国家智慧教育公共服务枢纽

标准规范

统一身份认证接入规范

教育部教育技术与资源发展中心

（中央电化教育馆）

目录

1. 相关背景

按照国家教育数字化战略行动的统一部署，根据第三次部长专题办公会议、2022 年教育部网信领导小组第一次会议和进鹏同志关于教育数字化的系列重要指示精神，以国家智慧教育公共服务平台（以下简称智慧教育门户）建设推动教育数字转型，促进教育高质量发展。到 2022 年底，构建国家智慧教育公共服务枢纽（以下简称国家公共服务枢纽），集成国家教育数字化战略行动的各级各类平台，覆盖基础教育、职业教育、高等教育各阶段资源类和服务类平台，打造统一身份认证枢纽，实现平台互联、数据互通、应用协同，用户“一网通览”“一网通办”，为推进教育大数据持续赋能教育教学、教育评价、教育治理、教育服务创新，实现资源内容、教育服务的动态汇聚和智能推送，实现基于国家公共服务枢纽的数据返还。为规范各级各类平台、服务的接入和数据采集，加强协同服务，强化运行情况的动态监测，促进资源共享，特编制本套规范。

2. 适用范围

本规范定义了各级各类系统统一的接入流程和实现要求，方便各类系统快速接入到国家公共服务枢纽，各级系统应按照国家公共服务枢纽标准规范建设和改造，遵循“标准规范统一、用户实名唯一”的要求，按照枢纽接口规范，为用户提供安全稳定的登录认证和各项服务，实现用户“一网通览”

“一网通办”。

3. 相关定义

本规范定义国家智慧教育公共服务枢纽相若干关键词及解释。

用户 广泛的含义是使用者，在国家公共服务枢纽中进行操作使用的人群，包括学生、老师、家长、学校管理员等。这些用户可以在公共服务枢纽中一点登录，全网漫游，无缝使用各类资源。

机构 即法人机构，包括教育机构和学校，其中教育机构指的是教育局、电教馆等事业单位；学校是有计划、有组织地进行系统的教育的组织机构。

令牌 接入国家公共服务枢纽的平台、服务访问国家公共服务枢纽的一个标识，API 接口只有拥有 token 才能正常使用。

区域 区域是数据共享中心的基本组成部分，可以只有一个区域，也可以有多个区域，每个区域可对应自身的数据共享中心。省、市、区县等，都是一个区域。

报文 报文可以看作是数据对象和事件对象的载体，数据对象和事件对象必须放在报文中才能够传递。报文同样使用 JSON 或者 XML 元素来表示，数据的传递都是由报文承载的。

数据模型 数据共享中心可以共享的数据是通过一系列数据对象进行定义的。数据模型是描述数据对象的语义模型，数据共享中心数据规范提供了各类数据对象的数据模型。

数据代理 数据代理的职责是将业务系统的数据转化为规范的格式，或将

接受到的数据转化为业务系统的数据格式，代理通过数据共享中心的 SDK 使用数据共享中心的服务，业务系统通过代理实现数据的交换与共享，业务系统无需关注数据共享的细节，可以完全按照面向数据对象的方式去完成数据共享。数据代理就是业务系统与数据共享中心之间的桥梁。

智教中国通行证统一身份认证 该功能提供统一登录和授权界面进行登录认证授权，允许各类平台或终端在用户获取授权的前提下直接访问其他平台。无需将用户的用户名和密码提供给第三方系统。类似“微信登录”，更适合移动端 APP 认证。

