上海市宝山区未来宝教育基座
三方应用对接技术规范文档
（V1.6.4）

2024 年 5 月

目　录

一. 开发前必读

1. 开发须知

在使用数字基座开放平台的能力开发应用前，请注意：

1) 在使用数字基座开放平台进行能力开始时，应提前和上海市宝山区教育局联系，完成服务商入驻材料申请和审核，完成服务商入驻环节；
2) 服务商入驻流程结束后，可以在教育数字基座开放平台进行开发账号申请，申请审核完成，可进入数字基座开放平台进行应用开发；
3) 针对已经在钉钉平台上开发的三方应用，可联系上海市宝山区教育局（或教育数字基座项目组）进行应用迁移到教育数字基座开放平台上；
4) 接入数字基座的应用需要根据使用场景进行多端适配：
   a) 若应用涉及为上海市社会民众提供服务，需接入“随申办”服务端
   b) 若应用涉及为区县教育局/学校提供服务，需接入“数字基座组织”应用端
   c) 若应用以 Web 端方式为多用户/多组织提供服务，需满足“Web 端”接入规范
5) 接入数字基座的应用需要接入三大中心（组织中心、应用中心、数据中心）
   a) 组织中心：按照教育数字基座用户体系和规范，完成单点登录和统一认证；
   b) 应用中心：按照教育数字基座应用中心要求完成应用创建、接口申请、免登调测、应用上架、审核、下单及应用分发机制；
   c) 数据中心：按照教育数字基座的数据中心对接需求完成业务数据对接，须提供库表或 API 接口等方式进行业务数据的上报、校验及交换共享；
6) 若在开发时需要获取数字基座服务端 API，可联系上海市宝山区教育局（或教育数字基座项目组）获取开放接口列表；
7) 教育数字基座应用（H5 应用还是小程序），都必须接入数字基座免登接口，即在用户打开应用时可直接获取用户身份无需输入用户账号和密码；
8) 如果开发的是小程序应用，确保你已经在开放平台配置了小程序 HTTP 域名和开发人员。
9) 如果开发的是 H5 微应用，需要进行 JSAPI 鉴权

当前，教育数字基座应用技术接入规范以满足应用全流程贯通为主，关于更多的 API 能力开放和应用接入流程完善，将根据数字基座产品迭代持续进行更新！

2. 基础概念

在开发前，可通过如下内容了解数字基座开放平台基本概念：

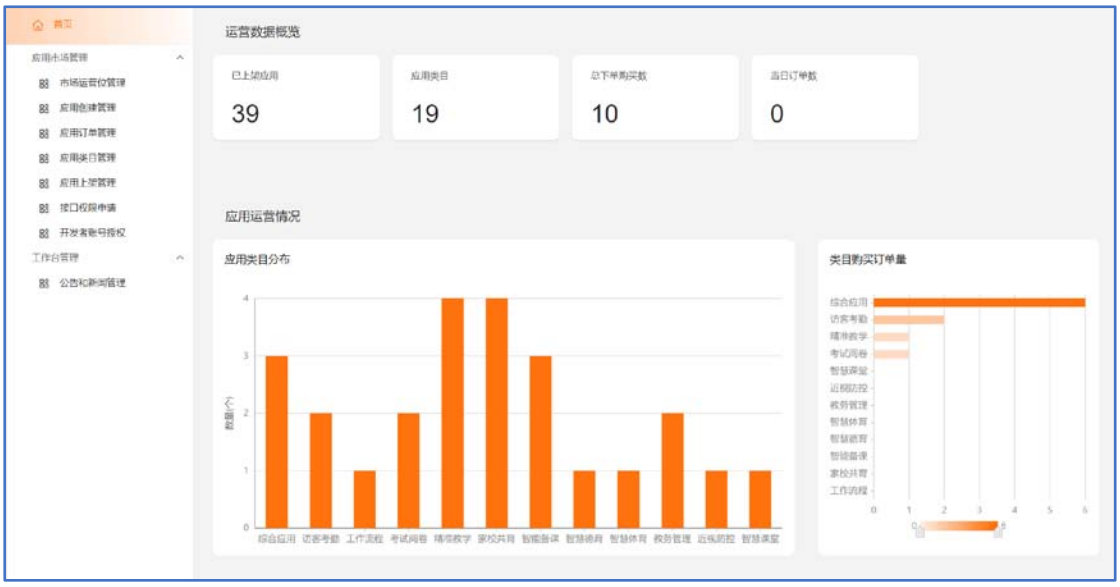
2.1. 运营服务平台

数字基座运营服务平台，主要是面向上海市宝山区教育局、数字基座运营主体、应用生态开发商等不同用户提供价值。其主要包括市场运营管理、开发者服务运营管理、运营数据监控：

其中，市场运营管理主要面向应用市场，提供各类流量运营的抓手和工具，包括向应用商提供流量运营和规则运营两大部分核心能力，提高运营效率；

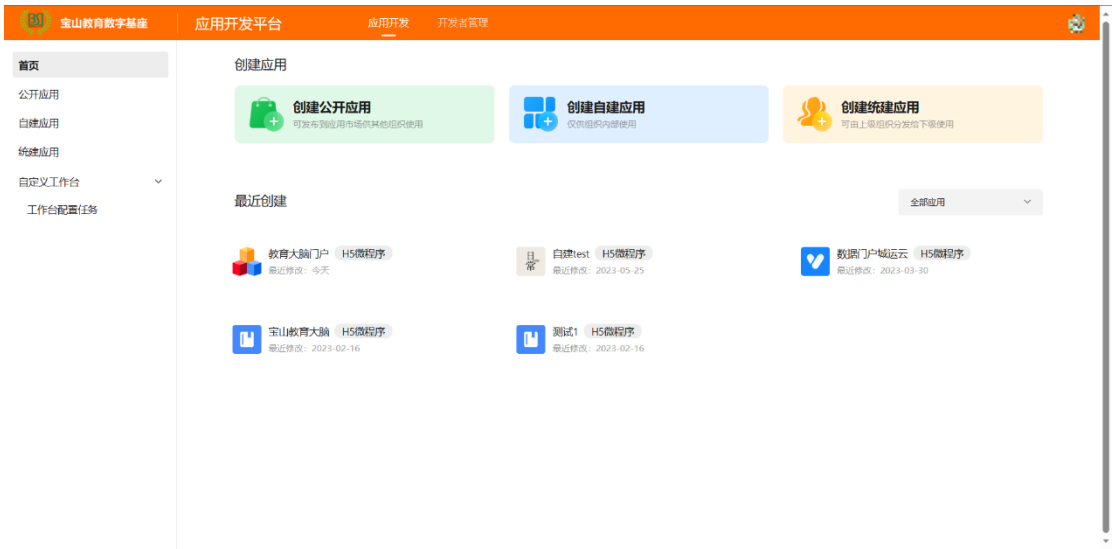
开发者服务运营管理主要面向开发者，以提供技术咨询服务为主，帮助开发者更好使用教育数字基座中枢能力，以满足多场景业务应用更好接入；

运营数据监控主要提供运营数据监控看板，包括采购量，安装量，打开次数，活跃次数等指标数据。



2.2. 开发者平台

数字基座开发者后台是管理应用开发的服务平台。开发者可以在提交完入驻信息后，进行数字基座服务商账号注册、配置应用信息、资源管理、服务调用接口，查看应用运行情况等功能。如下是数字基座应用开发平台效果图：



2.3. CorpId

CorpId 是企业在数字基座中的标识，每个企业拥有唯一的 CorpId。

登录数字基座开发者后台，在首页下查看企业的 CorpId。

2.4. UserId

用户在每个数字基座组织内都有唯一的 UserId，创建后不可修改。

登录数字基座管理后台，在通讯录页面单击用户姓名可查看用户的 UserId

2.5. UnionId

用户在当前开放平台账号范围内的唯一标识，同一个数字基座开放平台账号可以包含多个开放应用，同时也包含 ISV 的套件应用及企业应用。

可通过调用获取用户详情接口获取。

2.6. AppKey/AppSecret

AppKey 是数字基座企业内部应用的唯一身份标识，AppSecret 是对应的调用密钥。

在数字基座开发者后台创建企业内部应用后，系统会自动生成一对 AppKey 和 AppSecret。

登录数字基座开发者后台，在应用开发页面，单击已创建的应用，然后单击凭证与基础信息查看 AppKey 和 AppSecret。

如果企业内部应用授权给定制服务商开发，定制服务商需要根据 CustomKey 和 CustomSecret 获取授权。

2.7. SuiteKey/SuiteSecret

SuiteKey 是第三方企业应用的唯一身份标识，SuiteSecret 是对应的调用密钥。

在数字基座开发者后台创建第三方应用后，系统会自动生成一对 SuiteKey 和 SuiteSecret。

登录数字基座开发者后台，在应用开发页面，单击已创建的应用，然后单击凭证与基础信息查看 SuiteKey 和 SuiteSecret。

2.8. access_token

access_token 是企业后台通过数字基座接口获取信息的重要凭据。在调用数字基座接口时必须携带 access_token 用于验证接口的访问权限。

可通过调用 gettoken 接口获取 access_token。

2.9. AgentId

AgentId 是企业内部应用的唯一标识。在数字基座开发者后台创建应用后，系统会自动生成一个 AgentId。

登录数字基座开发者后台，在应用开发页面，单击已创建的应用，然后单击凭证与基础信息查看 AgentId。

3. 业务应用分类

教育数字基座以通过重构区域优质教育资源供给，培育可持续发展的教育应用新生态，形成“政府主导、市场参与、用户选择”的应用服务新机制，实现优质应用区级统建（或遴选），学校自主创新发展，按需购买的数字化运营新模式，最终构建“一校创新，全区受益”的数字化教育应用新格局。

当前应用服务商在接入教育数字基座前，可参考如下场景辅助进行业务判断：

3.1. 区域统建的公共服务应用

区域统建的公共服务应用，一般是由市级或区级统建，面向上海市内社会民众、管理者、各级各类学校和其他组织提供应用服务。

原则上，此类应用按照“市级统筹、区县解决”模式接入教育数字基座。其中，若应用涉及为上海市内人民群众提供服务，需要对接“随申办”适配改造；若应用设计为区县教育局、学校或其他教育组织提供服务，则需要接入“数字基座-应用端”进行适配改造。

同时，待建应用需要根据教育数字基座的三大中心进行相应的业务改造，详情如下所示：

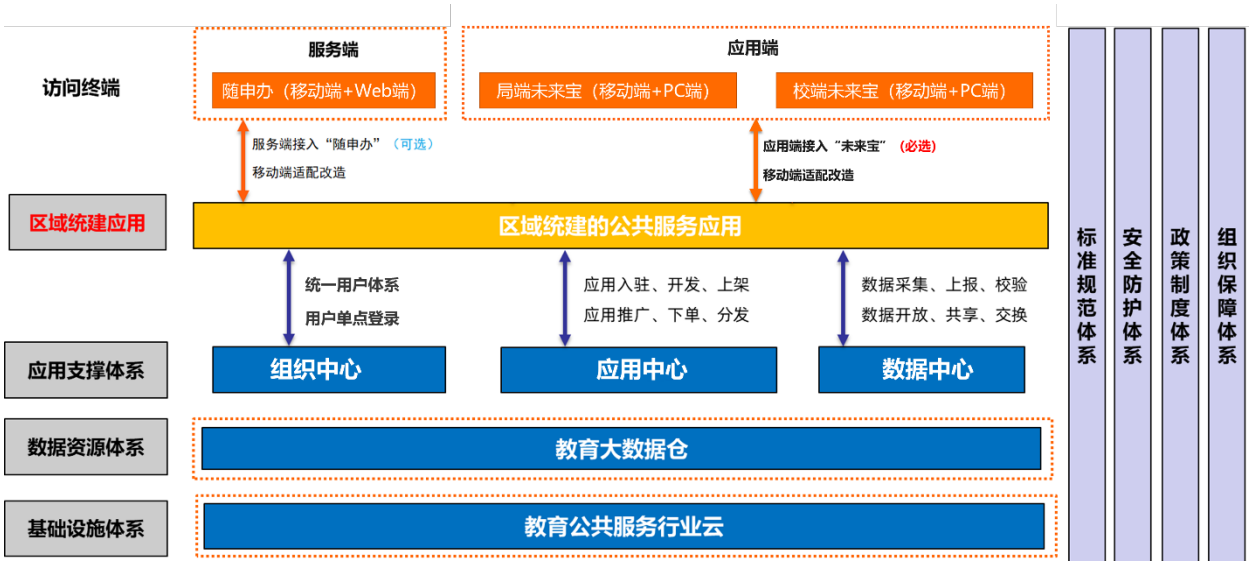


图. 区域统建应用服务接入技术框架图

3.2. 校园数字应用

校园数字应用，一般由区域（或学校）自建或生态厂商开发，主要是服务学校教师、学生、家长和管理者的独立数字化校园应用。如下所示，以学籍管理平台（招生应用）接入为例，其校园应用核心需接入校园端进行 PC 端和移动端接入适配改造。

应用端（校园端）—学生录取信息核对　　应用端（校园端）—发送录取通知　　应用端（校园端）—查询录取状态

图. 校园数字应用接入效果图

原则上，数字校园应用接入教育数字基座主要围绕数字基座应用端（即，区县教育局和学校应用端）的适配改造。其中，如果数字校园应用涉及到为社会家长提供教育公共服务，则需要同步进行适配接入“随申办”服务端。

