ICS 35.240.99
L 67

ZWFW

广 东 数 字 政 府 标 准 规 范

GDZW 0010-2019

广东省统一身份认证平台接入规范
（政务侧）

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（政务侧）对接国家统一身份认证系统，为全省政务人员提供统一的身份认证服务。实现“一个账号、一次登录、全省通用”。

本规范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政务人员统一身份认证的对接规范，规范对接流程和方法、服务接口、接口数据项目。

广东省统一身份认证平台接入规范（政务侧）

1 范围

本标准规定了广东省统一身份认证平台（政务侧）术语、总体要求、认证安全要求、业务系统接入规范、接口及参数说明。

本标准适用于广东省统一身份认证平台（政务侧）省级节点、地方和部门节点。

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 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

政务组织 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

用户 User

政务服务各业务管理平台的使用人员，是政务服务事项的业务受理单位的执行人员。

3.4

身份信息 Identity information

指政务人员身份的组成内容，身份信息包括姓名、身份证号、手机号等。

3.5

业务系统 The business system

指政务服务应用系统。如无特指，系指已集成在政务门户中的政务服务业务系统。直接与国家节点对接的业务系统在本规范系列中约定为直连业务系统。

3.6

统一身份认证 Unified identification

用户通过使用同一套用户凭证，可访问所有统一认证平台上与该用户身份对应的授权网络应用的过程。

3.7

单点登录 Single sign-on

在多个应用系统中，平台用户登录一次就可以访问所有相互信任平台应用系统的过程。

3.8

信任传递 Trust transfer

实现用户、业务系统的强身份鉴别、跨域条件下的信任传递。本建设方案特指在统一身份认证中心将已登录凭证传递到业务系统完成登录的过程。

3.9

凭证 Credentials

通过门户认证的用户身份的合法标识。

3.10

节点 Processing node

业务系统节点，具备身份认证服务能力的单元，是广东省统一身份认证平台（政务侧）的有机组成部分。

3.11

网关 Gateway

又称网间连接器、协议转换器。网关在网络层以上实现网络互连，是最复杂的网络互连设备，仅用于两个高层协议不同的网络互连。网关既可以用于广域网互连，也可以用于局域网互连。网关是一种充当转换重任的计算机系统或设备。

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)

ID标识号码（Identity Document）

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

Web 透过互联网访问的，由许多互相链接的超文本组成的系统（World Wide Web）

API 应用程序接口（Application programming interface）

5 业务系统接入规范

5.1 总体要求

业务系统接入广东省统一身份认证平台（政务侧）要求实现两个方面的对接，一是业务系统使用广东省统一身份认证平台（政务侧）账号登录，二是业务系统的组织机构用户信息同步。

5.2 登录

业务系统需关闭本系统用户注册、密码修改等身份认证功能，相关的功能通过广东省统一身份认证平台（政务侧）完成。用户在访问业务系统页面时，需要通过广东省统一身份认证平台（政务侧）进行认证登录，认证通过后，才允许访问业务系统。

用户访问业务系统，使用广东省统一身份认证平台（政务侧）账户登录流程如图1所示：

a) 用户访问业务系统，请求首先会通过广东省统一身份认证平台（政务侧）判断用户的登录状态，平台发现登录状态不存在或者失效时，跳转身份认证页面；

b) 用户根据页面选择扫码或者输入账号名及口令，提交请求；
c) 广东省统一身份认证平台（政务侧）对用户所输入的认证信息进行验证，验证通过后，把用户身份信息经签名后转发给后端的业务系统；
d) 业务系统接收用用户身份信息后，需验证签名正确性；验证通过后，关联本地系统的用户信息，判断用户的权限，允许用户登录办理业务。