4. 接入规范

国家智慧教育公共服务枢纽是政府提供教育资源、教育服务等基本公共服务的载体。所有接入的系统需遵循统一的命名规范、信息安全规范、界面设计规范。

4.1 接入流程

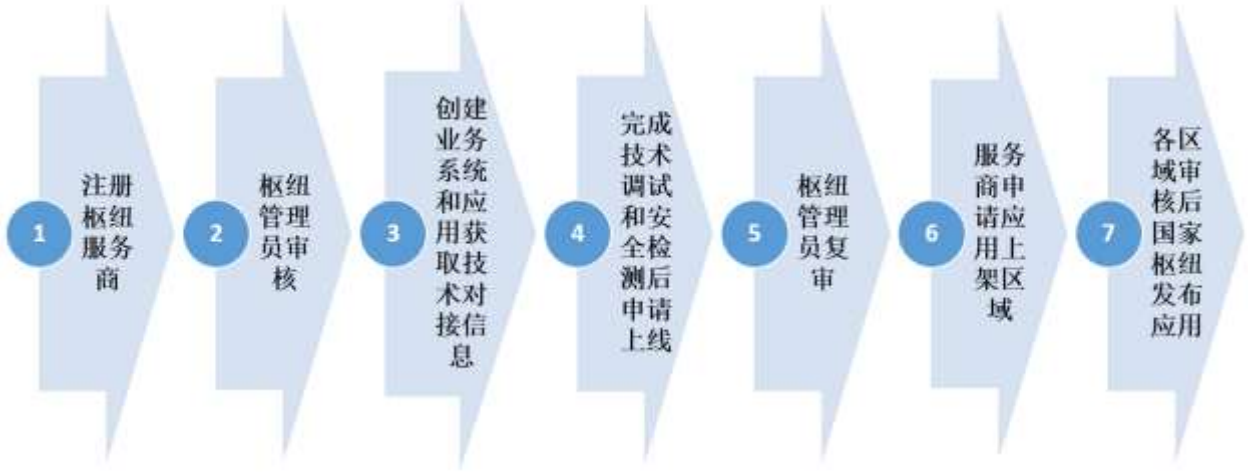

图 4 接入流程图

各级各类业务系统主管部门可在公共服务枢纽门户（https://system.smartedu.cn）注册服务商，枢纽管理员统一审核服务商资质。枢纽管理员收到服务商接入的申请资料，审核无误后服务商可自行创建业务系统信息和应用信息，应用可按终端和角色分别创建，应用创建完成会生成对应的 APPID 和 APPKEY，服务商依据本规范进行接口调试和技术测试后方可申请应用上线，枢纽管理员线上审核确认后应用即可上线。注意：不在白名单的服务端 IP 将无权限调用枢纽接口，接入 ID 和 KEY 与各应用一一对应，为避免统计数据错误，请勿滥用。

4.2 认证对接

智慧教育枢纽为各平台用户提供“智教中国通行证”统一身份认证服务，为各级各类业务系统提供统一标准的接入规范。

“智教中国通行证”统一身份认证务功能提供统一登录、授权界面进行

登录认证授权，允许各类平台或终端在用户获取授权的前提下直接访问其他平台。无需将用户的用户名和密码提供给第三方系统。类似“微信登录”，更适合移动端 APP 认证。OAuth 允许用户提供一个令牌给各应用，一个令牌对应一个特定的应用，同时该令牌只能在特定的时间内访问特定的资源。各应用可以通过 OAuth 的授权认证，使用公共服务枢纽的用户账号密码登录自身系统。该认证方式依托服务枢纽的 OAuth 认证服务，接入的系统如果有自身的用户中心服务和身份认证服务，平台可以使用自身账号登录，也可以使用“智教中国通行证”进行登录；用户第一次使用“智教中国通行证”在应用系统登录时，在应用系统形成账号绑定关系，以后登录则无需再次绑定；接入的系统如果没有自身的用户中心服务和身份认证服务，则无需绑定用户，只需要记录每次用户的登录信息。