同时，校园数字应用服务需要接入教育数字基座的三大中心（即组织中心、应用中心、数据中心）体系，详情如下图所示：

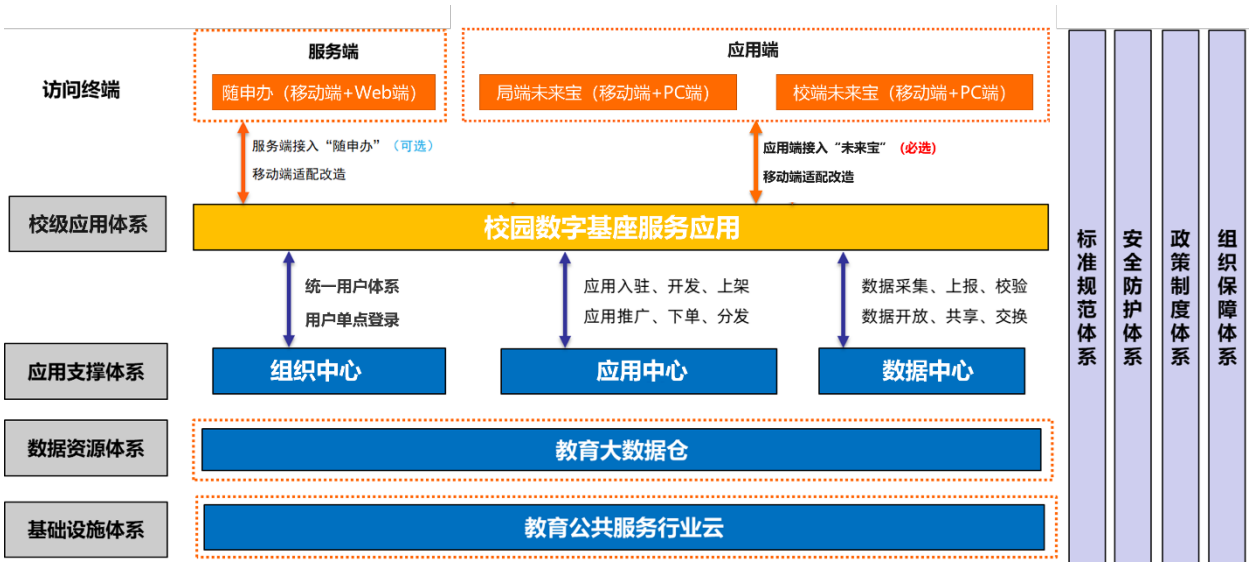


图. 校园数字应用接入技术框架图

3.3. 个人工作应用

个人工作应用，一般由区域自建或生态开发，用于服务老师或教职工可独立使用的工作，如备课工具、资源平台、在线公开课等。

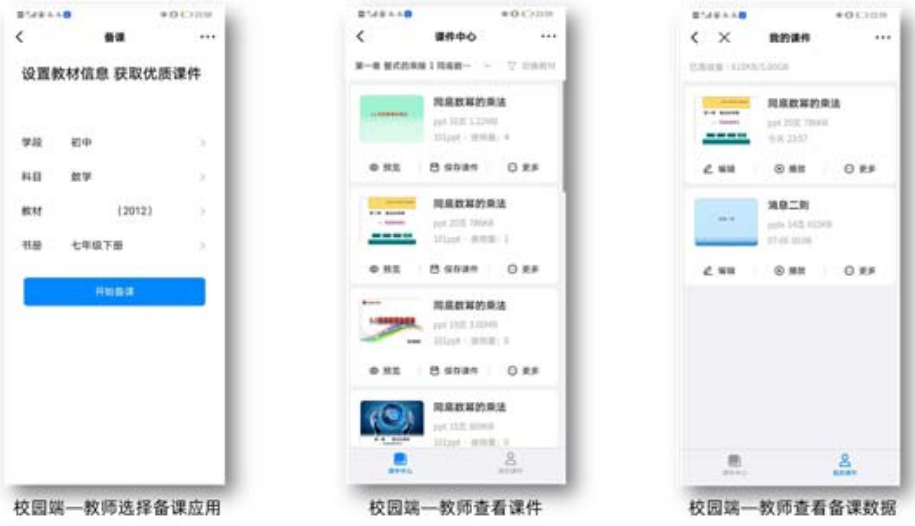


图. 个人工作应用接入效果图

个人工作应用，以满足区县/学校特定用户使用为主，原则上只需对应用端（区县/校园端）进行改造，无需接入服务端。

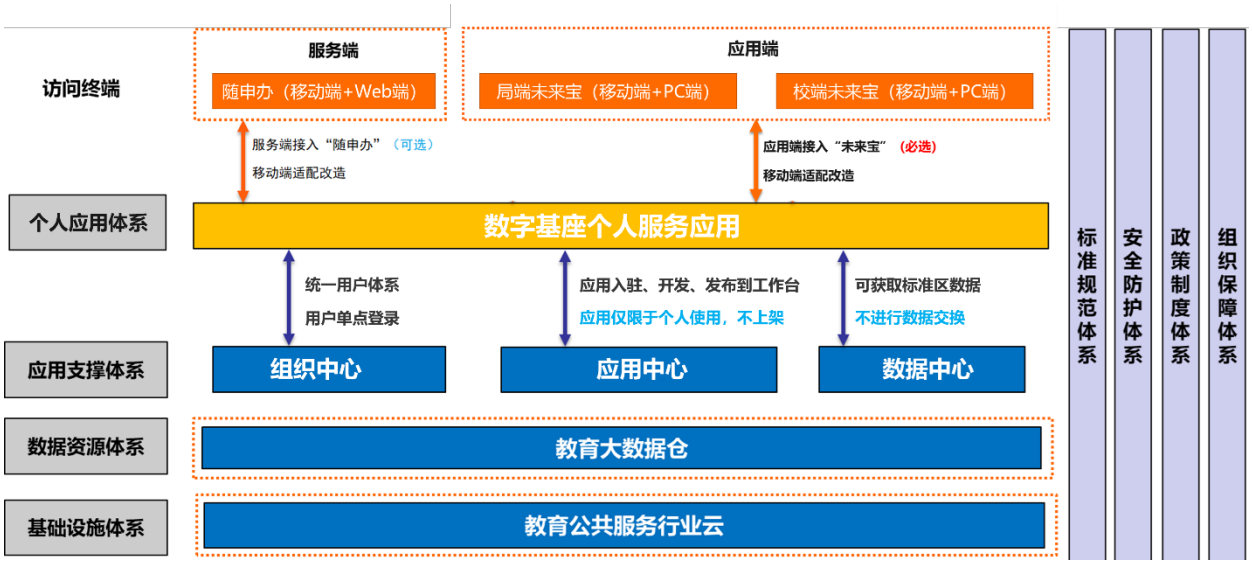


图. 个人工作应用接入技术框架

3.4. 行政部门内部应用

由政府内部自建或生态开发，服务政府管理者、各科室人员的政府服务类内部应用。

4. 应用类型介绍

基于上述业务应用类型所属，接入教育数字基座的应用分为：数字基座市统建应用、数字基座区域统建应用、数字基座公开应用、数字基座自建应用、Web 端应用。其详情如下所示：

应用类型	开发者	使用人员	支持能力
数字基座市统建应用	市教委批准的应用服务商	全市所有教育人员	小程序 H5 微应用
数字基座区域统建应用	区域教育局批准的应用服务商	区域内的所有教育人员	小程序 H5 微应用
数字基座公开应用	应用服务商	购买开通该三方应用的组织内部人员	小程序 H5 微应用
数字基座自建应用	组织内开发者 定制服务商	安装了该应用的组织内部人员	小程序 H5 微应用 机器人
Web 端接入应用	应用服务商 定制服务商 组织内开发者	使用“上海市宝山区教育局”相关应用的目标用户	教育局官网接入流程 数字基座单点登录

其中，数字基座市统建应用和区域统建应用，主要是全市或市区统一建设，需要全区域统一使用的应用系统，通过数字基座工作台直接下发到区域内所有学校；

数字基座公开应用和数字基座自建应用，主要是三方生态应用进行适配改造（或开发）接入教育数字基座的应用端（区县教育局/学校应用）；

Web 端应用接入，主要是针对原先接入“上海市宝山区教育局”官网的应用系统，如教师培训管理平台，则需要支持在数字基座-应用端（PC）支持统一入口集成、单点登录跳转等业务改造，同时还需要支持在原 Web 端应用登录使用与数字基座打通（至少接入数字基座单点登录）。

5. 入驻成为数字基座开发者

为了更好的提高与生态伙伴的合作效率，保障客户服务和体验，提升生态组织的管理规范性，对于教育数字基座生态合作服务商准入资质与流程做出如下要求。本要求适用于所有的教育数字基座生态合作服务商：

5.1. 企业基本资质要求

1）在中国境内注册，具有独立法人资格的合法企业；相应的经营范围，具有独立承担民事责任的能力；（提供合法有效的营业执照原件复印件，原件备查）

2）企业应具备《中国人民共和国政府采购法》第二十二条规定的条件；

3）企业工商注册经营范围必须包含该项目的服务内容；

4）为保障售后服务的及时性，企业应在上海市注册或在上海市设有长期稳定的办公场所；

5）具有良好的商业信誉和健全的财务会计制度，没有处于被责令停业、财产被接管、冻结、破产状态；

6）具有依法缴纳税收和社会保障资金的良好记录，参与本次项目前三年内，在经营活

动中没有重大违法记录。

5.2. 企业服务内容要求

1）业务范围：综合运用人工智能、大数据、云计算、物联网、虚拟仿真等信息技术，围绕“教、学、考、评、管”等教育领域重点环节，探索典型应用场景，具备推动相关技术、产品、方案等加快成熟的能力。

2）团队组成：企业应具有专门稳定的管理架构，至少包含产品设计、产品研发、系统运维、产品运维、项目管理等部门；企业在专业技术、人员组织、行业经验等方面具有部署、服务、经营管理的相应资格和能力，具有履行合同所必须的能力。

3）培训能力：企业应具有丰富的用户培训经验及系统的培训方法。在上海市具有完备的售后服务体系、业务支持等，以保证服务质量。

5.3. 企业技术背景要求

1）已完成国家信息安全等级保护三级认证，（提供等保三级备案证复印件加盖鲜章）；

2）企业在中华人民共和国境内提供非经营性互联网信息服务，应当依法履行备案手续，并取得国家机关单位许可备案（ICP 备案）（提供复印件加盖鲜章）；

3）已完成教育移动应用（app）备案（提供复印件加盖鲜章）；

4）已完成 ISO27001（信息安全管理体系）认证（提供复印件加盖鲜章）；

5）已完成 ISO20000(信息技术服务管理体系)认证（提供复印件加盖鲜章）。

二. 组织和账号创建

说明：仅针对尚未在未来宝创建过组织或团队的生态厂家，已经创建过组织或团队，不需要此步骤，可跳过。

1. 下载安装未来宝客户端

http://218.80.196.215:5000/appIssue/download?appId=37

2. PC 端创建组织，打开下方地址

https://oa.dingtalk.com/register_new.htm?lwfrom=2019111111293522001&source=CreateTeamPC_New#/