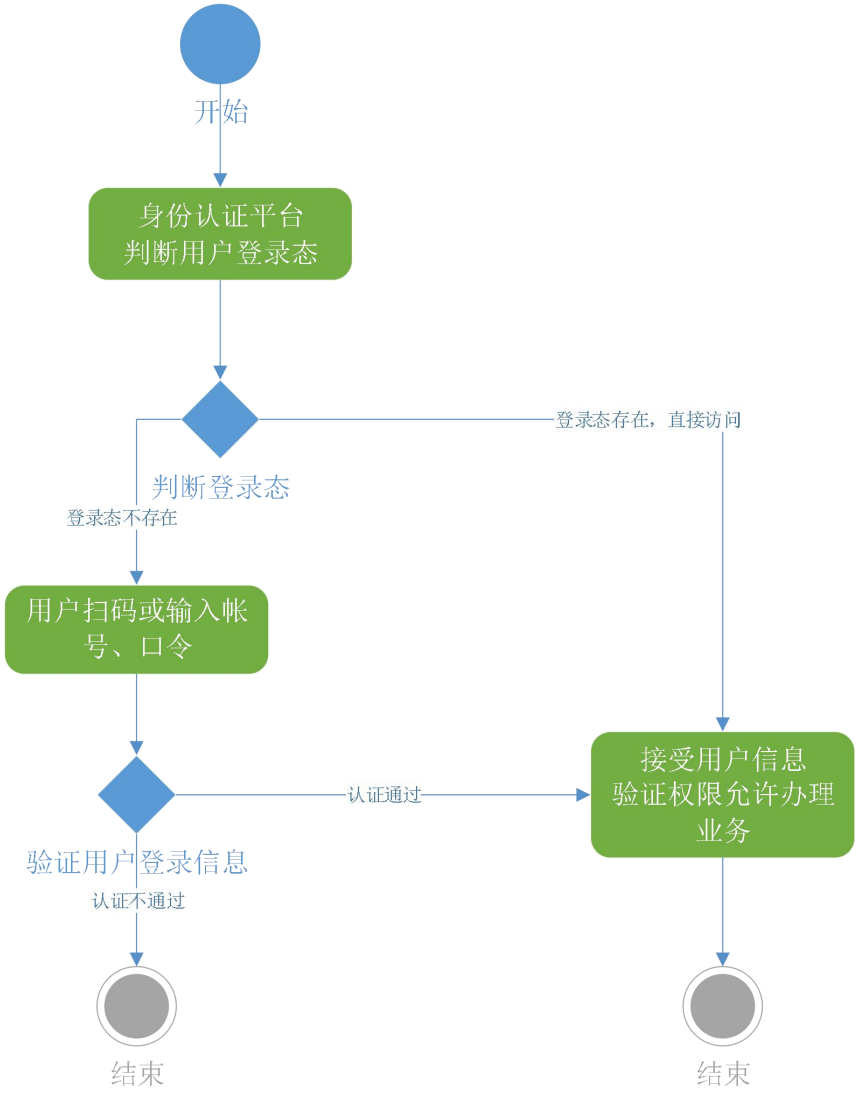

图 1　登录流程

5.3　同步政务组织及用户信息

业务系统需要同步广东省统一身份认证平台（政务侧）的单位和用户身份信息，从广东省统一身份认证平台（政务侧）获取所需要同步的单位（部门）ID。根据部门ID调用认证平台的接口，定时主动获取单位（部门）的组织机构和用户信息。

业务系统同步信息具体流程如图2所示：

a) 业务系统通过获取到的单位组织 ID，定时调用广东省统一身份认证平台（政务侧）的接口获取下级政务组织接口；
b) 业务系统根据返回的部门列表信息，存储到组织机构表，形成组织机构树；
c) 业务系统根据组织机构树的组织 ID，调用接口获取用户信息；
d) 业务系统存储用户信息并关联到组织机构树；流程结束。