4.2.1 使用场景

目标：统一身份认证服务主要适用于接入到国家智慧教育平台的各类应用系统，依赖“智教中国通行证”进行单点登录。

特点：业务系统需要使用“智教中国通行证”进行登录，可以使用国家枢纽提供的统一身份认证服务。接入的系统如果有自身的用户中心服务和身份认证服务，平台可以使用自身账号登录，也可以使用“智教中国通行证”进行登录；用户第一次使用“智教中国通行证”在应用系统登录时，在应用系统形成账号绑定关系，以后登录则无需再次绑定；接入的系统如果没有自身的用户中心服务和身份认证服务，则无需绑定用户，只需要记录每次用户的

登录信息。

4.2.2 时序图

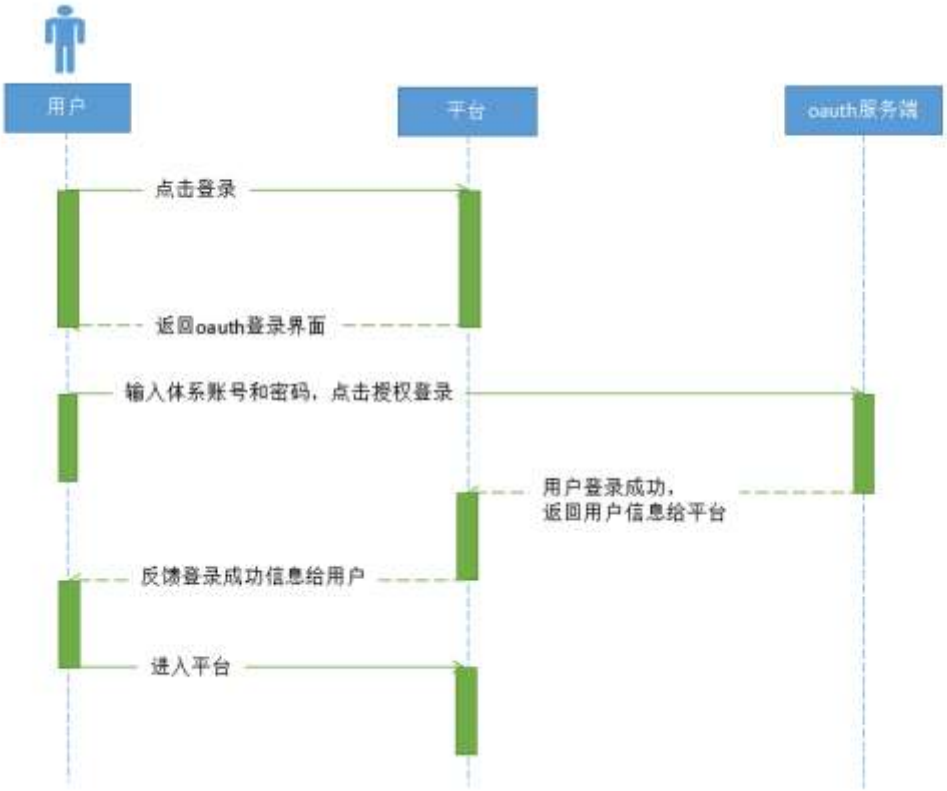

图 9 OAuth 授权认证时序图

4.2.3 开发规范

4.2.3.1 配置 OAuth 登录入口

第三方系统接入流程完毕后,需要拿到 OAuth 的登录地址和 oauth 的 LOGO 图片进行跳转到登录认证页面。

在第三方系统中加载服务枢纽 logo(logo 平台可以自己设定大小和样式)和 oauth 链接。

- Oauth 链接地址:

■ 测试链接：

- https://ip:port/uias/oauth/authorize?client_id=***&grant_type=authorization_code&response_type=code&redirect_uri=平台回跳 url