3. 手机端创建团队

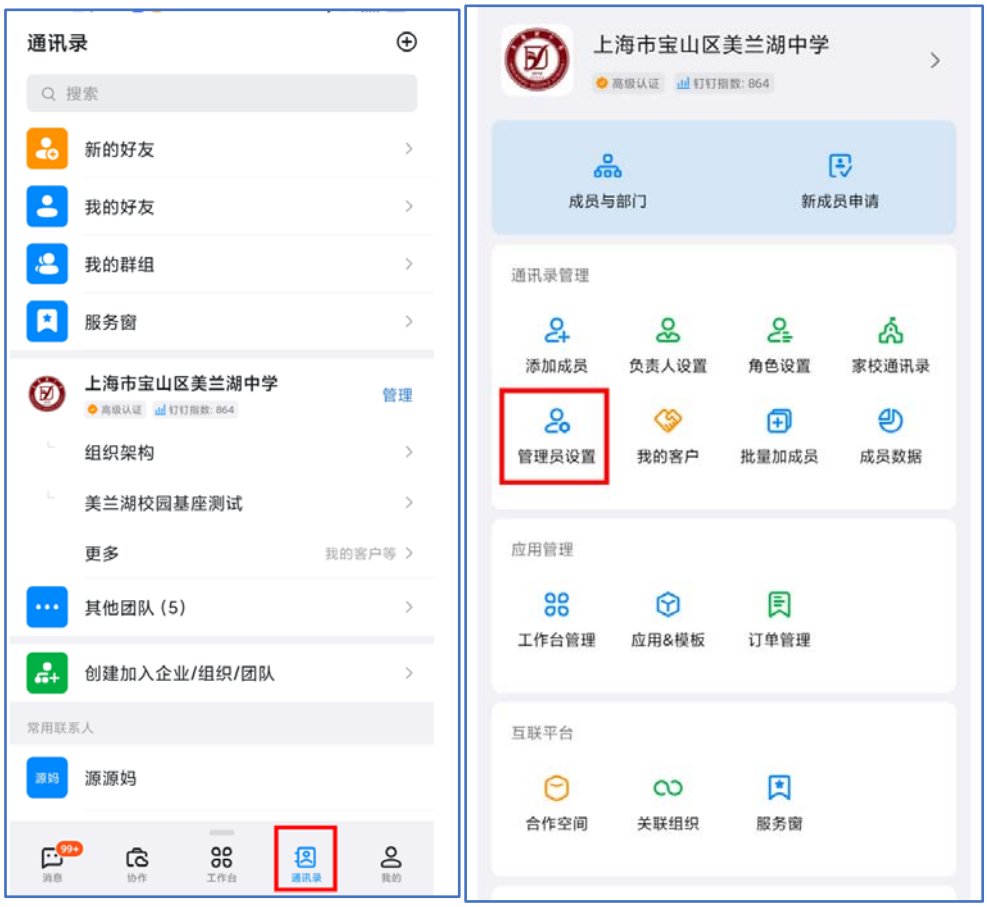
（1）手机端登录未来宝 APP 之后，找到【通讯录】

（2）弹出的界面中选择创建团队

（3）在弹出的页面中填写相关信息后，点击创建即可

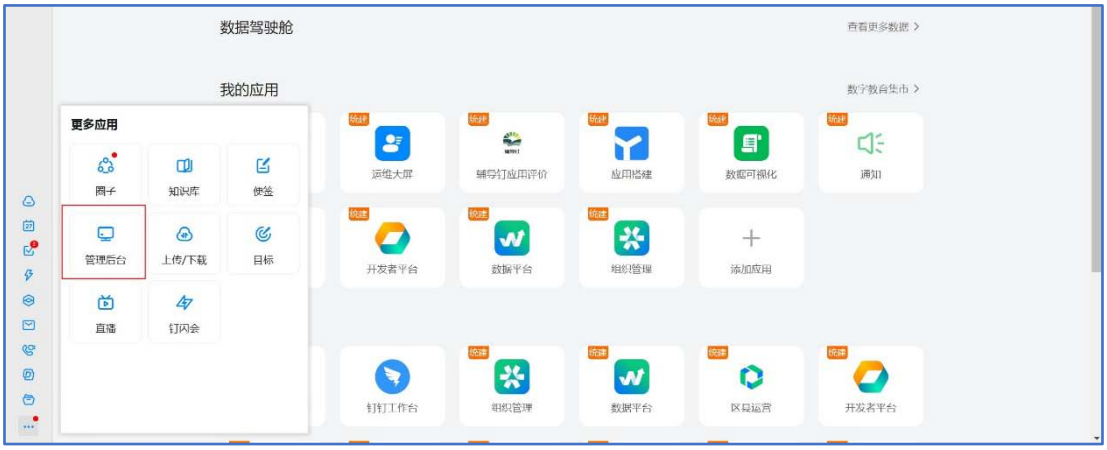
4. 设置组织管理员（用创建团队/组织的账号操作）

（1）手机端登录未来宝 APP，点击通讯录，然后在需要设置管理员的团队上点击管理，打开管理界面，即可看到管理员设置选项，点击进入设置主管理员和子管理员。



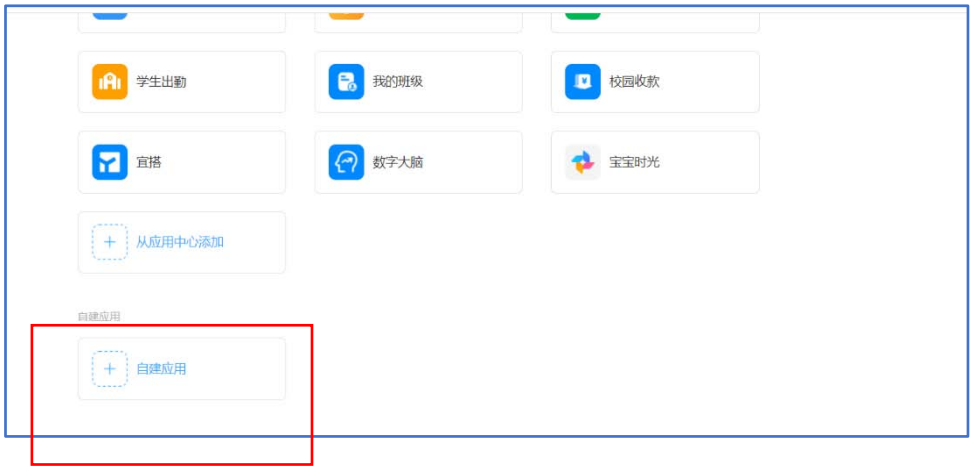
5. 查询 corpid（需要用管理员身份进入）

（1）在 PC 端客户端左下方，找到三个点，点击之后可以看到后台管理选项。



（2）然后在打开的界面中找到工作台选项。

（3）下拉到最下端，点击自建应用



（4）在打开的页面的右上方可以查看到所属组织的 CorpId，

备注：可以提前复制这个 corpid，后面注册开发者会用到

6. 账号创建

（1）由组织管理员创建账号，组织管理员登录 PC 端之后，点击左下方的【…】，选择管理后台，在通讯录模块增加账号。

（2）由开发者自己创建账号，在 PC 客户端注册或在手机端注册。注册完毕后再加入对应的组织，加入组织操作建议使用手机端操作。

PC 端注册账号入口如上图所示，点击后按照页面提示完成账号注册

手机端注册账号位置如上图所示，点击后按照页面提示完成账号注册

手机端加入组织（团队）的入口在通讯录模块的右上方，如上图所示

选择加入类型界面如上图所示

输入关键词可以进行搜索匹配，如上图所示，选择需要加入的组织，等待学校/组织管理员审核就可以了。

三. 开发者账号登录

1. 开发者平台登录地址

https://digitalbase.edu-aliyun.com/render/web/open/#/login

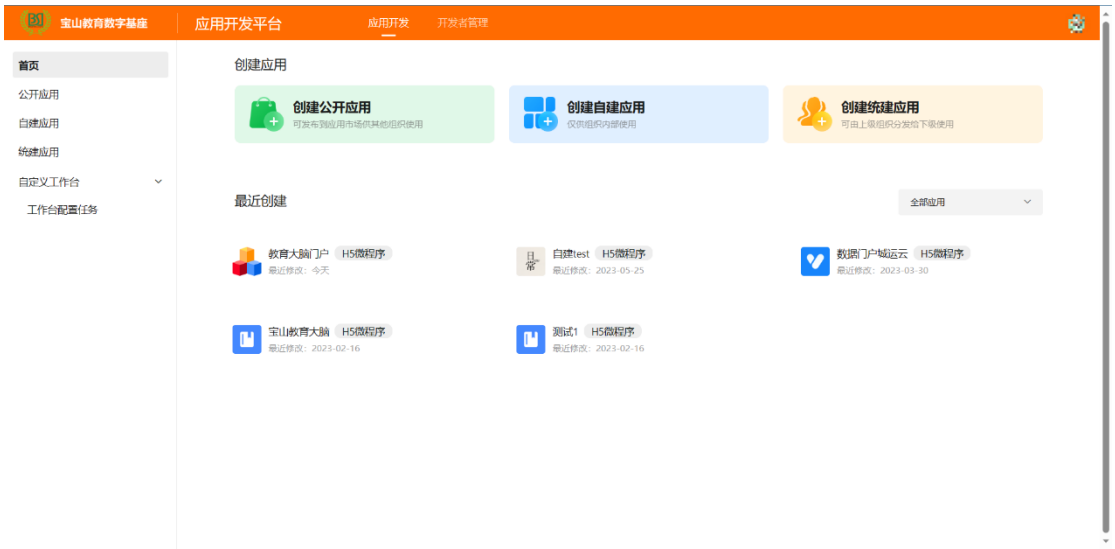
2. 开发者账号登录

（1）进入未来宝教育基座开发者登录页面后，选择钉钉账号登录

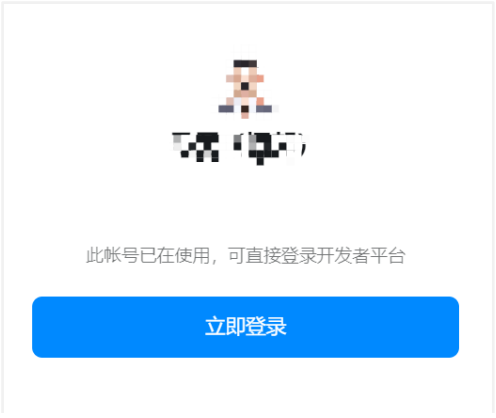
（2）弹出对应登录框时，使用开发者之前创建的未来宝账号登陆即可，如果开发者已经在手机端登录了未来宝，则可以选择二维码的方式来登录（使用未来宝手机客户端扫码登录）。

（3）在完成账号密码登录后，会弹出一个组织列表（当前开发者账号加入过的所有组织都会罗列出来），请选择本次应用创建或应用维护所属的组织，比如是帮助学校创建或维护应用则选择对应的学校（前提是学校已经把开发者加入到学校组织）。

（4）选择完组织后就进入开发者平台。



（5）在第（1）步选择 App 账号登录之后，如果开发者的账号在短期内已经登录过开发者平台，则会记录开发者的登录状态，弹出如下提示，直接点击立即登录即可。



（6）如果上一步所选的组织没有开通基座开发者功能，则会弹出如下图所示二维码，需要对应的组织管理员（**注意：这里的组织管理员指的是上一步选择的组织下的管理员）扫码安装到学校**。

如果该管理员账号下对应多个组织（假设存在同一个用户多个学校任职的情况），扫码安装

过程中，务必选择上一步开发者登录时所选择的组织。

四. 开发数字基座应用

教育数字基座服务商在入驻成功之后，可进行数字基座三方应用开发或者应用接入。

1. 数字基座自建应用开发

1.1. 应用说明

数字基座自建应用是组织基于教育数字基座平台的开放能力，开发个性化的教育相关应用供本组织内部使用。自建应用发布后，组织内部用户可以直接从工作台中打开使用该应用。

类型	开发者	使用者	支持的应用类型
数字基座自建应用	组织内部开发者	安装了该应用的组织内部人员	小程序、H5 微程序

1.2. 应用创建

1.2.1. 登录（注册）数字基座开发者平台

进入数字基座开发者平台登录界面，用未来宝 App 扫码确认即可登陆，若首次登陆，需要填写注册信息，需要填写：姓名、手机号、所在公司、账号昵称。

1.2.2. 新建应用

首次登录开发平台后，在首页中，点击【创建自建应用】，开始新建自建应用，或点击自建应用目录，在「自建应用」页面，点击【创建应用】。

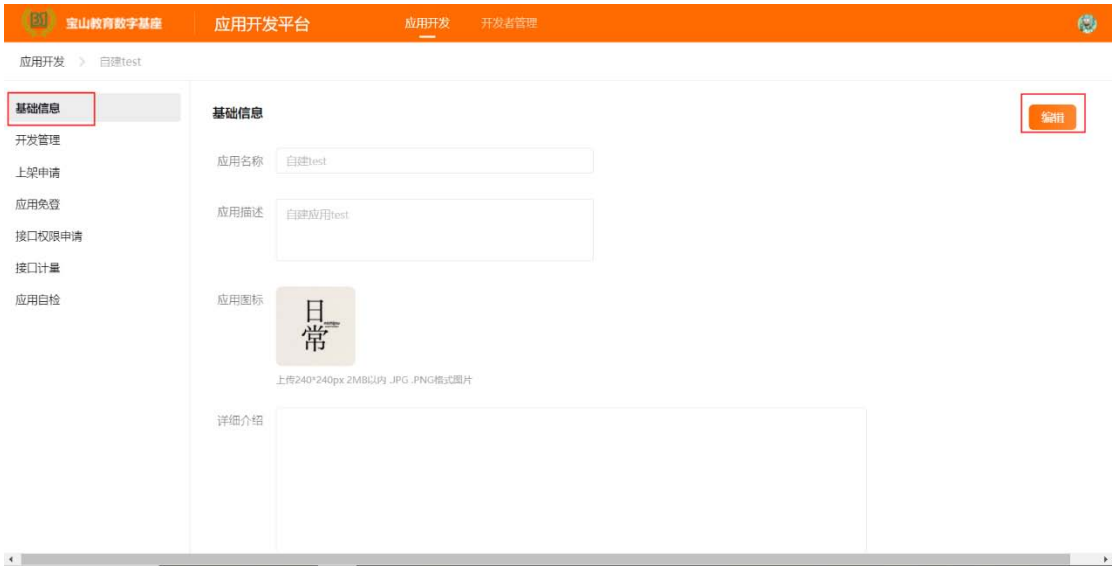
在出现的弹窗中，按照要求填写信息。

填写说明：应用名称最多 20 个字符；应用描述最多 250 个字符；应用图标：240*240px 率以上，1:1，120Kb 以内，无圆角 JPG/NPG 格式图标。

创建完成后，即可看到新创建的自建应用

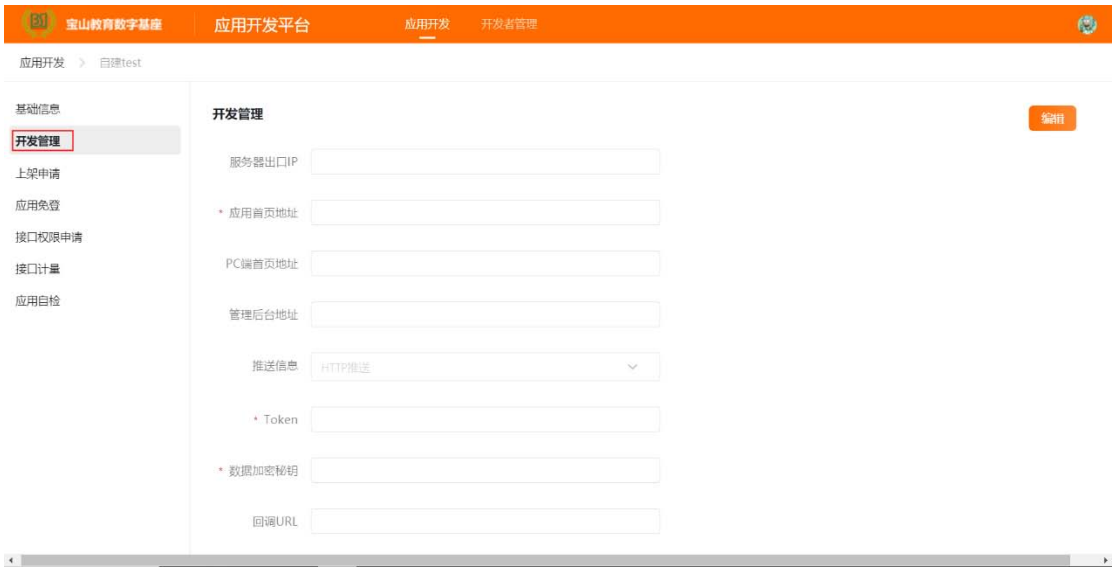
1.2.3. 应用配置

待平台运营人员审核通过后，应用凭证信息自动生成（SuiteId、AppId、SuiteKey、SuiteSecret）。点击【编辑】可以修改应用的应用名称、应用描述、应用图标。



1.3. 应用开发与部署

1.3.1. 开发管理配置



服务器出口 IP（必填）：调用数字基座服务端 API 时的合法 IP 列表，多个 IP 时请用“,”逗号隔开。支持带一个*通配符的 IP 格式。

应用首页地址（必填）：输入 http 或 https 开头的网址链接。

PC 首页地址：用户可以在 PC 端数字基座工作台上打开这个应用并显示这个链接的内容，请输入 http 或 https 开头的链接。

管理后台地址：组织管理员可以在数字基座运营工作台打开这个应用并进行管理，请输入 http 或 https 开头的链接。

推送信息：请选择【HTTP 推送】。

Token（必填）：由开发者自己制定。制定规则：必须为英文或数字，长度为 3~32 个字符。用于生成签名、校验回调请求的合法性。本应用下相关应用产生的回调消息都使用该值来解密。

数据加密秘钥（必填）：可自动生成。回调消息加解密参数，是 AES 密钥的 Base64 编码，用于解密回调消息内容对应的密文。本应用下相关应用产生的回调消息都使用该值来解密。

回调 URL：填写的 URL 要准确，可通过验证有效性按钮测试回调 URL 是否能够正常使用。在应用开通授权等事件的时候，服务器端需要通过该地址向 ISV 的服务器推送数据。

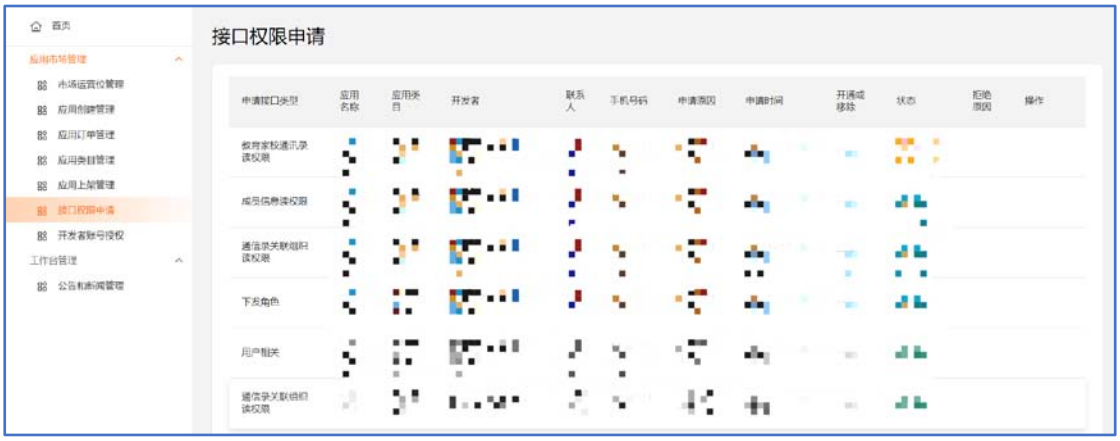
1.3.2. 应用免登

数字基座平台提供了免登录机制，只需提供应用自身的中间跳转页的 URL 即可。

1.3.3. 接口权限申请

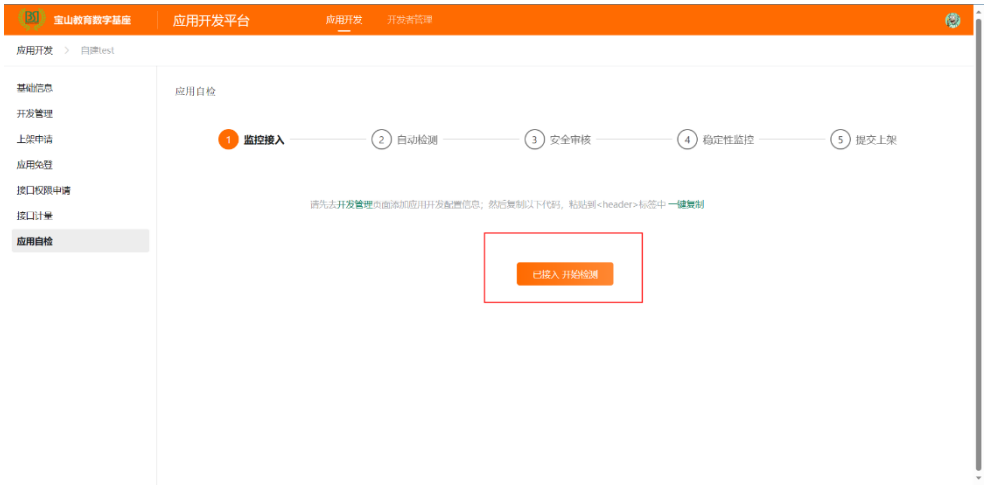
点击【申请权限】，在「申请权限」的弹窗中，按照要求填写信息。提交信息后，等待运营人员审批。支持接口权限进行批量申请或单个申请。