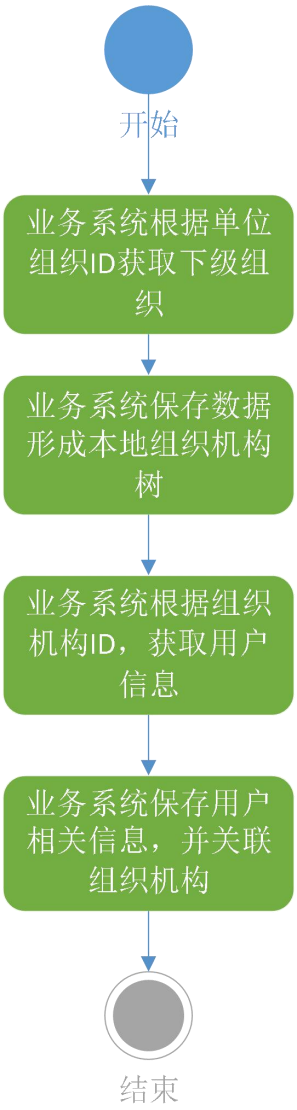

图 2 同步政务组织及用户信息

5.4 政务组织机构及用户信息初始化

业务系统的政务组织机构及用户信息需要进行初始化导入到广东省统一身份认证平台（政务侧），该工作建议由业务系统使用单位的分级管理员来完成，分级管理员账号通过各省直单位、各地市政务主管部门提出申请，由政务服务主管部门根据申请进行分配，分级管理员根据实际需要初始化政务组织机构和用户信息，并可以实时管理权限内单位组织机构和用户信息。

分级管理员管理权限内的政务组织及用户信息流程如图3所示：

a) 广东省统一身份认证平台（政务侧）根据业务系统接入的单位提出的申请分配分级管理员账号；
b) 分级管理员获取到账号后，登录广东省统一身份认证平台（政务侧）用户中心并下载组织及用户信息的导入模板；
c) 分级管理员按照模板要求收集并整理好对应的各单位组织机构及用户信息；
d) 分级管理员进入用户中心初始化导入政务组织机构及用户信息，流程结束。

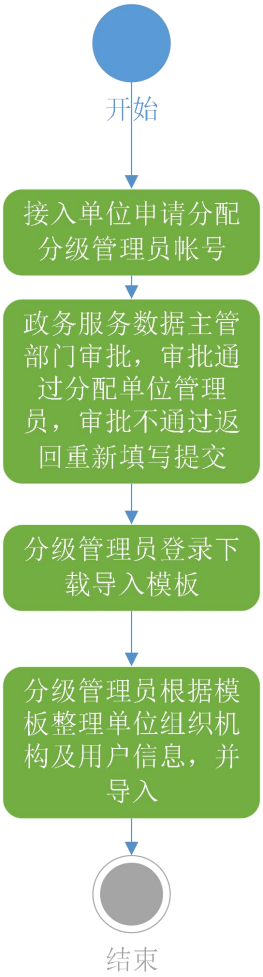

图 3 政务组织机构及用户信息初始化

6 接入工作流程

6.1 概述

接入工作流程主要包括接入前准备、接入前技术核准、接入改造、接入联调、接入开通五个阶段。

6.2 接入前准备

申请节点按以下要求进行准备：

a) 各节点应明确本地域名规划和认证服务节点域名规划，明确 IP 地址，制定部署方案，明确地方和部门节点部署位置，确保服务器部署在安全区域内；

b) 制定接入方案，描述对接环境和应用系统，描述接口调用方案，描述 IP 网络拓扑、 IP 地址、域名，描述安全防护方案。云平台、负载均衡设备、CDN 服务应单独详细描述；