■ 参数说明：

client_id:在国家公共服务枢纽接入之后就会生成一个 AppId 和 AppKey,AppId 即为 client_id 是应用认证授权的唯一标识，AppKey 即为 client_secret 是应用的密钥。

grant_type：授权模式,固定传“authorization_code”。

response_type：返回类型，固定传“code”。

redirect_uri：登录成功后跳转到第三方系统的地址，也是平台接入时候的 url 地址。

■ 服务枢纽 logo 图标放置在第三方系统的示例

图 10 第三方示例

4.2.3.2 授权登录

老师、学生等用户打开第三方系统后，需要通过“智教中国通行证”登录到第三方系统，点击服务枢纽 logo 标记可以跳转到 oauth 登录页面，如下图：

图 11 从服务枢纽 logo 跳转到 oauth 登录页面

图 12 授权确认页面

登录说明：

a)输入“智教中国通行证”帐号和密码；

b)验证用户信息和配置参数成功，用户授权成功后，重定向到平台的回调地址；

c)回调地址格式：

http://ip:port/XXX?code=9d82a9ca

- 回调地址(http://ip:port/XXX)：是第一步中的回调地址 redirect_uri。
- code：枢纽用户成功登录后的临时授权码，一次有效，有效期为 5 分钟。

4.2.3.3 根据授权码获取接口访问令牌

第三方系统调用枢纽接口的第一步，访问令牌是服务商使用接口的凭证，通过访问令牌服务商可以使用自身权限下的各种接口。

根据授权码 code 换取 access_token

- https:// ip:port /uias/oauth/token
- Post 请求类型：application/x-www-form-urlencoded
- Post 请求参数：

  grant_type：authorization_code 固定值

  code：授权码

  client_id：应用 id，系统自动生成 APPID；

  client_secret：应用秘钥，系统自动生成 APPKEY；

  redirect_uri：登录成功后跳转到第三方系统的地址，也是第三方系统接入时候的 url 地址；

- 响应报文

```
{
    "access_token": "c517268c-cab6-4987-93ee-83084f667f8b",
    "token_type": "bearer",
```

```
    "refresh_token": "98db9a15-f9d2-4e22-a1ef-f31af77d69fb",
    "expires_in": 7199,
    "scope": "userInfo",
    "client_id": "0MOD9Mi1vk2UHAQk6AHFe40ARj1YDKkK"
}
```


access_token: 访问令牌，2 个小时有效期

refresh_token: 刷新 token, 7 天有效期

expires_in: 访问令牌过期时间

scope: 授权范围

client_id: 客户端 APPID

token_type: 令牌类型

- 具体 API 请参照《接口规范》。

4.2.3.4 根据访问令牌获取用户通行证信息

第三方系统根据 Oauth 成功登录后回调的参数，调用枢纽开放接口服务可以获取登录用户的信息。请使用智教中国通行证 ID（唯一标识）绑定本平台用户，用于确定唯一的教育用户。

- 调用接口信息如下：
  - ■网关请求地址：

http://IP:PORT/data/user/getUserInfo

请求参数：

access_token：请求访问令牌

  - ■请求报文：


```
{
    "access_token": "9d82a9ca43887a73c2e2"
}
```


  - ■请求签名，具体 API 请参照《接口规范》
  - ■应答报文：

```
{
    "data": {
        "defaultIdentity": "0",
        "gender": "2",
        "name": "李好",
        "smartEduCard": "1101012011123423434"
    },
    "retCode": "000000",
    "retDesc": "请求成功",
    "success": true
}
```


- 具体 API 请参照《接口规范》。

4.2.3.5 刷新访问令牌

① 接口描述

刷新访问令牌信息。

② 前置条件

获取到刷新 token：refresh_token。

③ 请求说明

表 1 请求说明

url	http://ip:port/uias/oauth/token
请求方式	Post
格式	application/x-www-form-urlencoded
是否需要鉴权	是
请求数限制	是
接口方向	第三方系统>公共服务枢纽

④ 请求参数

a) 请求 Body 参数：

表 2 请求参数

序号	字段名	约束	类型	说明
1	refresh_token	必选	String	刷新 token
2	grant_type	必选	String	refresh_token 固定值
3	client_id	必选	String	应用 id，系统自动生成 APPID;
4	client_secret	必选	String	应用秘钥，系统自动生成 APPKEY
5	redirect_uri	必选	String	登录成功后跳转到第三方系统的地址，也是平台接入时候的 url 地址;

