务系统向省统一认证平台申请的 client_id
	service：默认值为 initService；需要单独使用数字证书登录时，值为：userService
	scope ：应用向省统一认证平台请求的属性,默认为 all。
	redirect_uri ：认证完成并且用户对应用授权后返回的地址，此地址可以得到 grant_code 授权码。
	response_type 固定为 code
返回值	grant_code ：授权码。 获取方式，例如 request.getParameter("code")
http 请求方式	GET
说明	生产服务器地址:待提交接入申请表并批准后告知 测试服务器地址:待提交接入申请表并批准后告知

https://*********/tif/sso/connect/page/oauth2/authorize?service=initService&response_type=code&client_id=gdbscs&scope=all&redirect_uri=http%3a%2f%2fwww.gz13jd.gov.cn%2fcgs%2fhtml%2fhall%2findex.html

b） 正确返回示例：

grant_code：授权码。

获取方式，例如request.getParameter("code")

code：9fdeb881-b1e1-424d-8c16-b6e3e8bbe7b2%40node1

c） 错误返回示例：

报错参数不对或重定向地址不匹配等，未能获取到code值

d） 注意事项：

code值只能被使用一次，且有效时间为180s。

7.3.3.3 获取令牌

表 5 获取令牌接口说明表

接口功能	通过授权码获得访问令牌 access_token
url	待提交接入申请表并批准后告知
参数	client_id ： 应用向省统一认证平台预先申请的 client_id
	client_secret ： 应用向省统一认证平台预先申请的密钥
	code ： 授权码
	scope ： 应用向广东省统一认证平台请求的属性。
	redirect_uri ： 认证完成并且用户对应用授权后返回的地址。
	grant_type 固定为 authorization_code
返回值	access_token ： 访问令牌。 expires_in ： 有效期，单位是秒 token_type：获得的 Token 类型，Bearer 例如： {"expires_in":59,"token_type":"Bearer","access_token":"17120008-13ff-40fa-b573-7fcd3e638f25" }
http 请求方式	POST
说明	生产服务器地址:待提交接入申请表并批准后告知 测试服务器地址:待提交接入申请表并批准后告知

a） 请求示例：

https://********/tif/sso/connect/page/oauth2/access_token?client_id=gdbscs&scope=all&client_secret=123qwe&grant_type=authorization_code&redirect_uri=http%3a%2f%2fwww.gz1212jd.gov.cn%2fcgs%2fhtml%2fhall%2findex.html&code=9fdeb881-b1e1-424d-8c16-b6e3e8bbe7b2%40node1

b） 正确返回示例：

{"expires_in":59,"token_type":"Bearer","access_token":"17120008-13ff-40fa-b573-7fcd3e638f25"}

c） 错误返回示例：

报错参数不对或重定向地址不匹配等，未能获取到access_token值。

7.3.3.4 获取用户信息

表 6 获取用户信息接口说明表

接口功能	通过访问令牌 access_token 获得用户信息
url	待提交接入申请表并批准后告知
参数	access_token ： 访问令牌
返回值	access_token ： 访问 token expires_in ： 有效期，单位是秒 token_type：获得的 Token 类型，Bearer 其它都是用户信息。
格式	JSON
http 请求方式	GET
说明	生产服务器地址:待提交接入申请表并批准后告知 测试服务器地址:待提交接入申请表并批准后告知

请求示例：

http请求方式get

获取用户信息示例：

https://**********/tif/sso/connect/page/oauth2/tokeninfo?access_token=cce0319f-d1c5-499a-91ac-452e1666c813@node10

a) 返回示例：

access_token ： 访问token

expires_in ： 有效期，单位是秒

token_type：获得的Token类型，Bearer

其它用户信息。

7.3.3.5 退出登录

表 7 退出登录接口说明表

接口功能	通过调用接口退出省统一身份认证单点登录
url	待提交接入申请表并批准后告知
参数	redirect_uri ： 退出单点登录后返回的地址。
返回值	无
格式	无

http 请求方式	GET
说明	生产服务器地址:待提交接入申请表并批准后告知 测试服务器地址:待提交接入申请表并批准后告知

请求示例：Http请求方式get

https://**********/_tif_sso_logout?redirect_uri=http%3a%2f%2fwww.gzl212jd.gov.cn%2fcgs