c) 各节点应具备信息安全等级保护二级（或以上）的安全防护能力；

d)约定接入各方的工作职责。

6.3 接入申请

地方和部门节点向省政务服务数据主管部门申请接入，申请时根据需要包含以下内容：

a) 政务业务系统接入广东省统一身份认证平台（政务侧）申请；

b） 网关接入申请；

c） 订阅网关服务申请；

d） 发布网关服务申请；

e） 其他必须的信息。

6.4 接入核准

对申请节点提供的技术信息和接入方案进行评测后，省政务服务数据主管部门核准是否接入，核准后节点建立以下接入要素：

a） 申请节点的服务地址数据（建立IP、域名、访问控制列表等）；

b） 回复服务地址列表，申请方通过读取服务地址获取包括登录认证服务、票据服务、 令牌服务、隐性登录服务、用户信息查询、登出服务消息订阅服务等地址；

c） 其它必须的信息。

6.5 接入改造

应遵从本标准对接入节点范围内的政务服务门户和业务系统中的身份认证相关业务进行梳理，按照政务服务认证流程进行接入改造。

申请节点应选定统一模式或协同模式，按选定方式进行改造。

统一模式：登录认证、用户空间管理等功能都由省节点统一身份认证平台完成，地方和部门节点通过对接省节点完成本地用户登录认证及跨节点信任传递。

协同模式下：登录认证、用户空间、单点登录均由各地方和部门节点建设完成，在现有系统内增加指向省节点的链接，通过和省节点的信任传递系统对接，实现跨节点访问通用。

6.6 接入联调

应遵从本标准、对接入节点范围内的政务服务门户和业务系统中的身份认证相关业务进行联调。

6.7 接入开通

省政务服务数据主管部门根据申请信息完成配置、开通接入服务后，通知申请方完成接入。

7 业务系统接口规范

7.1 接入接口要求

业务系统通过但不限于网关和OAuth2.0接入的方式对接统一身份认证平台。统一身份认证平台对外提供两种接入模式，网关模式和OAuth2.0模式。网关模式主要由准入网关作为中间件实现与统一身份认证中心的对接；OAuth2.0模式由业务系统经API网关对接统一身份认证中心，通过OAuth2.0协议进行访问。

7.1.1 网关接入调用流程

网关接入调用流程如图 4。

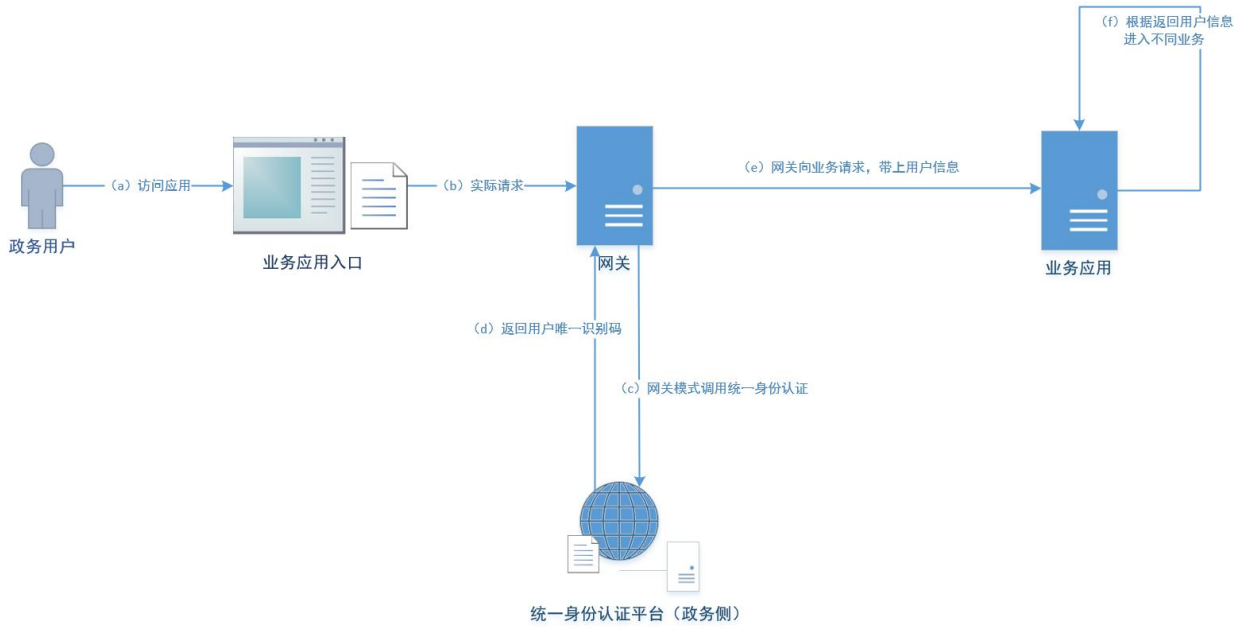

图 4 网关接入调用流程

a） 政务用户访问应用；
b） 实际访问请求定向到网关；
c） 网关定向至统一身份认证，政务用户进行身份认证；
d） 身份认证返回用户唯一标识码；
e） 网关将访问请求带上用户信息后，重定向至业务应用；
f） 业务应用根据用户信息进行业务处理。