运营人员在教育数字基座的「运营平台」主页中，点击【接口权限申请】，对申请进行同意或拒绝操作。



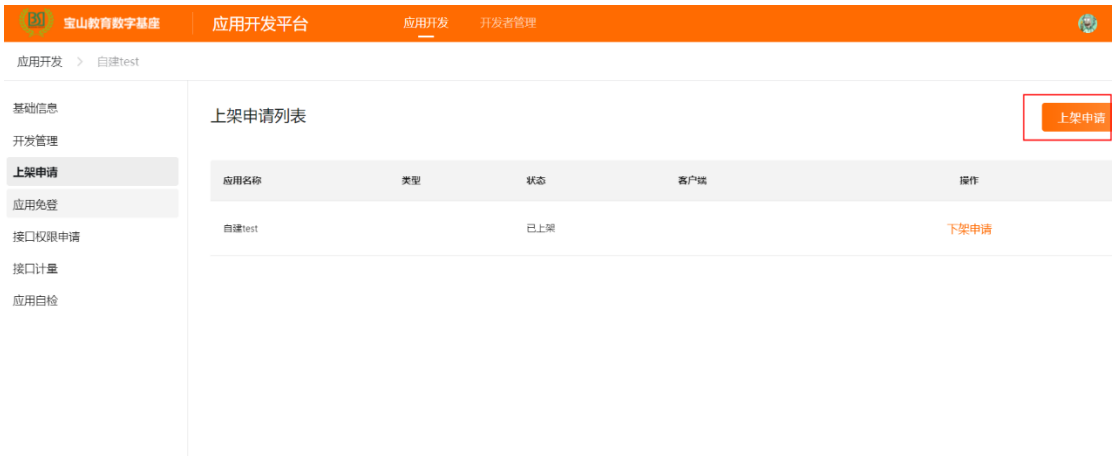
1.3.4. 应用自检

点击【已接入 开始检查】进行「自动检测」，完成 7 项所标注的项目后，则可进行下一步「安全审核」。而后根据操作步骤及信息提示完成「稳定性监控」，则可提交上架应用。



1.3.5. 应用上架

在应用开发选择应用上架，点击右上角的上架申请，在出现的弹窗中点击上架即可。



2. 数字基座公开应用开发

2.1. 应用开发说明

数字基座公开应用是由应用服务商开发的第三方数字基座教育应用，可以通过上架到数字基座应用市场售卖给数字基座的组织使用，也可以通过服务商在开发者后台创建应用分发项目进行线下应用分发给组织使用。是能够实现开发一个应用，授权分发给不同的组织使用的应用类型。

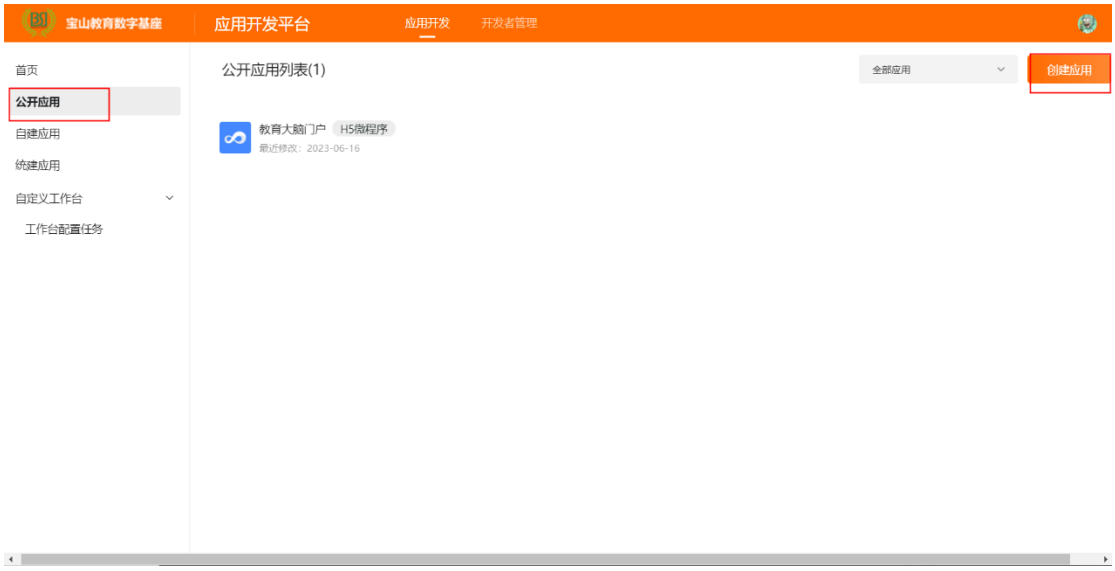
如果数字基座公开应用在数字基座应用市场展示，组织管理员可以在数字基座应用市场上搜索，找到需要的数字基座公开应用，开通后让组织内的用户使用。

	开发者	使用者	支持的应用类型
数字基座公开应用	应用服务商开发者	开通公开应用的用户	小程序、H5 微程序

2.2. 创建应用

在登陆数字基座开发平台后，在首页点击【创建公开应用】，或者在公开应用管理目

录页面点击【创建应用】。



在弹窗中，按照要求填写信息。创建完成后，应用凭证信息自动生成（SuiteId、AppId、SuiteKey、SuiteSecret、AppCode）。

填写说明：应用名称最多 15 个字符；应用描述最多 120 个字符；应用图标：JPG/NPG 格式图标，宽高比为 1:1，240px*240px 以上，2MB 以内。

2.3. 开发管理

2.3.1. 开发概述

和数字基座自建应用开发相同，数字基座公开应用开发也支持小程序和 H5 微应用，但公开应用还需要进行应用授权等开发。

开发流程：1.调用服务端接口，进行业务集成。2.注册回调。3.授权应用开通。4.数字基座公开应用必须接入未来宝免登、通讯录和工作通知能力。5.前端开发

2.3.2. 基础配置

在创建公开应用后，需要完成基础配置。

服务器出口 IP（必填）：调用教育数字基座服务端 API 时的合法 IP 列表，多个 IP 时请用“,”逗号隔开。支持带一个*通配符的 IP 格式。

应用首页地址（必填）：输入 http 或 https 开头的网址链接，如：https://www.dingtalk.com。

PC 首页地址：用户可以在 PC 端教育数字基座工作台上打开这个应用并显示这个链接的内容，请输入输入 http 或 https 开头的链接。

管理后台地址：组织管理员可以在教育数字基座运营工作台打开这个应用并进行管理，请输入输入 http 或 https 开头的链接。

推送信息：请选择【HTTP 推送】。

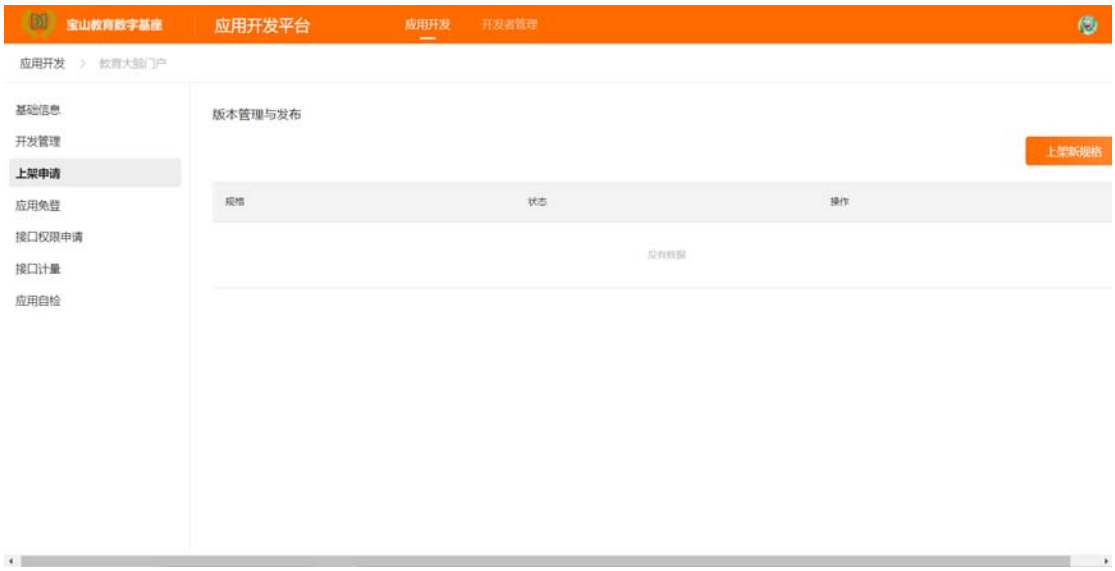
Token（必填）：由开发者自己制定。制定规则：必须为英文或数字，长度为 3~32 个字符。用于生成签名、校验回调请求的合法性。本应用下相关应用产生的回调消息都使用该值来解密。

数据加密秘钥（必填）：可自动生成。回调消息加解密参数，是 AES 密钥的 Base64 编码，用于解密回调消息内容对应的密文。本应用下相关应用产生的回调消息都使用该值来解密。

回调 URL：填写的 URL 要准确，可通过验证有效性按钮测试回调 URL 是否能够正常使用。在应用开通授权等事件的时候，服务器端需要通过该地址向 ISV 的服务器推送数据。

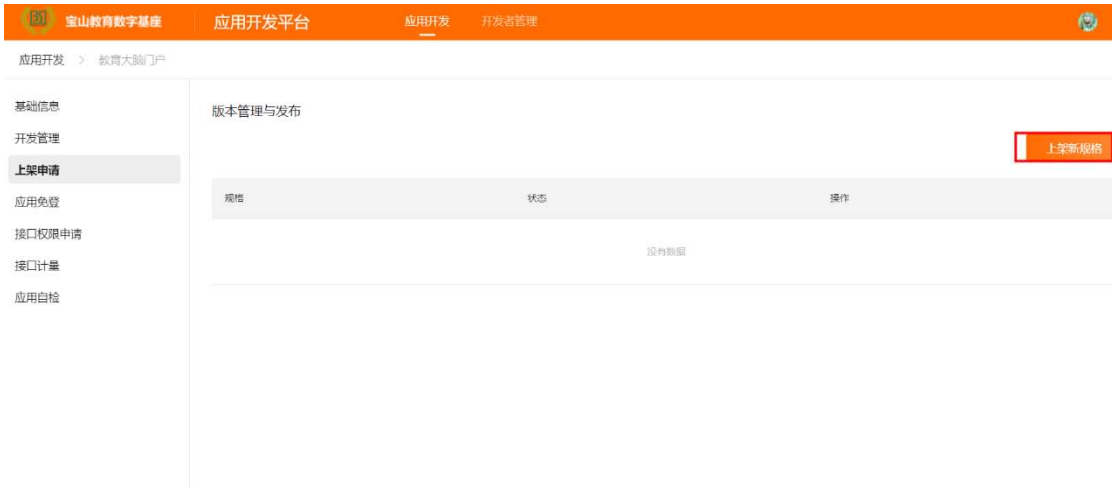
2.4. 版本管理与发布

进入数字基座公开应用后，点击左侧【应用上架】（图 4-12），即可查看此应用的版本。公开应用通过版本的发布和上架，能够实现在应用市场上的展示和售卖。



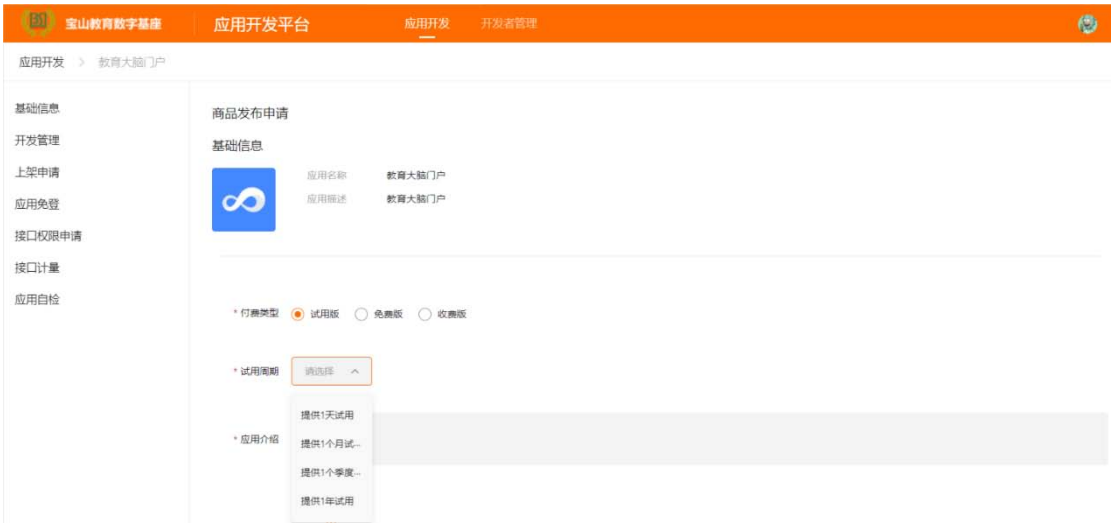
2.4.1. 关于版本的说明

一个应用通过发布版本的方式对外输出应用服务，一个应用可以有多个版本。
发布者通过对版本的发布，从而高效便捷的发布应用。
新建的公开应用没有任何版本，此时需要新建规格：