⑤ 返回参数

表 3 返回参数

序号	字段名	约束	类型	说明
1	access_token	必选	String	访问令牌，2 个小时有效期
2	token_type	必选	String	令牌类型
3	refresh_token	必选	String	刷新 token， 7 天有效期
4	expires_in	可选	Int	访问令牌过期时间
5	scope	可选	String	授权范围

6	client_id	可选	String	客户端 APPID
7	id_token	可选	String	授权身份 id_token，统一退出参数

⑥ 接口示例

表 4 接口示例

请求报文：

```
{
    "refresh_token":"1212****",
    "grant_type":"refresh_token",
    "redirect_uri":"xxxxxxxx",
    "client_id":"xxxxxx",
    "client_secret":"xxxxxx"
    }
```

应答报文：

```
{
        "access_token":  "2f52a68f-9cec-44fc-8c7e-c6008ab30547",
        "token_type":  "bearer",
        "refresh_token":  "d7355e72-6985-41d7-875c-25449b8c8dd4",
        "expires_in":  7199,
        "scope":  "userInfo",
        "client_id":  "OMOD9Mi1vk2UHAQk6AHFe4OARj1YDKkK",
        "id_token":  "*******"
}
```

- 具体 API 请参照《接口规范》。

4.2.3.6 统一登出接口

① 接口描述

国家枢纽登出之后，同步登出第三方系统。

② 前置条件

获取到 id_token：id_token。

③ 请求说明

表 5 请求说明

url	http://ip:port/uias/token/logout?id_token_hint=***&logout_redirect_uri=http://***thirdlogout.domain
请求方式	Get
格式	Get 方式
是否需要鉴权	是
请求数限制	是
接口方向	第三方系统>公共服务枢纽

④ 请求参数

a) 请求参数：

表 6 请求参数

序号	字段名	约束	类型	说明
1	id_token_hint	必选	String	授权身份 id_token 的值
2	logout_redirect_uri	必选	String	回调前台退出地址，实现客户端清理缓存和退出

⑤ 返回参数

表 7 返回参数

登出回调地址： http://***thirdlogout.domain ，该地址由客户端提供，实现客户端前台退出操作

⑥ 接口示例

表 8 接口示例

请求报文： http://ip:port/uias/token/logout?id_token_hint=***&logout_redirect_uri=http://www.baidu.com/logout 应答报文： http://www.baidu.com/logout 客户端清理本地用户缓存和退出

- 具体 API 请参照《接口规范》。

4.2.3.7 统一登出通知接口（由第三方系统提供）

① 接口描述

统一认证退出时，会通知当前用户已经登录过的平台或应用进行统一退出，需要退出的平台和应用，需要提供该接口。统一登出通知，分为前台退出和后台退出 2 种。

② 前置条件

用户在当前浏览器访问具体应用，需要统一退出

前台退出和后台退出如下：

- 前台退出方式，需要提供 https 退出地址

表 9 请求说明

url	https://(第三方前台退出接口地址)?access_token=*** 该接口必须提供 https 退出方式
请求方式	Get
格式	Get 方式
是否需要鉴权	是
请求数限制	是
接口方向	公共服务枢纽>第三方系统

a) 请求参数

表 10 请求参数

序号	字段名	约束	类型	说明
1	access_token	可选	String	访问令牌，2 个小时有效期,平台枢纽颁发的令牌

b) 接口处理逻辑

该前台退出接口，用于清空本地的用户当前浏览器登录状态，包含 cookie，缓存，token 等信息，access_token 为平台枢纽颁发的令牌，平台和应用方可根据此字段，判断来源于平台枢纽，找到对应的具体用户信息，精准退出。