7.1.2 OAuth2.0 接入调用流程

OAuth2.0 接入调用流程如图 5。

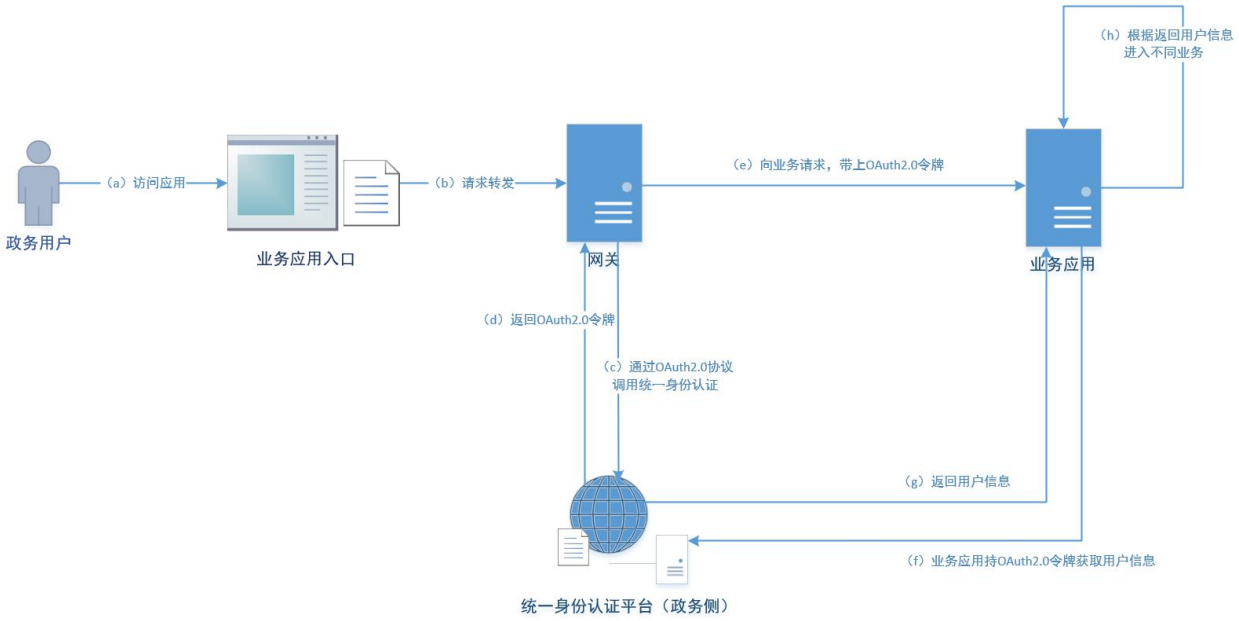

图 5 OAuth2.0 接入调用流程

a） 政务用户访问应用；

b） 实际访问请求被定向到 API 网关；
c） 准入网关调用统一身份认证，对政务用户进行身份认证；
d） 身份认证按 OAuth2.0 协议返回认证令牌；
e） 准入网关将访问请求带 OAuth2.0 认证令牌重定向至业务应用；
f） 业务应用持令牌访问统一身份认证平台（政务侧）；
g） 统一身份认证平台（政务侧）根据令牌返回用户信息；
h） 业务应用根据用户信息进行业务处理。

7.2 组织机构及用户信息同步接口

业务系统通过调用广东省统一身份认证平台（政务侧）的相关接口获取组织机构及用户信息。接口主要提供如下功能：机构查询和用户查询接口。

7.2.1 根据组织单元 ID 获取组织单元信息

接口名称：getUnitByUnitID
接口描述：获取组织单元信息。
输入参数：

字段	说明	类型	是否必填	备注
unitid	组织单元 ID	string	是	

调用示例：

```
{"unitid":"5566"}
```

成功返回组织单元全部信息。

结果示例：


```
{
    "unitname": "XX 部门",
    "isvirtual": false,
    "extend": {
        "orgType": "3",
        "weworkpartyid": [5*2]
    },
    "parentunits": [{
        "unitid": "073ku***************va",
        "order": 10*****823,
        "priority": 1
    }],
    "unitid": "073tk***************l1",
```

"createtime": "2019-01-07T09:52:47.927Z",

"updatetime": "2019-01-07T09:52:47.927Z",

"unitpath": ["/广东省政府/XX 厅/ XX 部门"],

"errcode": 0,

"errmsg": "ok"