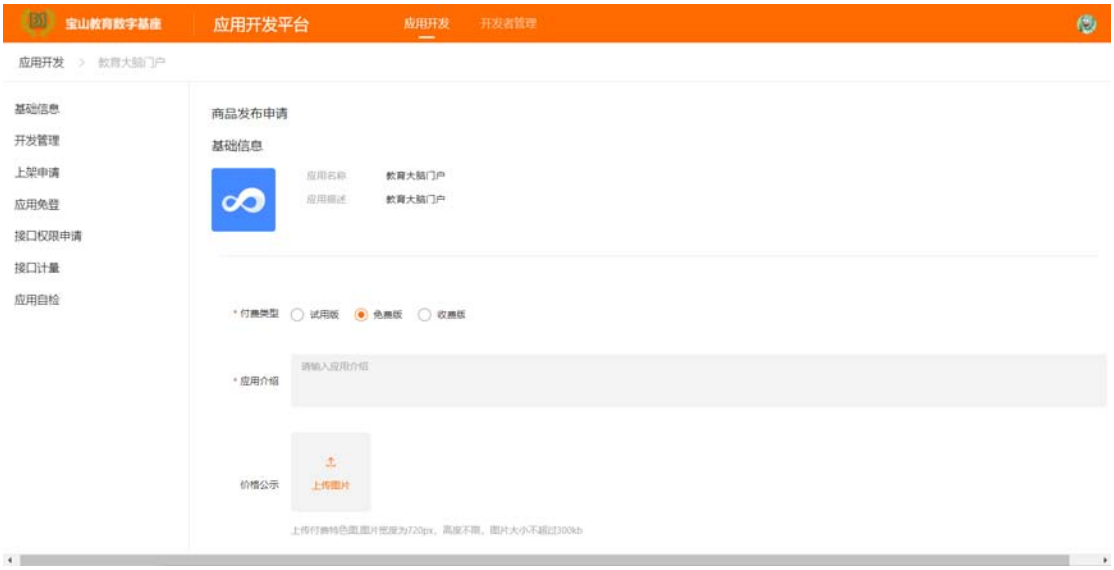


2.4.2. 商品发布申请

填写说明：应用介绍最多 250 个字符；价格公示：宽 720px，长度不限，图片大小 300Kb 以内，JPG/NPG 格式图标。
付费类型：对公开应用进行付费设置，收费方式有 3 种：试用版、免费版、收费版。
试用版：提供了四种试用周期（1 天、1 个月、1 个季度、1 年）

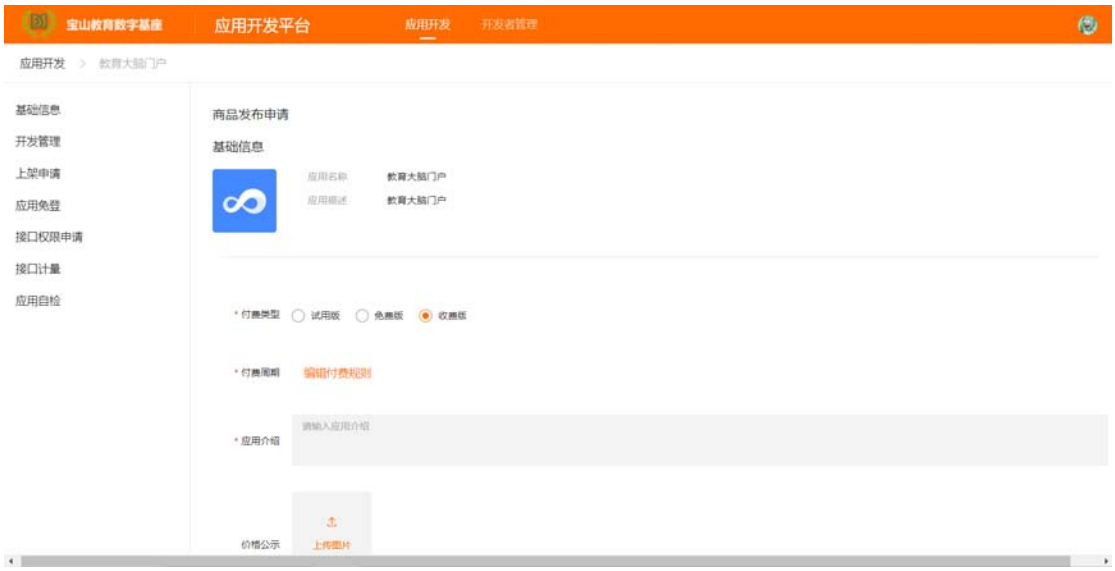


免费版

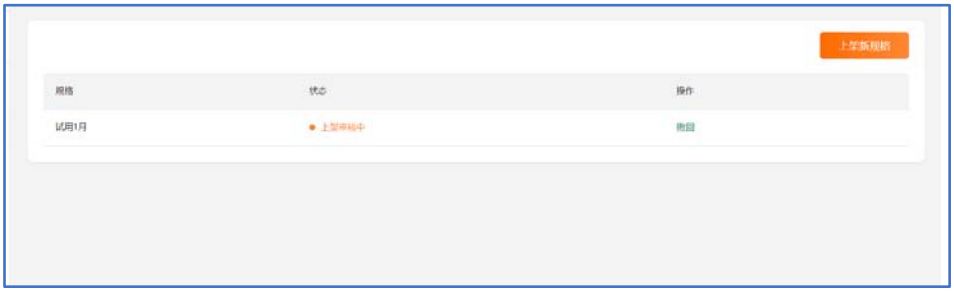


收费版

新建的应用默认是没有付费规则的，需要手动编辑。



提交保存后即可看到对应的版本已处于「上架待审核」状态。待平台运营人员审核通过后，版本立即上架。上架后也可以随时申请下架。



2.4.3. 配置收费规则

新的应用默认是没有付费规则的，需要手动添加几个收费规则

添加一行后，点击保存，保存后可随时删除

2.5. 应用免登

免登开发：平台提供了免登录机制。只要提供应用自身的中间跳转页的 URL 即可。

2.6. 接口权限申请与应用自检

操作方式与自建应用的接口权限申请一致。
操作方式与自建应用的应用自检一致。

2.7. 三方应用上架安全规范

三方应用上架，应完成网络安全等级保护定级，确定安全保护等级，并承诺正式对外服务前（或上架后不少于 6 个月内）落实等保测评和整改；应用上架前应委托第三方具有安全服务资质的机构开展一次安全评估关提交安全测试报告及整改报告（以 PDF 格式提交）。

2.7.1. 安全要求

1) 上架应用必须配置并使用 SSL 协议，并且代码和提供的服务中也都使用 https 协议。
2) 上架应用必须使用教育数字基座用户体系，使用提供的随申办免登接口获取用户身份信息，禁止自建登录体系。
3) 上架应用所有接口都需要结合有效 session 值进行用户身份鉴定，避免出现未授权访问及其他权限溢出的情况。
4) 如有存储用户文件的场景，为保证数据安全及稳定性，禁止文件存储在 ECS 服务器上，需使用对象存储 OSS 存储数据。
5) 系统使用所有第三方组件必须为最新无已知公开漏洞版本。
6) 每月应安排专人开展不少于 1 次日志分析，主要分析系统访问、用户登录、用户操作等日志是否存在异常，并确保各类日志存储不少于 6 个月。
7) 对发现的应用安全漏洞应在 3 天内完成修复（特别紧急的漏洞应在当天完成），操作系统、数据库、中间件等应根据原厂商公布情况或监管部门预警要求及时更新。
8) 根据网信、公安及上级主管部门要求，落实人员做好重要时期网络安全值守，重点监测并防范网络攻击、应用信息内容安全等。

2.7.2. 测试工具

1) 抓包改包工具

Tools: Burp Suite
Editions: Community
Download: https://portswigger.net/burp/
或 Charles、Fiddler

2) 端口扫描工具:

Tools: NmapDownload:
Windows: https://nmap.org/book/inst-windows.html
MAC: https://nmap.org/book/inst-macosx.html

2.7.3. 测试用例

1) 上架应用应参考“**测试用例**”完成应用安全测试，并根据“**附录 1 测试报告模板**”输出应用安全测试报告。
2) 对于测试用例当中的非漏洞测试项（NO.01 至 NO.04），必须提供测试内容。
3) 对于测试用例当中的漏洞测试项（NO.05 至 NO.09），如无法提供可由三个月内漏洞扫描报告代替。

编号	测试名称	使用工具	测试过程	测试结果	修复方案
NO.01	开发信息	人工	review 代码及环境，确定开发语言、开发框架、数据库类型、连接数据库框架、域名和 IP	例如：开发语言：java jdk1.7 开发框架：spring 数据库类型：Mysql 连接数据库框架：mybatis 域名：xxx.xxx.com IP：111.111.111.111	\
NO.02	数据库信息	人工	查看生产数据库数据库表结构	附数据库表、字段结构信息	禁止存储用户的敏感信息，包括但不限于身份证号码、银行卡号
NO.03	域名/IP 对外开放端口信息	nmap	nmap 使用命令：nmap -sV -T4 -Pn -p1-65535 ip	附端口扫描结果截图，需要能看出来被扫描的 IP 和扫描结果。	对外只允许开启 22、80 和 443 端口
NO.04	敏感信息	人工和抓包工具	review 代码及环境。1. 是否存在接口返回或展示用户较敏感信息 3. 服务端业务日志是否打印或存储敏感信息	1. 敏感信息已打码处理 2. 没有打印或存储敏感信息	1. 返回或展示较敏感信息(例如手机号、邮箱)需进行打码处理 2. 服务端业务日志不允许

编号	测试名称	使用工具	测试过程	测试结果	修复方案
					打印或存储敏感信息
NO.05	越权漏洞	抓包工具	修改请求 URL 参数中的 ID 类参数	1. 使用 A 用户身份,通过修改请求参数的方式，无法获取其他用户数据 2. 使用普通用户身份，无法通过访问管理员类接口的方式获取数据或者进行修改类操作。	做好权限校验。校验用户身份禁止通过取参数的内容方式进行判断。
NO.06	跨站漏洞	人工	在用户可以输入的地方，输入 js 代码 '"><img src=x onerror=alert(1)>	用户输入的 js 代码在展示页面未执行	对于用户输入的内容做好过滤。
NO.07	SQL 注入漏洞	人工和抓包工具	修改请求中用于查询类的参数	程序未执行参数中的 sql 语句	禁止拼接 sql 语句，需要使用预编译模式进行数据库操作
NO.08	CSRF 漏洞	人工或抓包工具	修改增删修改类请求接口中的 referer 或 token	修改 referer 或 token 后，增删修改无法执行成功	对增删修改类请求接口的 eferer 做白名单校验或在参数中增加随机 token

2.7.4. 测试报告模板

1) NO.01 开发信息

填写表格

信息	描述	备注
开发语言		
开发框架		
数据库类型及版本		

信息	描述	备注
连接数据库框架或函数		
域名		
IP		

开发语言：Java、Python、PHP 等开发框架：Spring、Django、ThinkPHP 等数据库类型：Mysql 5.7 、Redis 5.0.3 等连接数据库框架：MyBatis、SQLAlchemy 等域名：提供服务的域名 IP：ECS 的 EIP、SLB 的 IP

2） NO.02 数据库信息

填写表格(数据库表、字段结构信息);如表和字段较多，仅填写与用户信息相关的表和字段。要求：禁止存储用户的敏感信息(包括但不限于身份证号码、银行卡号等)。如有特殊需求请说明使用场景。

数据库字段名	字段描述	备注

3） NO.03 域名/IP 对外开放端口信息

填写表格并附扫描情况截图要求：EIP 仅开放远程连接端口(如 22、3389 端口)；SLB 仅开放 web 服务端口(如 80、443 端口)；域名仅开放 web 服务端口(如 80、443 端口)。如有特殊端口开放请说明场景。

域名/IP	端口开放信息	备注
EIP：xxx.xxx.xxx.xxx		

域名/IP	端口开放信息	备注
SLB：xxx.xxx.xxx.xxx		
域名：xxx		

将"xxx"替换成域名或 IP 如有 EIP(弹性公网 IP)，请提供 EIP 的端口开放信息；如有多个 EIP，则需提供所有的 EIP 端口开放情况。内网 IP 端口信息无需提供 nmap 使用命令：nmap -sV -T4 -Pn -p1-65535 ip

4） NO.04 敏感信息

填写表格要求：1. 返回或展示较敏感信息(例如手机号、邮箱)需进行打码处理 2. 服务端业务日志不允许打印或存储敏感信息

场景信息	情况描述	备注
是否存在接口返回或展示用户较敏感信息		
服务端业务日志是否打印或存储敏感信息		

5） NO.05 越权漏洞

使用工具：抓包工具

测试情况：

相关接口	功能描述	备注

截图信息：

需要结合自己的业务场景进行测试。填写表格，并附测试情况截图。

要求：所有接口都需进行测试，并且都不存在越权漏洞，但截图可仅提供部分接口的测试截图。

截图要求： 至少需要两张截图，一张 A 用户正常的请求，一张 A 用户修改了 URL 参数的请求。截图需能看出请求的 URL 及返回的内容。

6） NO.06 跨站脚本攻击漏洞

测试情况：

存在输入输出内容的页面	功能描述	备注
xxxx.com/my	修改个人信息的页面	不存在跨站漏洞
xxxx.com/my	查看个人信息的页面	不存在跨站漏洞

截图信息：

填写表格，并附测试情况截图。

要求：所有存在输入内容的页面都需进行测试，并且都不存在 XSS 漏洞，但截图可仅提供部分接口的测试截图。

截图要求：至少需要一张截图，查看内容被插入了 HTML 代码的页面。截图需能看出内容中的 HTML 代码被执行。或使用 APPSCAN 等漏洞扫描工具检测证明不存在 XSS 漏洞。

7） NO.07 SQL 注入漏洞

测试情况：

SQL 操作的代码实现方式	备注

截图信息：

1） 填写表格，并附测试情况截图。

2） 截图要求：使用 SQLMAP 等工具检测证明不存在 SQL 注入漏洞或将执行 SQL 语句相关的关键代码进行截图。使得能够看出来未使用拼接 SQL 语句的方式。

8） NO.08 跨站请求伪造漏洞

使用工具：抓包工具

测试情况：

相关接口	功能描述	备注

相关接口	功能描述	备注
xxx.com/my?username=&age	修改个人信息的接口	不存在跨站请求伪造漏洞
xxx.com/my?delusername=	删除个人信息的接口	不存在跨站请求伪造漏洞

截图信息:

填写表格，并附测试情况截图。

要求：所有接口都需进行测试，并且都不存跨站请求伪造漏洞漏洞，但截图可仅提供部分接口的测试截图。

截图要求：至少需要两张截图，一张正常的 REFERER 或 CSRF-TOKEN 的请求，一张修改了 REFERER 或 CSRF-TOKEN 的请求。截图需能看出请求的内容及返回的内容。或使用 APPSCAN 等漏洞扫描工具检测证明不存在 CSRF 漏洞。