- 后台退出方式，需要提供后台退出地址，https 和 http 不限，从枢纽后台统一异步通知对应的应用方退出

表 11 请求说明

url	https://(第三方后台退出接口地址)?access_token=***
请求方式	Get
格式	Get 方式
是否需要鉴权	是
请求数限制	是
接口方向	公共服务枢纽>第三方系统

a) 请求参数：

表 12 请求参数

序号	字段名	约束	类型	说明
1	access_token	必选	String	访问令牌，2 个小时有效期,平台枢纽颁发的令牌

b) 接口处理逻辑

该后台退出接口， access_token 为平台枢纽颁发的令牌，平台和应用方可根据此字段，映射本地平台具体的用户，通过后台注销的方式，清理具体用户的缓存信息，实现退出。

- 具体 API 请参照《接口规范》。

4.2.3.8 平台栏目或应用访问接口（临时）

① 接口描述

平台栏目或应用访问接口，目前临时用于套头页内封装地址重定向跳转到第三方系统主域名之外的跳转入口，可指定跳转到具体栏目或服务入口。后续接入枢纽的服务入口统一通过接口获取，服务入口跟着用户走。

② 前置条件

获取到 client_id

③ 请求说明

表 13 请求说明

url	http://ip:port/uias/app/view?client_id=***&state=base64 编码（http://thirdaddr.domain）
请求方式	Get
格式	Get 方式
是否需要鉴权	是
请求数限制	是
接口方向	第三方系统>公共服务枢纽

④ 请求参数

a) 请求参数：

表 14 请求参数

序号	字段名	约束	类型	说明
1	client_id	必选	String	访问目标平台或应用的 client_id
2	state	可选	String	可选参数，访问目标平台或应用的重定向绝对地址，该地址需要申请白名单，需要 base64 编码。如果该参数不传，未登录情况下，跳转到平台应用首页地址；已登录情况下，平台应用默认的回调地址。如果改参数已传，未登录情况下，跳转到平台应用重定向

				地址；已登录情况，跳转到回调地址，state 作为参数原样返回，由平台应用端处理具体的页面跳转

⑤ 返回参数

重定向地址：

1. 未登录：

   a. 未携带 state 传参： 跳转到平台应用的默认首页地址

      http://appindex.domain

   b. 携带 state 传参：跳转到 state 解码 base64 后的绝对地址

      http://thirdaddr.domain

2. 已登录：

   a. 未携带 state 传参:跳转到平台应用默认回调地址带 code 参数

      https://平台回跳 url?code=xxxx-xxxx-xxxx

   b. 携带 state 传参：跳转到平台应用默认回调地址带 code 参数和 state 参数，需要根据 code 获取用户信息，base64 解码获取地址后平台应用内部跳转

      https://平台回跳 url?code=xxxx-xxxx-xxxx&state=base64（http://thirdaddr.domain）

⑥ 接口示例

表 15 接口示例

请求报文： http://ip:port/uias/app/view?client_id=***&state=base64 编码 （http://thirdaddr.domain）

- 具体 API 请参照《接口规范》。

4.2.3.9 第三方系统绑定用户信息采集接口

① 接口描述

枢纽平台采集第三方系统绑定用户信息接口。

② 接口鉴权方式

数据签名

③ 请求说明

表 16 请求说明

url	http://ip:port/data/collect/third/bindUserInfo
请求方式	Post
格式	Json
是否需要鉴权	是
请求数限制	是
接口方向	第三方系统>公共服务枢纽