}

7.2.2 根据组织单元 ID 获取某个组织单元下的所有组织单元

接口名称：getChildUnitByUnitID

接口描述：根据组织单元 ID 获取某个组织单元下的所有组织单元。

输入参数：

字段	说明	类型	是否必填	备注
unitid	组织单元 ID	string	是	

调用示例：

```
{
        "unitid":"5566"
}
```

成功返回组织单元数组。

结果示例：

{

"units": [{

"unitname": "XX 部门",

"isvirtual": false,

"extend": {

"orgType": "3",

"weworkpartyid": [582]

},

"parentunits": [{

"unitid": "073ku**********va",

"order": 107*****23,

```
            "priority": 1
        }],
        "unitid": "073tk***************11",
        "createtime": "2019-01-07T09:52:47.927Z",
        "updatetime": "2019-01-07T09:52:47.927Z",
        "unitpath": ["/广东省政府/XX 厅/ XX 部门"]
    }],
    "errcode": 0,
    "errmsg": "ok"
}
```


7.2.3 获取组织单元所有用户

接口名称：getUsersByUnitID
接口描述：获取某个组织单元下的所有用户。
输入参数：

字段	说明	类型	是否必填	备注
unitid	组织单元 ID	string	是	

调用示例：

```
{
        "unitid":"5**6"
}
```

成功返回所有用户列表。

结果示例：


```
{
    "users": [{
        "username": "史 XX",
        "displayname": "史 XX",
        "account": "11***************1",
        "gender": "1",
        "mobilenumber": "138********",
        "certificatetypeid": "5",
        "certificatenumber": "440113********0133",
        "status": 0,
```

```
            "userid": "073kv**************xo",
            "createtime": "2018-12-21T11:55:14.353Z",
            "updatetime": "2018-12-26T04:22:10.494Z",
            "units": [{
                "unitid": "073ku**************va",
                "order": 10******91,
                "unitleader": false,
                "position": "",
                "priority": 1
            }],
            "birthday": ""
        }, {
            "username": "余 XX",
            "displayname": "余 XX",
            "account": "22**************2",
            "gender": "1",
            "mobilenumber": "137****3456",
            "certificatetypeid": "5",
            "certificatenumber": "440110********2188",
            "status": 0,
            "userid": "073ly**************ig",
            "createtime": "2018-12-23T15:01:41.301Z",
            "updatetime": "2018-12-26T04:22:11.269Z",
            "units": [{
                "unitid": "073ku**************va",
                "order": 10******35,
                "unitleader": false,
                "position": "",
                "priority": 1
            }],
            "birthday": ""
        }],
        "errcode": 0,
        "errmsg": "ok"
    }
```


7.3 数据元说明

7.3.1 组织机构信息

统一身份认证平台组织机构信息包含但不限于表 1 的组织机构信息内容。

表 1　组织机构信息表

序号	数据元名称	字段名	数据类型	是否可空	说明
1	机构节点名称	unitname	varchar2(100)	非空	
2	机构节点 ID	unitid	varchar2(100)		
3	创建时间	createtime	Date	非空	
4	更新时间	updatetime	Date	非空	
5	部门全路径	unitpath	varchar2(2000)	可空	
6	父部门 ID	Parentunits.unitid	varchar2(100)	非空	
7	排序号	Parentunits.order	Int	非空	
8	是否主部门	Parentunits.priority	varchar2(32)	可空	1 是，0 否
9	部门类型	Extend.orgType	varchar2(4)	可空	包含： 市级行政区划 区县行政区划 乡镇级行政区划 单位集 单位

					部门

7.3.2 用户信息

统一身份认证平台用户信息包含但不限于表 2 的用户信息。

表 2 用户信息表

序号	数据元名称	字段名	数据类型	是否可空	说明
1	用户名称	username	varchar2(100)	非空	
2	显示名称	displayname	varchar2(100)	可空	
3	账号	account	varchar2(100)	非空	
4	性别	gender	Int	非空	
5	手机号码	mobilenumber	Int	非空	
6	证件类型	certificatetypeid	Int	非空	
7	证件号码	certificatenumber	varchar2(100)	非空	
8	用户 ID	userid	varchar2(32)	非空	支持与部门 ID 一对多的关系。即：一个用户可以属于多个部门场景。
9	创建时间	createtime	Date	可空	
10	更新时间	updatetime	Date	可空	
11	所属部门 ID	Units.unitid	varchar2(32)	非空	
12	排序号	Units.order	Int	非空	
13	是否领导	Units.unitleader	Int	可空	
14	职位	Units.position	varchar2(100)	可空	