9） NO.09 内容安全

- 填写表格

要求：必须提供过滤不当内容的措施。例如对发布色情、赌博等涉嫌违法违规的词汇、图片、文件、音视频等进行过滤。

建议接入阿里云内容安全服务： https://www.aliyun.com/product/lvwang

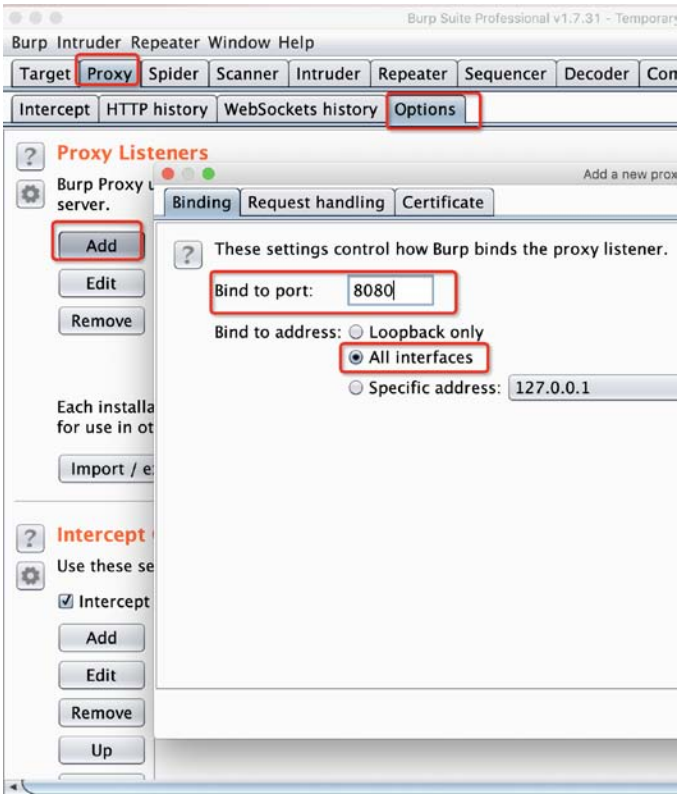
场景信息	具体措施	备注
是否对不当内容进行过滤		

- **burpsuite 使用&导入证书**

设置代理

如图设置代理,端口可自定义。

PC 端:设置 burpsuite 代理监听地址及端口



移动端，以 iOS 为例:填写 burpsuite 的代理地址及端口

WIFI -- HTTP 代理 -- 配置代理

导入证书

手机端在浏览器内访问代理地址 `http://ip:port` 下载并导入证书。

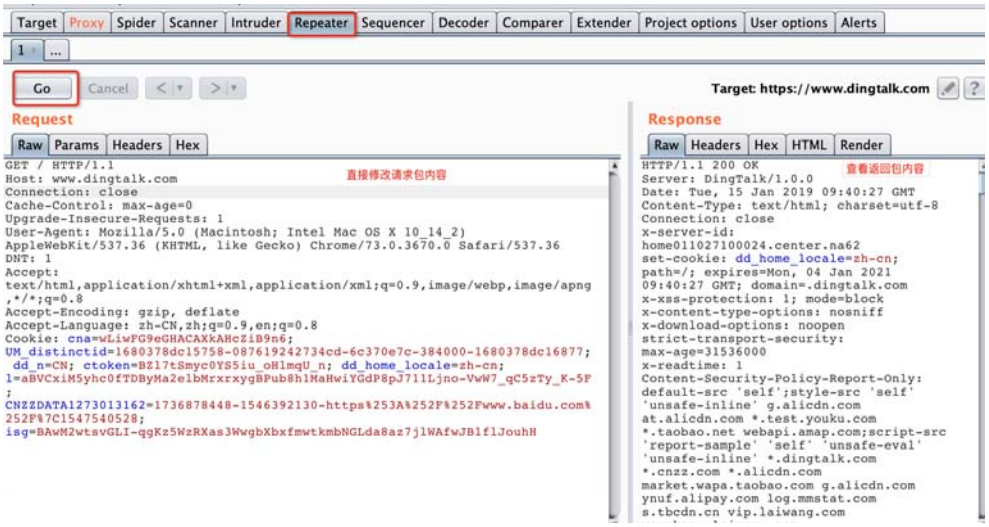
Tips:在 iOS 下，有两处需要设置信任。设置 -- 通用 -- 关于本机 -- 证书信任设置设置 -- 通用 -- 描述文件与设备管理

拦截数据包&修改数据包

拦截数据包并发送到 Repeater 窗口:

在 Repeater 窗口修改数据包并重放:

在左侧窗口直接修改请求包内容,然后通过 Go 按钮发送该请求；在右侧窗口可查看返回的内容。



2.7.5. 附录漏洞扫描报告

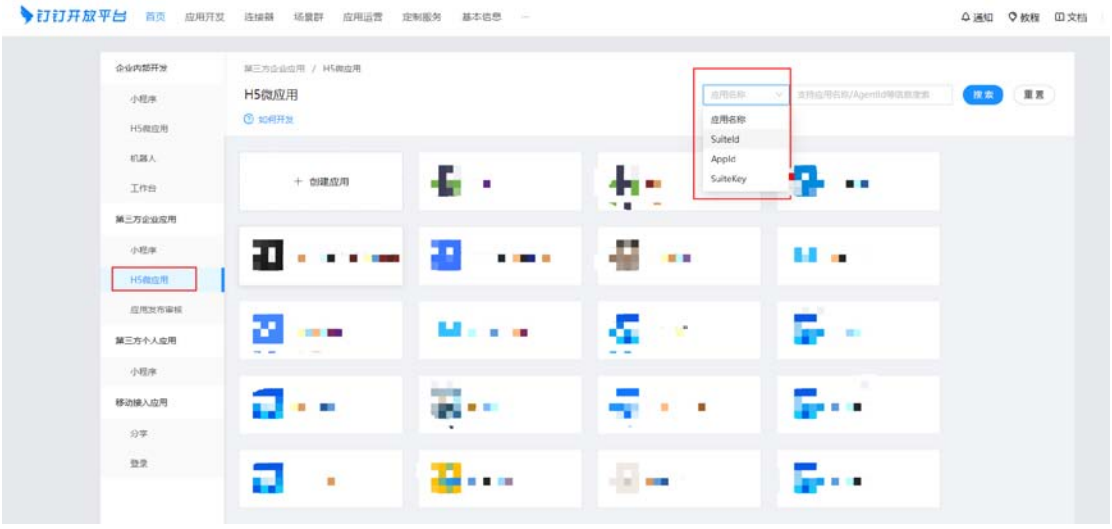
> *漏洞测试项（NO.05 至 NO.09）内容如无法提供测试内容，应提供三个月内漏洞扫描报告。*

2.8. 应用部署

在应用上架后，如需下发给组织安装使用，需要联系运营人员并提供应用的 Appid，由运营人员给出部署安装的二维码，转发给组织管理员扫码安装应用。应用安装后即可使用。部署二维码生成方法：

1. 登录钉钉开放平台：https://login.dingtalk.com
2. 点击应用开发

3. 在第三方企业应用中选择 H5 微应用，根据开发者提供的 Appid 搜索对应的应用。



4. 点击版本管理与发布，在部署二维码处点击查看二维码，点击生成后，即可查看。

3. 应用业务数据回流

数据回流的对接流程如下：

宝山教育局-资源目录排查.xlsx

1. 应用方内部排查业务流程相关的数据（登记在《宝山教育局-资源目录排查.xlsx》表格中，需登记业务系统存在的业务数据范围）；
2. 根据表格内容进行回流数据的资源定义；
3. 双方确认资源，对接方案(接口或其他）

方案可选以下形式

方案一：基座提供宝山区教育私有云前置库，应用系统向前置库上报数据（要求**应用系统部署在宝山区教育私有云环境或具备宝山区校校通网络条件**）

方案二：应用方提供可读数据库，基座主动读取应用业务数据；

方案三：基座提供标准 API，由应用方调取上报数据；

方案四：应用提供稳定 API，由基座调用抽取数据；

4. 数据回流对接,应用方回流数据中涉及到学校、年级、班级、用户等信息时，需提供和宝山基座的数据关系，如数据中有学校信息，则回流数据需要提供对应学校在基座中的唯一标识（cropid)。

4. 应用接入及改造

4.1. 改造自查表

生态伙伴（开发者）可以根据自己的产品特点，结合下表对自己的产品要改造的内容进行初步判断。能力升级的诉求不再此处标识，需要单点的进行产品分析判断。

接入程度	适用场景	界面改造	用户免登	组织架构	消息代办	数据回流

链接型	适用百度搜索、新闻站点、学校/教育部门网站等场景，没有复杂的业务交互和用户体系的公共服务平台（教育部的教育云平台也推出了纯链接版） 这类平台只需要做超链接接入即可让用户便捷使用，可能需要做移动适配	Y	N	N	N	N
传统网页型	过去建立的通过 WEB 网页使用的平台应用，其用户体系是按需开通。可以根据平台后续的主要任务考虑是否进行移动端适配改造，PC 端可直接植入。	Y	Y	N	Y	Y
客户端型（native，无法 H5 化）	有自己独立的 APP/PC 端的客户端应用，如果对底层技术有特殊要求，无法进行 H5 改造的情况下，可以在保留原有端的情况下，通过移动端跨端跳转，PC 端独立入口保留的方式实现。此时需要做一个虚拟应用上架学校，完成服务端的消息调用、通讯录调用 （如果是以学校为单位使用的场景，需要进行组织架构的对接）	N	N	视情况	Y	Y
客户端型（可以 H5 化）	对于原先为独立 APP/PC 端的客户并且可以进行 H5 化改造的产品，采用的方式是对原产品 H5 改造，并接入数字基座的统一端接入 （如果是以学校为单位使用的场景，需要进行组织架构的对接）	Y	Y	视情况	Y	Y
微信小程序/公众号服务	同客户端型的应用场景，根据其使用模式考虑改造（学校为单位使用/个人用户直接使用） 小程序/公众号中的应用一般都完成了 H5 化，只需要在基座中做部分前端 JSAPI 的调用调整即可	视情况	Y	视情况	Y	Y
钉钉小程序/微应用	如果已经是钉钉上的标准第三方生态，只需要在数据回流方面投入改造，组织关系、免登可以通	N	N	N	N	Y

	过钉钉现有体系进行桥接					

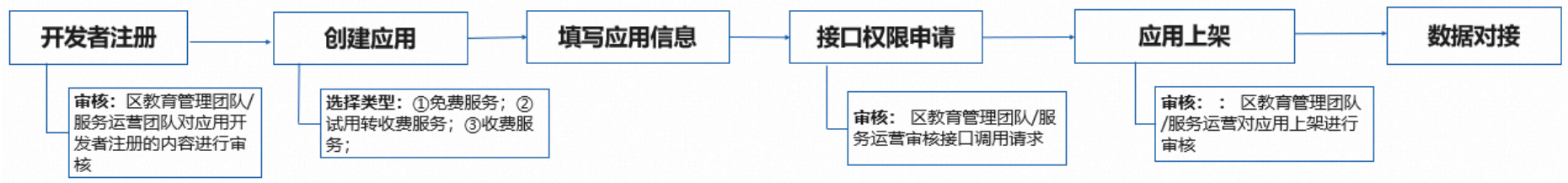
4.2.接入顺序和建议

考虑到应用接入需要投入开发成本，为了平衡交付速度和客户体验，生态伙伴（开发者）可以不用一次性完成自查表中所有的改造，而是分阶段的去进行优化，建议链接开放型从 L1 开始，其他的要从 L2 开始

接入级别	达成效果	实现模式
L1：入口统一	通过快捷链接（业务系统 URL 上翻）的形式，将内部业务系统快速搬到基座，把工作台作为企业办公的统一入口	创建应用超链接即可
L2：权限统一	通过集成 SSO 实现系统免登，无需账密一键进入应用主界面，同时借助通讯录能力将组织架构&角色与业务系统打通，实现权限的一体化管控	1、接入统一用户，实现基座账号和原有系统账号的绑定，用户一个账号畅游各类平台； 2、传统网页可以直接做一个支持扫码登录的模式，未来宝扫码登录，第一次登录进行账号绑定； 3、移动应用端需要 H5 接入基座端后，调用标准免登即可，第一次登录进行账号绑定； 增强能力，可以 1.5 版本实现 4、组织架构打通：涉及到学校使用的，需要完成两边架构的同步；
L3：功能集成	通过集成基座的办公协同开放能力，如审批、考勤、日程、待办、IM、音视频、文档、日志、网盘等，将业务系统上的核心产品功能搬到基座上	1、完成消息代办体系的对接，实现统一消息出口； 2、完成界面改造，便于消息打开后跳转到对应的处理界面，不需要额外打开网站\APP 去处理
L4：数据互通	提供连接器能力，打破各应用之间的数据孤岛；同时提供丰富维度的数据服务，真正实现基座上的管理数字化	数据回流：数据回流区域后，能够被学校端的报表应用进行获取，以进行数据的报表呈现

4.3.对接流程

生态应用上架至教育数字基座应用中心进行服务分发，创建主体为应用开发者，创建应用的类型有多类型。


开发者注册
审核：区教育管理团队/服务运营团队对应用开发者注册的内容进行审核
创建应用
选择类型：①免费服务；②试用转收费服务；③收费服务；
填写应用信息
接口权限申请
审核： 区教育管理团队/服务运营审核接口调用请求
应用上架
审核： ： 区教育管理团队/服务运营对应用上架进行审核
数据对接

五. 开放能力接口说明

为了更好地让教育数字基座服务好上海市教委、各区县教育局、学校用户、学习者及生态开发者等不同用户，现通过教育数字基座开放平台为应用服务商提供开放的能力接口，以及通过数字基座应用开发规范（接入应用 LOGO 设计规范、前后台的视觉色彩设计规范）和应用商运营规范，保证构建一个优质、健康、绿色的教育数字基座生态环境。

1. 服务端 API

因教育数字基座的开放能力在持续更新，其具体提供的服务端 API 接口将持续更新。

当前重点围绕组织中心、通讯录、日程、沟通协同、教育专项等维度开放其能力。后续在接入教育数字基座中有具体能力需求，可以直接教育局进行相关业务接口扩展的沟通。

以下是教育数字基座接口详情表格：

权限分类	权限信息	接口
组织中心	组织树查询	根据省编码获取地市列表
		根据地市编码获取区县列表
		根据区县编码和学校关键字查询学校列表
		根据学校编码查询校区列表
		获取已激活的教育组织的上级组织信息
		获取已激活的教育组织的下级组织信息
		通过组织 id 获取教育数字基座组织详情
	角色相关	获取教育数字基座下发角色列表
		根据教育数字基座 corpid 获取教育数字基座组织 id
		根据教育数字基座 userid 获取角色 id
	用户相关	根据教育数字基座 userid 获取用户认证状态
		根据 userid 和 corpid 查询教育数字基座 userid
		根据手机号获取教育数字基座 userid
		根据教育数字基座用户 id 换取钉钉用户 id
	班级相关	根据学校编码查询年级列表
		根据学校编码和年级编码查询班级列表
		根据学年查询学校的班级列表
		查询班级详情（班级信息、班主任、任课教师）
	学生相关	查询班级内学生列表
		查询学生个人信息
		获取组织下所有学生的照片列表
	教职工相关	根据组织查询教工列表
		通过老师获取老师下所有的班级
消息通知	教育数字基座消息网关	消息通知（先判断是否有钉钉，有则用钉钉发，无则短信发）
教育数字基座回调通知消息	人员变更	用户加入组织
		用户离开组织

		用户信息变更
		用户认证状态变更
	组织变更	组织信息变更
		下级组织增加
		下级组织减少
	角色变更	下发角色新增
		用户角色变更
		角色成员变更
	家校变更	升班
		学生所在班级变更
		班级班主任变更
		家庭成员变更
身份验证	免登接口	教育数字基座免登 SDK 接口
未来宝 APP	教育元数据读权限	查询教育组织类型
		获取学科元数据列表
		获取学段元数据列表
		获取学科实例详情
		获取学科实例列表
	教育在线课堂数据读权限	回放课程
		获取课堂明细数据
		获取课堂概要数据
		获取课程列表
		获取课程参与方列表
		获取课程详情
	教育元数据写权限	删除学科实例
		创建学科实例
		更新学科实例
	教育在线课堂数据写权限	修改课程
		加入课程
		结束课程
		删除课程
		添加课程参与方
		移除课程参与方
		创建课程
		开始课程
	教育班级圈数据读权限	班级圈动态列表开放
		获取班级圈话题列表
	教育行业数字化认证信息读权限	获取数字化证书
	通讯录读取权限	部门列表
		部门人员 ID 列表
		人员信息
		部门信息