④ 请求参数

a) 请求 head 参数：数据签名参数

参考《接口规范》4.3.2 数据签参数说明

参数	说明
Cc-Appid	应用 ID
Cc-Signature	数据加密签名。signature 计算结合了应用的 APPKEY、请求中的 timestamp、nonce,签名计算方法参考数据签名加密方法小节。
Cc-Timestamp	时间戳。与 nonce 结合使用，用于防止请求重放攻击。如：1573439583805。
Cc-Nonce	随机数。与 timestamp 结合使用，用于防止请求重放攻击。

b) 请求 Body 参数：

表 17 请求参数

序号	字段名	约束	类型	说明
1	access_token	必选	String	访问令牌（bindType 为绑定=1 时必传，解绑=2 时可选）
2	thirdUserId	必选	String	第三方系统唯一用户 ID
3	thirdAccount	可选	String	第三方系统用户账号
4	bindType	必选	String	绑定类型，1：绑定，2：解绑
5	smartEduCard	必选	String	智教中国通行证 ID（唯一标识），用于确定唯一的教育用户

⑤返回参数

表 1 返回参数

序号	字段名	约束	类型	说明

1	retCode	必选	String	返回码 000000:成功 200001:必选参数为空 100001:绑定失败 800001:用户会话票据失效
2	retDesc	必选	String	返回码描述
3	data	必选	String	返回数据

⑥接口示例

表 2 接口示例

■请求报文：


```
{
    "access_token": "9d82a9ca-*********-43887a73c2e2",
    "thirdAccount": "****",
    "thirdUserId": "******",
    "bindType": "1",
    "smartEduCard": "4508***58"
```


■应答报文：


```
{
  "data":
  "retCode": "000000",
  "retDesc": "请求成功",
  "success": true
}
```


- 具体 API 请参照《接口规范》。

5. 接入要求

5.1 登录要求

a) 要求第三方系统可使用智教中国通行证账号密码登录，类似使用微信登录平台的效果；

b) 各第三方系统个人中心需有国家通行证入口，未绑定的可以绑定，已绑定的可展示通行证信息；（可选）

c) 要求国家智慧教育平台登录后，实现可免登录到目标第三方系统：首次访问需绑定已有用户或者注册新用户，后续访问直接免登录；绑定用户请使用智教中国通行证 ID（唯一标识），用于确定唯一的教育用户。

d) 接入的第三方系统绑定自身用户成功后需按照开发规范 4.2.3.9 的接口上报用户账号绑定信息。

5.2 登出要求

a) 使用通行证登录到目标第三方系统，登出目标第三方系统时，需同步登出国家平台通行证；

b) 使用通行证登录到国家平台，免登录到目标第三方系统后，国家平台登出需同时登出目标第三方系统；目标第三方系统需提供登出链接或接口。（可选）

5.3 通行证补充注意事项

a) 绑定用户时请使用国家智慧教育平台用户通行证 ID 号进行绑定；

b) 同一个通行证 ID 号可对应多个用户身份，身份目前支持六种：学生、教师、家长、学校工作人员、教育部门人员、其他；每个身份归属不同的机构或者学校。

c) 接入的第三方系统系统用户账号支持多身份多机构的可自行适配国家通行证的信息；接入的第三方系统用户账号仅支持单身份单机构的，需在平台、应用侧支持多个用户账号绑定同一个通行证。

d) 国家公共服务枢纽是在国家服务体系基础上进行了升级，之前已在国家服务体系实名认证过的用户，如所填写的信息准确合规的，可直接使用手机号登录或者找回通行证的密码；对于未实名的或者信息填写不合规的用户需在国家智慧教育平台注册申请通行证。登录通行证后，可自行维护所属学校、用户身份、账号绑定的手机号、邮箱等信息。

6. 版本记录

表 100 版本记录

版本号	时间	记录人	变更原因	变更描述
V1.0	2022/06/12	国家智慧教育平台产品组	框架基线稿	新建
V1.1	2022/07/01	国家智慧教育平台产品组	修改平台认证章节	修改平台认证章节，支撑平台间互信互任对接

V1.2	2022/07/27	国家智慧教育平台产品组	1、修改开发规范，统一接入方式，新增接入要求，规范接入效果 2、刷新token，7天有效期	修改4.2章节，新增章节5接入要求