15	是否主职部门	Units.priority	Int	可空	

8 认证安全加密要求

8.1 基本要求

a) 系统所使用的加密算法需要支持国密规范；

b) 地市和省级节点需要对隐私数据进行保护；

c) 地市和省级节点在用户登录认证会话中禁止暴露令牌，令牌等认证信息应在认证服务器之间传递，禁止经由用户设备或其他第三方传递；

d) 地方和部门节点间传输令牌、用户信息等数据时，应对通讯进行加密和签名：

e) 地市和省级节点应使用 HTTPS 协议对外提供服务，禁止使用 HTTP 协议。

8.2 系统安全要求

按省统一身份认证系统规定密码口令、验证码、登录异常提醒、登录异常处理、登录日志审计规范要求。

- **口令**

a) 系统应具备对口令强度检测的能力，并对用户进行提示（尽量不要以姓名拼音、电话号码以及出生日期等作为口令或者口令的组成部分），阻止常见弱口令的配置；

b) 应以不可逆加密技术保存口令，禁止以明文方式保存或者传输；

c) 采用不可逆加密算法认证过程中，每次认证时，由服务端随机生成 盐值参与运算；

d) 修改口令时，保留口令修改记录，包含账号、修改时间、修改原因等，以备审计。

- **验证码**

a) 短信验证码的长度要求

1）纯数字类：不少于 6 位 ；

2）英文字符+数字类：不少于 4 位。

b) 单位时间内，应限制用户可获取动态短信验证码的次数，对于超过可获取次数的用户，暂停下发动态短信验证码。

- **登录异常提醒**

a) 设置用户业务认证登录失败提醒策略，当用户登录失败超过限定次数时，发送消息到已登记的手机号或邮箱，提醒用户是否为本人操作；

b) 同一时间同一账号在多终端进行尝试登录应发送短信提醒。

- **登录异常处理**

a) 设置用户业务认证登录策略，限定连续登录失败次数（如 5 次）、锁定时间（如 1 小时）、解锁方式；

b) 应配置同一用户连续认证失败次数，连续认证失败次数超过限定次数（如 5 次）时，锁定该用户使用的账号；

c) 应配置当来自同一终端、IP 的不同账号连续认证失败次数，认证失败次数超过限定次数（如 5 次），锁定来自该终端、IP 的登录请求。

- **登录日志审计**

a) 应配置登录日志留存，对用户登录进行记录，登录日志内容至少包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时用户使用的 IP 地址；

b) 审计登录日志，如在限定时间内（例如 5 分钟），同一用户名产生的登录日志条数超过限定数量，则报告账号异常。

8.3 通讯接口分类

- **一级接口**

通讯接口不涉及用户身份信息的定义为一级。

- **二级接口**

通讯接口涉及用户身份信息，使用散列值的定义为二级。

二级接口遵从以下安全要求：

a) 一级接口所遵循的要求；

b) 用户信息进行散列时，调用省节点下发的散列函数获取散列值；

c) 遵循本规范8.4的通讯加密与签名，对请求和回复进行签名。

- **三级接口**

通讯接口涉及用户身份信息的，使用散列值的定义为三级。

a) 二级接口所遵循的要求；

b)用户信息进行散列时，调用省节点下发的散列函数获取散列值；

c) 遵循本规范8.4的通讯加密与签名，对请求和回复进行签名。

8.4 接口和通讯安全要求

对于可能传递敏感信息的接口调用，应采用加密和签名等方式加强安全。要求如下：

a) 服务请求应包含节点 ID 、时间戳、请求级别等信息；

b) 请求方对主体内容须进行加密和签名，接收方收到请求后进行解密和验签；

c) 接收方回复数据应进行加密和签名，请求方收到数据时进行解密和验签。

8.5 浏览器访问通讯安全要求

用户登录Web服务，应采用 HTTPS 协议，禁止使用HTTP协议。浏览器访问过程中禁止明文传递用户口令，应加密或散列处理。统一身份认证系统各节点间Web重定向，应使用 HTTPS 协议，只能携带票据、不能使用 令牌。请求参数中若出现证件号、手机号等隐私信息时，应使用散列值。

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）