7.4 小程序接入规范

7.4.1 接入场景

a) 登录

个人或法人用户在各政务应用 APP 或者小程序发起登录请求时,跳转至统一身份认证小程序进行登录操作。

b)实名核验

个人用户登录各政务应用 APP 或者小程序之后，发起实名核验请求，跳转至统一身份认证小程序进行实名核验。

7.4.2 接入要求

7.4.2.1 APP 接入要求

a) 必须在微信开放平台上注册移动应用，获得移动应用的APPID并关联小程序；
b) APP唤起小程序的代码块中username为小程序的原始ID；
c) APP唤起小程序的代码块中的path为跳转小程序的页面路径；
d) APP唤起小程序的代码块中的bundle_id 与申请的应用一致，不可用“测试版本Bundle ID”；
e) APP唤起小程序的代码块中的keystore和包名应保持与申请应用时所用的一致；
f) Android APP需要配置回调的进程信息。

7.4.2.2 小程序接入要求

a) 小程根据测试、上线的需求，填入欲唤起的小程序APPID;；
b) 小程序唤起小程序的接口中，path参数为欲跳转打开的页面路径；
c) 小程序唤起小程序时，在联调测试情况下，要填入唤起小程序的版本。

7.4.3 接口说明

7.4.3.1 接口概述

业务系统对接统一身份认证小程序可调用自然人刷脸登录、自然人实名核验、法人账号密码登录等接口。

7.4.3.2 自然人刷脸登录

表 8　自然人刷脸接口说明表

路径 path	（个人和法人登录统一入口 pages/authenticate/index/index） pages/authenticate/login/login-face/login-face
参数	from:唤起来源，app 为’app’，小程序为’miniProgram’，web 为’web’ appName:app 或小程序名称 skipbind: 是否跳过二级/三级账号绑定，跳过为 1，不跳过为 0，默认值为 0
返回值	"account": "zhang123" // 账号名 "account_type": "human" // 账号类型，"human"为个人账号 "cid": "440**********56" // 证件号码 "ctype": "10" // 证件类型，各证件类型见下方 "level": "四级" // 账号等级 "login_type": "SG-GASMHS" // 登录途径，"SG-GASMHS"为刷脸登录 "name": "张三" // 个人名称, "mobile": "138****0909" // 手机号
证件类型说明	"10": "身份证" "14": "港澳居民来往内地通行证" "15": "台湾居民来往大陆通行证" "20": "护照" "22": "港澳台居民居住证" "23": "外国人永久居留身份证" "40": "其他" "49": "统一社会信用代码" "50": "组织机构代码证" "80": "其他有效机构身份证件"
备注	a)若是业务小程序唤起的场景，返回数据格式为 json 格式； b)若是业务 app 唤起的场景，返回数据格式为 json 字符串格式。

7.4.3.3 自然人实名核验

表 9　自然人实名核验接口说明表

路径 path	pages/authenticate/login/realname-auth/realname-auth
参数	from: 唤起来源，app 为’app’，小程序为’miniProgram’，web 为’web’ appName:app 或小程序名称 account:待核验账户 cname:待核验姓名 cid:待核验身份证号
返回值	"account": "zhang123" // 核验的账号名 "auth": true // 核验结果，true 为成功，false 为失败
备注	a)若是业务小程序唤起的场景，返回数据格式为 json 格式； b)若是业务 app 唤起的场景，返回数据格式为 json 字符串格式。

7.4.3.4 法人账号密码登录

表 10　法人账号密码登录接口说明表

路径 path	（个人和法人登录统一入口 pages/authenticate/index/index） pages/authenticate/login/login-account/login-account
参数	from: 唤起来源，app 为’app’，小程序为’miniProgram’，web 为’web’ appName: app 或小程序名称 type: 2 // 1 代表个人，2 代表法人
返回值	"account": "junhe123" //账号名 "account_type": "corp" //账号类型，"corp"为法人账号 "cid": "914419**********60A" //证件号码 "ctype": "49" //证件类型，各证件类型见下方 "level": "三级" // 账号等级 "login_type": "password" //登录途径，"password"为账号密码登录 "name": "数字广东网络建设有限公司" // 法人名称 "mobile": "138****0909" // 经办人手机号
备注	a)若是业务小程序唤起的场景，返回数据格式为 json 格式； b)若是业务 app 唤起的场景，返回数据格式为 json 字符串格式。