个人权限	个人手机号信息	获取用户个人信息
	日历应用中日程写权限	添加日程参与者
		删除日程参与者
		删除日程
		创建日程
		设置日程响应邀请状态
		修改日程
	日历应用中日程读权限	查询日程列表
		查询单个日程详情
	通讯录个人信息读权限	获取用户通讯录个人信息

1.1. 未来宝主要接口清单

序号	接口名称	接口获取方式说明	备注
1	获取主干组织列表	https://open.dingtalk.com/document/orgapp-server/obtain-backbone-organization-list	获取教育局组织信息
2	获取分支组织列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-branch-organization-list	获取学校组织信息
3	获取班级详情	https://open.dingtalk.com/document/orgapp-server/obtains-queries-department-details	获取教育局、学校部门详情
4	获取班级列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-department-node-list	获取教育局、学校部门列表
5	获取班级人员列表	https://open.dingtalk.com/document/orgapp-server/obtains-a-list-of-home-school-user-identities	获取教师、家长、学生列表
6	获取班级人员详情	https://open.dingtalk.com/document/orgapp-server/obtain-the-identity-details-of-home-school-personnel	获取教师、家长、学生详情
7	获取班级内学生的关系列表	https://open.dingtalk.com/document/orgapp-server/queries-the-list-of-relationships	获取学生的家长关系列表，如爸爸妈妈哥哥姐姐等

8	获取学生监护人详情	https://open.dingtalk.com/document/orgapp-server/obtain-the-relationship-between-home-and-school-personnel	获取学生监护人详情
9	获取学段元数据列表	https://open.dingtalk.com/document/isvapp-server/dingtalk-the-main-data-of-the-education-ecosystem-to-query	
10	获取学科元数据列表	https://open.dingtalk.com/document/isvapp-server/dingtalk-the-main-data-of-the-education-ecosystem-query-the-subject	
11	获取学科实例详情	https://open.dingtalk.com/document/isvapp-server/query-dingtalk-education-subject-instances	
12	获取学科实例列表	https://open.dingtalk.com/document/isvapp-server/get-the-list-of-subject-examples	
13	新增未来宝待办任务	https://open.dingtalk.com/document/isvapp-server/add-dingtalk-to-do-task	
14	获取未来宝待办任务详情	https://open.dingtalk.com/document/isvapp-server/obtain-dingtalk-pending-tasks-details	接口最多可以获取到 180 天内已完成状态的待办任务；未完成状态的待办任务无此

			限制。
15	更新未来宝待办任务	https://open.dingtalk.com/document/isvapp-server/updates-dingtalk-to-do-tasks	
16	更新未来宝待办执行者状态	https://open.dingtalk.com/document/isvapp-server/update-dingtalk-to-do-status	
17	使用模板发送工作通知消息	https://open.dingtalk.com/document/isvapp-server/work-notification-templating-send-notification-interface	在调用接口前，确保已经在开发者后台配置并启用了消息模板。 第三方企业应用调用本接口，发送工作通知消息需要注意以下事项： 单次发送人数最大1000。

			每分钟接收人数最大 5000。给同一员工，每天只能发送一条内容相同的消息。 每天给每个员工最多可发送 100 条。
18	发送普通消息	https://open.dingtalk.com/document/isvapp-server/send-normal-messages	发送普通消息，需要在前端页面调用 JSAPI 唤起联系人会话选择页面，选中后会返回会话 cid，然后再调用服务端接口向会话里发送一条消息

1.2. 获取班级组织、人员（任课教师、家长、学生）数据接口说明

序号	动作	路径	接口说明文档	说明
1	获取分支组织列表	1、获取第三方应用授权企业的access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用auth_corpid填主干组织（教育局）的corpid
		2、获取分支组织列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-branch-organization-list	
2	获取主干组织列表	1、获取第三方应用授权企业的access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用auth_corpid填分支组织（学校）的corpid
		2、获取主干组织列表	https://open.dingtalk.com/document/orgapp-server/obtain-backbone-organization-list	
3	获取班级列表	1、获取第三方应用授权企业的access_token	https://open-dev.dingtalk.com/apiExplorer?spm=ding_open_doc.document.0.0.12bd722fuYCRZ2#/?devType=isv&api=dingtalk.oapi.service.get_corp_token	针对三方应用auth_corpid填需要查询部门对应的组织的corpid，查学校的部门就填学校的corpid，查教育局部门就填教育局的corpid

		2、获取班级列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-department-node-list	super_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
4	获取班级详情	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取班级列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-department-node-list	super_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
		3、获取班级详情	https://open.dingtalk.com/document/orgapp-server/obtains-queries-department-details	dept_id 通过第 2 步获取

5	获取班级人员列表	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取班级部门列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-department-node-list	super_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
		3、获取班级部门详情	https://open.dingtalk.com/document/orgapp-server/obtains-queries-department-details	dept_id 通过第 2 步获取
		4、获取班级人员列表	https://open.dingtalk.com/document/orgapp-server/obtains-a-list-of-home-school-user-identities	class_id 是根据第 3 步返回的 dept_type 和 dept_id 确定，当 dept_type 为班级时，dept_id 就是 class_id

6	获取班级人员详情	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取班级部门列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-department-node-list	super_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
		3、获取班级部门详情	https://open.dingtalk.com/document/orgapp-server/obtains-queries-department-details	dept_id 通过第 2 步获取
		4、获取班级人员列表	https://open.dingtalk.com/document/orgapp-server/obtains-a-list-of-home-school-user-identities	class_id 是根据第 3 步返回的 dept_type 和 dept_id 确定，当 dept_type 为班级时，dept_id 就是 class_id

		5、获取班级人员详情	https://open.dingtalk.com/document/orgapp-server/obtain-the-identity-details-of-home-school-personnel	role 和 userid 根据第 4 步返回的信息中获取

1.3.获取行政组织、人员（教职工）数据接口说明

序号	动作	路径	接口说明文档	说明
1	获取组织 corpid	H5 微应用获取组织 corpid	https://open.dingtalk.com/document/isvapp-client/obtain-enterprise-corpid	在应用首页地址和 PC 端首页地址中使用$CORPID$做为参数占位符，当用户在工作台打开应用时，钉钉容器会将$CORPID$替换为当前访问用户的企业 CorpId。
		小程序获取组织 corpid	https://open.dingtalk.com/document/isvapp-client/dd-corpid	使用 dd.corpId 接口获取当前访问用户的企业 corpId。
2	获取分支组织列表	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填主干组织（教育局）的 corpid
		2、获取分支组织列表	https://open.dingtalk.com/document/orgapp-server/obtains-the-branch-organization-list	
3	获取主干组织列表	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填分支组织（学校）的 corpid
		2、获取主干组织列表	https://open.dingtalk.com/document/orgapp-server/obtain-backbone-organization-list	

4	获取部门列表	1、获取第三方应用授权企业的access_token	https://open-dev.dingtalk.com/apiExplorer?spm=ding_open_doc.document.0.0.12bd722fuYCRZ2#/?devType=isv&api=dingtalk.oapi.service.get_corp_token	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取部门列表	https://open.dingtalk.com/document/isvapp/get-department-list	dept_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
5	获取部门详情	1、获取第三方应用授权企业的access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取部门列表	https://open.dingtalk.com/document/isvapp/get-department-list	dept_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
		3、获取部门详情	https://open.dingtalk.com/document/isvapp/query-department-details0-v2	dept_id 通过第 2 步获取
6	获取人员列表	1、获取第三方应用授权企业的access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取部门列表	https://open.dingtalk.com/document/isvapp/get-department-list	dept_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕

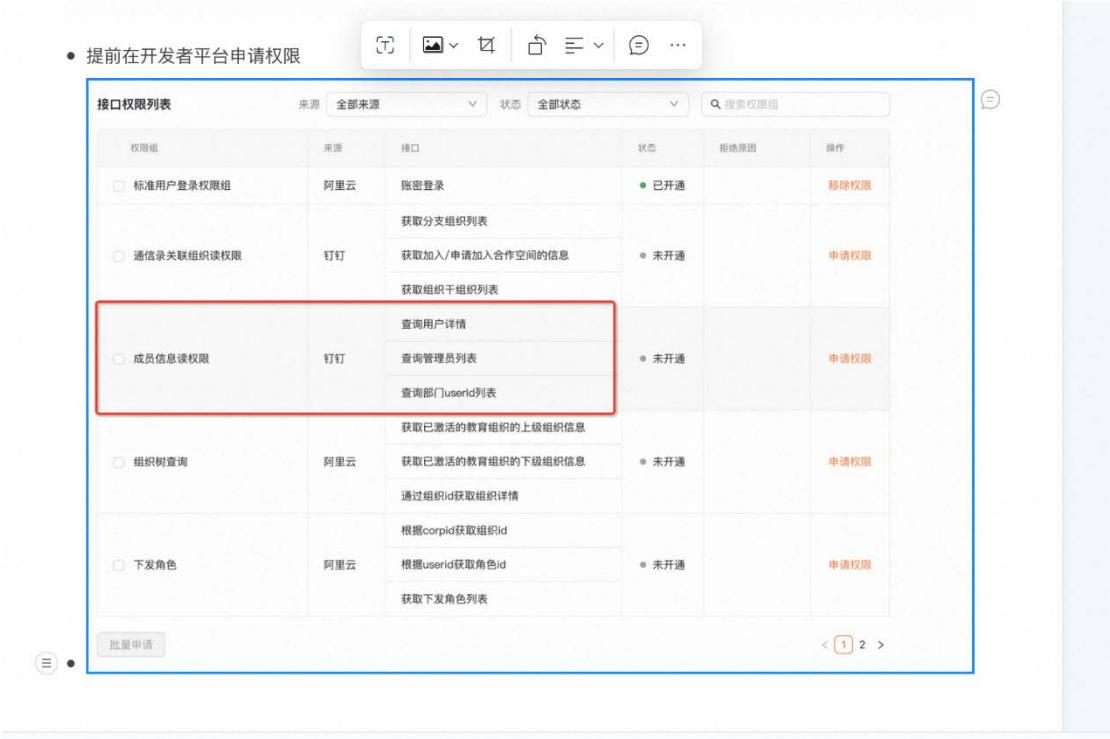
		3、获取部门详情（按需调用）	https://open.dingtalk.com/document/isvapp/query-department-details0-v2	dept_id 通过第 2 步获取
		4、获取部门用户列表	https://open.dingtalk.com/document/isvapp/queries-the-simple-information-of-a-department-user	不包含子部门下的员工，可以根据第 2 步获取的 dept_id 一次获取各子部门下的人员
7	获取人员详情	1、获取第三方应用授权企业的 access_token	https://open.dingtalk.com/document/isvapp-server/obtains-the-enterprise-authorized-credential	针对三方应用 auth_corpid 填需要查询部门对应的组织的 corpid，查学校的部门就填学校的 corpid，查教育局部门就填教育局的 corpid
		2、获取部门列表	https://open.dingtalk.com/document/isvapp/get-department-list	dept_id 可以不填，获取第一层级部门节点 id，再根据这个 id 循环调用部门列表接口，直至把当前组织的多级部门列表遍历完毕
		3、获取部门详情（按需调用）	https://open.dingtalk.com/document/isvapp/query-department-details0-v2	dept_id 通过第 2 步获取
		4、获取部门用户列表	https://open.dingtalk.com/document/isvapp/queries-the-simple-information-of-a-department-user	不包含子部门下的员工，可以根据第 2 步获取的 dept_id 一次获取各子部门下的人员
		5、获取用户详情	https://open.dingtalk.com/document/isvapp/queries-the-complete-information-of-a-department-user	根据 userid 查询信息
		6、获取部门用户详情（按需调用）	https://open.dingtalk.com/document/orgapp/queries-the-complete-information-of-a-department-user	根据 dept_id 查询信息(如果是根部门，该参数传 1；只获取当前部门下的员工信息，不包含子部门内的员工。

2. 教育数字基座单点登录

用于指导应用接入教育数字基座，完成用户体系和数字基座用户体系绑定，实现用户在数字基座工作台免登进入应用。

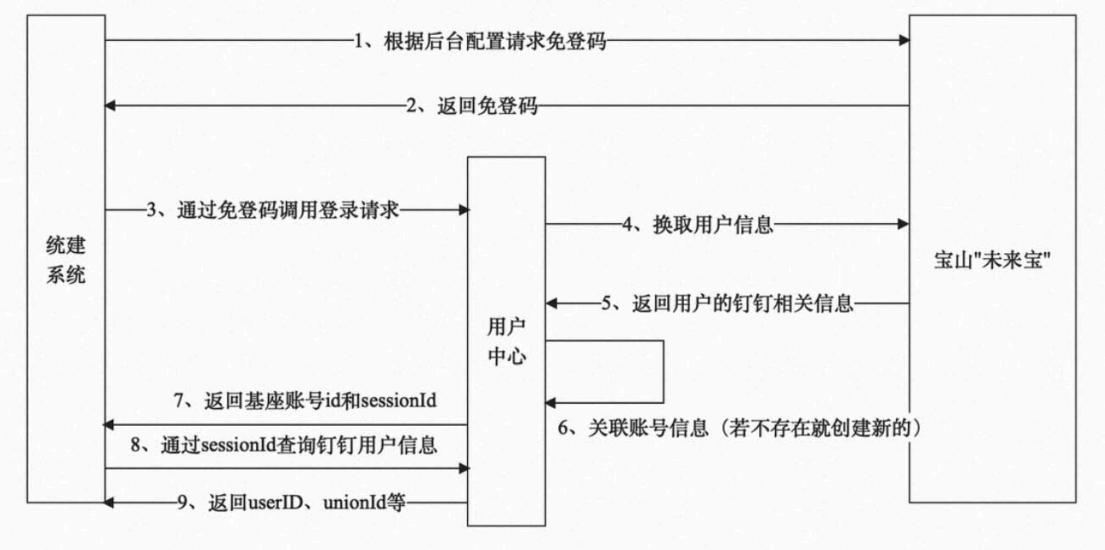
第一步：第三方应用开发者可以在未来宝教育基座的开发者平台创建完应用后，查询获取应用的 SuiteId、AppId、SuiteKey、SuiteSecret，这些信息在调用基座的 API 接口时将作为入参参数。

第二步：接口申请



第三步：请求接口获取数字基座用户 id，并实现用户绑定、免登；

应用开发者根据下面流程图请求接口获取数字基座用户 id，并完成数字基座用户与应用系统用户的绑定，最终实现用户免登录。



2.1. 通过 http 调用单独登录相关接口接入文档

请求路径

- 完整请求路径=网关域名+接口 uri
- 网关域名
  - 上海宝山环境：https://digitalbase.edu-aliyun.com
- 接口 uri
  - 每个接口有特定 uri,以接口文档提供为准
    - 样例： /topapi/cube/StdLoginService_loginByAuth
- 请求方法
  - post