8 用户信息同步规则

8.1 总体规则

业务系统接入省统一身份认证平台，涉及到用户信息的关联和同步，总体规则如下：

a) 兼容现有账户。用户首次使用省统一身份认证平台账号进入业务系统时，业务系统需提供用户本地已有账号的关联功能，如用户在业务系统没有账号，则自动创建用户信息，内容与省统一身份认证平台用户信息一致；

b) 用户自愿更改。同一用户在省统一身份认证平台为三级及以下可信账户、或在省统一身份认证平台和业务系统均为四级及以上可信账户的情况，当两者信息不一致时，业务系统需分别列出省统一账户用户信息和本地用户信息，业务系统根据用户选择，决定是否将本地用户信息更改为省统一账户用户信息；

c) 个性化信息自行维护。省统一身份认证平台仅提供账号名、证件名称、证件号码等用户基本信息，业务系统可根据自身业务特点，要求用户补充个性化数据，完善用户信息。对于用户个性化数据，由业务系统自行维护和管理；

d) 用户基本信息修改。用户只能在省统一身份认证平台修改基本信息。用户进入业务系统后，若需修改用户基本信息，业务系统应跳转至省统一认证平台供用户进行修改；

e) 实名账户转换。若账户在省统一认证平台为四级及以上可信级别，在业务系统为三级及以下可信级别的情形，业务系统须将本地关联用户信息更改为实名用户信息。

8.2 经办人账户的处理规则

用户为经办人账户(子账户)时，在使用经办人账户访问使用省统一账号登录业务系统时，对用户信息采用图2处理流程：

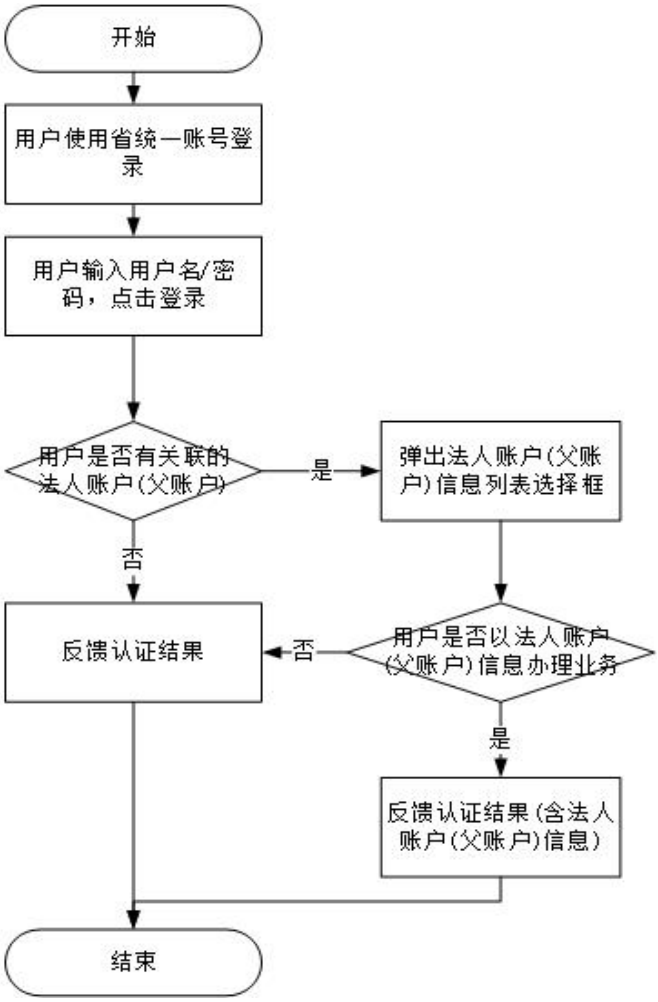

图 2　经办人账户代办处理流程

在以上流程中，针对用户是否为经办人账户分别进行以下两种处理方式，即根据用户的绑定关系判断用户是否有法人账户(父账户)选择不同的办理流程。

a)　若用户存在一个或更多的法人账户(父账户)，用户登录后，弹出“法人账户(父账户)信息选择框”，由用户自行选择是否以某个法人账户(父账户)身份进入业务系统；

b) 用户选择不以法人账户(父账户)身份访问业务系统时，则以自身的信息访问业务系统；用户选择以法人账户(父账户)身份访问业务系统时，则统一认证平台反馈给业务系统的认证结果中包含法人账户(父账户)信息。

参 考 文 献

[1] 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（国办发〔2018〕45号）
[2] 国家发展改革委关于印发“十三五”国家政务信息化工程建设规划的通知（发改高技〔2017〕1449号）
[3] 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（国办发〔2017〕39号）
[4] 国务院关于促进云计算创新发展培育信息产业新业态的意见（国发〔2015〕5号）
[5] 广东省人民政府关于印发广东省“数字政府”建设总体规划(2018-2020年)的通知（粤府〔2018〕105号）
[6] 广东省人民政府办公厅关于印发2019年全省一体化在线政务服务平台服务能力提升工作方案的通知（粤办函〔2019〕253号）