通用入参

○ 每次请求必须携带的通用参数，用户验签，校验接口权限等

参数名	参数位置	类型	描述
accessKey	url 参数	字符串	开发者平台创建应用时分配的 SuiteKEY
timestamp	url 参数	字符串	当前时间的时间戳，单位为毫秒
signature	url 参数	字符串	数字签名,使用开发者平台创建的应用的 SuiteSercet 和时间戳生成，生成方法下文给出 ● 生成签名的时间戳和上一个参数用的时间戳保持一致

○ php 生成 signature 方法

```
 private function computeSignature($accessSecret, $timestamp){
        $s = hash_hmac('sha256', $timestamp, $accessSecret, true);
        return base64_encode($s);
}
```

● 带上通用参数的 url 实例

■ https://digitalbase.edu-aliyun.com/topapi/cube/StdLoginService_loginByAuth?accessKey=suiteiorrtt4pwlu3ipdr&signature=kdXme%2FVkuJwGVVhvmXd4KAoYkr%2F4sIFjZNpCRwPOq%2BU%3D&timestamp=1646881799540

业务入参

○ 每个接口业务相关的参数，具体参考接口列表

○ 统一以 json 方式作为 http 请求 body 参数

○ 样例

```
{
  "appCode": "app_202304186824508",
  "authCode": "7f269fbbfee731d79f45fb0fccb98033",
  "thirdPlatformCode": "DINGDING"
}
```

○ 带上业务参数的完整 curl 请求样例

```
curl --location --request POST 'https://daily-
```

```
cube.zjedu.com/topapi/cube/StdLoginService_loginByAuth?accessKey=suiteh5pwkfpuejfrbs8t&signature=kkH9v8cuQIZmTntynsomvFdQf0NfvS84QZu
YAXHZ2gE=&timestamp=1681808203706' \
--header 'Content-Type: application/json' \
--header 'Postman-Token: ae1752c5-9011-478a-8fad-701e0388f07b' \
--header 'cache-control: no-cache' \
--data-raw '{
  "appCode": "app_202304186824508",
  "authCode": "7f269fbbfee731d79f45fb0fccb98033",
  "thirdPlatformCode": "DINGDING"
}'
```

出参格式

参数名	参数位置	类型	描述
errCode	响应 body	整型	错误码 ● 若请求成功，返回为 0
errmsg	响应 body	字符串	错误信息 ● 若请求成功,返回为 ok
sub_code	响应 body	字符串	子错误码
sub_msg	响应 body	字符串	子错误信息
request_id	响应 body	字符串	请求 id,用于排查问题

● 请求出错返回样例

```
{
    "errcode": 50201,
    "errmsg": "下游服务异常-下游 api 服务错误:调用失败",
    "sub_code": "B_STDUSER_AUTH_CODE_INVALID",
    "sub_msg": "三方授权码无效",
```

```
    "request_id": "eac0a87192168188734697378 62d022e"
}
```


- 请求成功返回样例


```
{
    "errCode": 0,
    "errMsg": "ok",
    "requestId": "eac0a8719d16818878051491677d0a97",
    "result": {xxxxx}

}
```


2.2. 通过未来宝（钉钉）免登码登录

- url
  - https://digitalbase.edu-aliyun.com/user/api/v2/login/loginByAuth
- 请求方式
  - post
- 入参列表

参数名	是否必传	参数位置	参数类型	描述
authCode	是	body	字符串	三方平台的授权 authCode • 如果是未来宝客户端里打开的应用，就是取未来宝的免登码 获取免登码参考：https://open.dingtalk.com/document/isvapp/logon-free-process
appCode	是	body	字符串	应用的 appCode，在教育基座开发者平台注册应用后拿到
thirdPlatformCode	是	body	字符串	三方平台的编码 • 未来宝（钉钉） DINGDING
authType	是	body	字符	授权类型

			串	• 未来宝（钉钉）免登码 DING_AUTO_LOGIN
corpId	是	body	字符串	当前组织的 corpId

o 出参列表

参数名	参数类型	描述	样例
accountInfo	对象	登录账号信息	{ "accountId":"dd7021eb2a4e49daad4d0a0127643b65", 账号 id "mobile":"188****0264",脱敏手机号 "avatar":"",头像地址 "authenticationStatus":"AUTHENTICATED",认证状态

			"nationCode":"CN", "status":"ACTIVATED" }
sessionId	字符串	登录成功的sessionId，有效时间2小时	

2.3. 通过sessionId查询用户未来宝信息（userId,unionId等）

- url
  - https://digitalbase.edu-aliyun.com/user/api/v2/ding/queryDingInfoBySession
- 请求方式
  - get
- 入参列表

参数名	是否必传	参数位置	参数类型	描述
sessionId	是	header	字符串	传登录之后拿到的 sessionId

- 出参列表

参数名	参数类型	描述	样例
unionId	字符串	未来宝 unionId	
userId	字符串	未来宝 userId	
corpId	字符串	未来宝组织 id	
corpName	字符串	未来宝组织名称	
nickName	字符串	昵称	
avatar	字符串	头像地址	

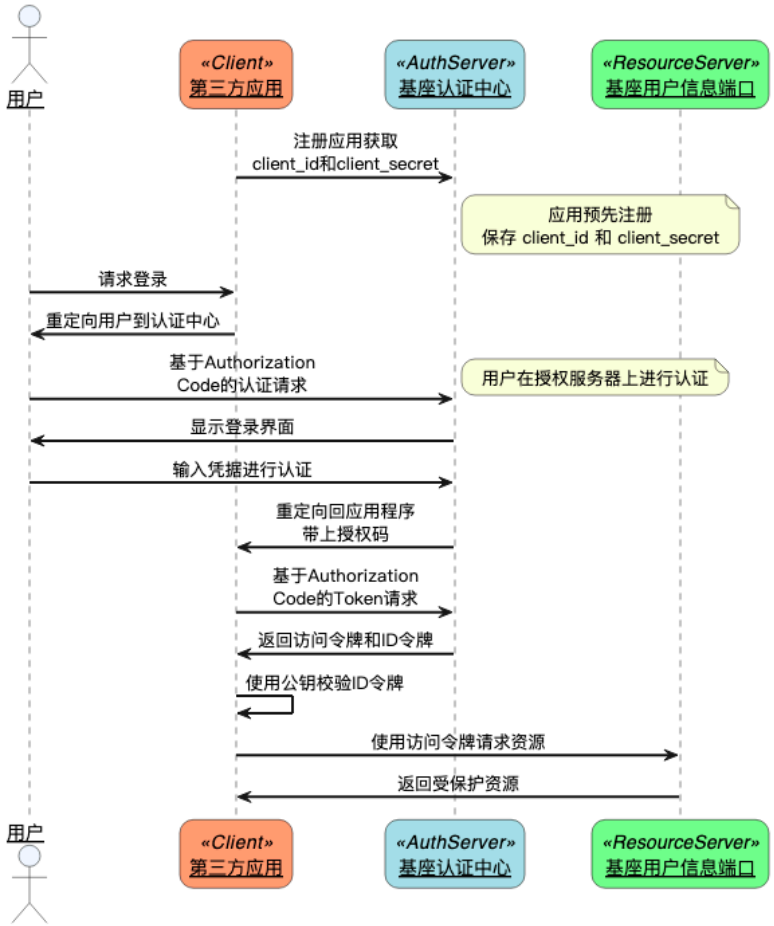
- 异常情形

  - 若返回 http 错误码 401，代表 session 已过期，需要重新调用下登录接口

3. 统一认证授权

开发者创建应用后，需要通过上架申请、审核通过后，即可接入教育基座统一认证授权体系。

本节内容描述了基座认证接入的技术规范，包括如何通过接口进行用户认证、获取 token、获取用户信息以及用户登出等功能。本规范适用于希望接入区认证系统的第三方应用。通过基座实现对所有的学校及教育局直属单位（第三方公司）提供的各种软件应用进行用户身份认证整合，实现单点登录。


用户
«Client»
第三方应用
«AuthServer»
基座认证中心
«ResourceServer»
基座用户信息端口
注册应用获取
client_id和client_secret
应用预先注册
保存 client_id 和 client_secret
请求登录
重定向用户到认证中心
基于Authorization
Code的认证请求
用户在授权服务器上进行认证
显示登录界面
输入凭据进行认证
重定向回应用程序
带上授权码
基于Authorization
Code的Token请求
返回访问令牌和ID令牌
使用公钥校验ID令牌
使用访问令牌请求资源
返回受保护资源
用户
«Client»
第三方应用
«AuthServer»
基座认证中心
«ResourceServer»
基座用户信息端口

3.1.技术规范接口说明

3.1.1. 获取 CLIENT_ID 和 CLIENT_SECRET

在开始接入认证流程之前，第三方应用必须注册并获得 CLIENT_ID 和 CLIENT_SECRET。这些信息将用于认证过程中的客户端身份验证。

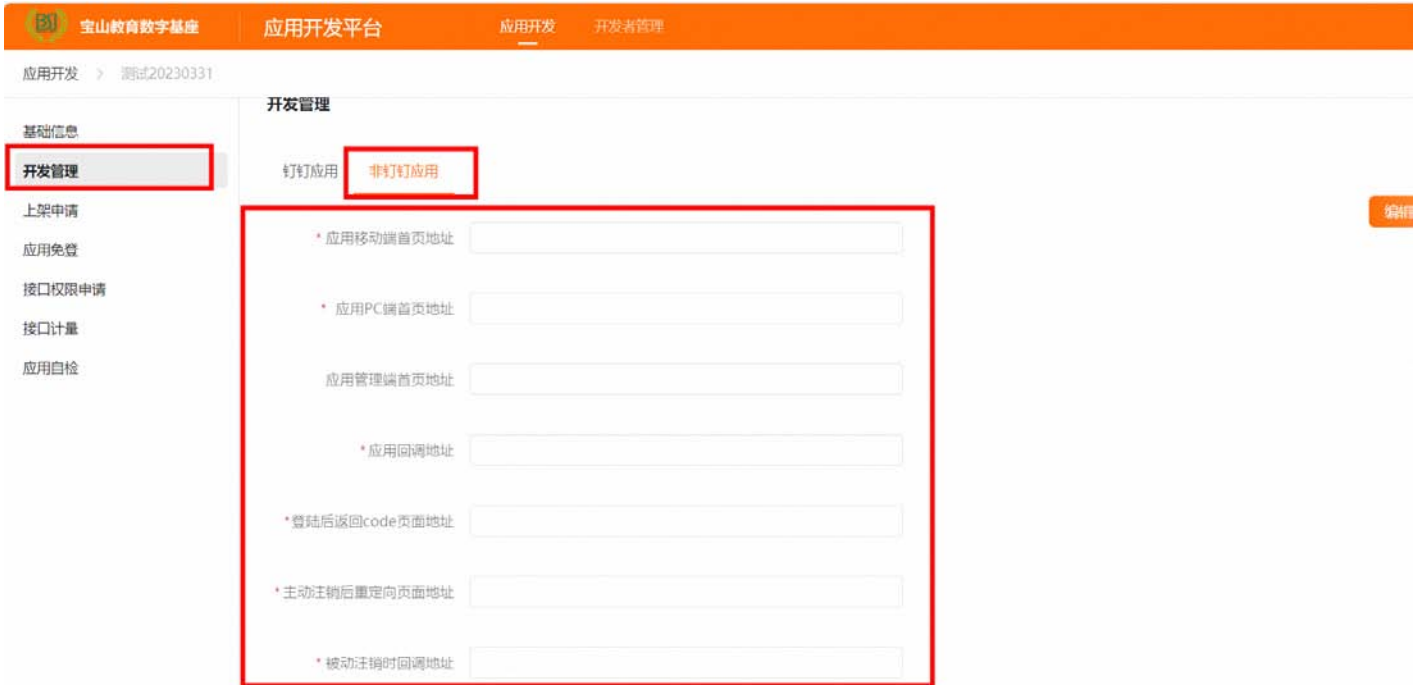
请按以下步骤操作：

1.访问开发者平台

2.创建一个新的应用；

3.在应用注册完成后，在应用基本信息页面查看应用的 CLIENT_ID 和 CLIENT_SECRET，此时该 CLIENT_ID 为禁用状态，开发者需要操作申请上架，而后联系审核人员审核后，该 CLIENT_ID 可以用于统一认证接入。

4.审核通过后，需要在开发者平台对应用回调地址、请求 IP 地址等进行配置(配置页面如下图)后，可以进行如下流程。



应用移动端首页地址、应用 PC 端首页地址：填写应用在不同端的应用首页 URL；
应用管理首页地址:非必填，输入管理员在未来宝(钉钉)管理后台访问该应用的地址
应用回调地址：用于接收未来宝事件事件推送的地址；
登陆后返回 code 页面地址：用户登陆后跳转的地址；
主动注销后重定向页面地址：用户在应用端主动登出后跳转的地址；
被动注销后回调地址：用户在应用端被动登出后未来宝基座回调应用的地址；

3.1.2. 基于 Authorization Code 的认证请求

第三方应用发现用户处于未登录状态时，需引导用户打开如下页面：

https://edu-org.bsedu.org.cn/oauth2/authorize?client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&response_type=code&scope=SCOPE&state=STATE

参考链接如下：
https://edu-org.bsedu.org.cn/oauth2/authorize?client_id=suitevysrsk5s7ue3hdlt&redirect_uri=https%3A%2F%2Fclient.sh.cn%2Fphp%2Findex.php&response_type=code&scope=openid&state=123

注意：跳转回调 redirect_uri，应当使用 https 链接来确保 code 的安全性。
参数说明：

参数	是否必须	说明
client_id	是	第三方应用的唯一标识（suiteKey）
redirect_uri	是	授权后重定向的回调链接地址，请使用 urlencode 对链接进行处理，开发者平台中对应的配置项为：登陆后返回 code 页面地址
response_type	是	返回类型，请填写 code
scope	是	应用授权作用域，请填写 openid 或 openid%20orgInfo，如果 scope 中增加 orgInfo，那么用户信息端口将返回该用户所在的所有组织列表
state	是	重定向后带上 state 参数，开发者可以填写 a-zA-Z0-9 的参数值，最多 128 字节

链接校验成功，则进入下一步，“认证中心”与用户进行交互，在用户未登录时，引导用户进行身份认证。
链接校验失败，则显示错误提示页面。

3.1.3. 基于 Authorization Code 的 Token 请求

如果用户身份认证成功，页面将跳转至 redirect_uri?code=CODE&state=STATE。
code 说明：code 作为换取 id_token 和 access_token 的票据，每次用户认证带上的 code 将不一样，**code 只能使用一次，5 分钟未被使用自动过期**。
参考链接：
https://client.sh.cn/index?code=SplxlOBeZQQYbYS6WxSbIA&state=123

3.1.3.1. 使用 code 请求 Token

第三方应用获取到 code 后，可以通过 code 换取 id_token 和 access_token。发起请求时可以使用 client_secret_post、client_secret_jwt 或 client_secret_basic 的客户端认证方式提交请求。

默认使用 client_secret_jwt 方式，避免 client_secret 在公网传输，如果需其他认证方式，请联系运营。

1.client_secret_jwt 客户端认证方式

```
POST /oauth2/token HTTP/1.1
Host: edu-org.bsedu.org.cn

client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer
&client_assertion=CLIENT_GENRATED_JWT
&client_id=CLIENT_ID
&grant_type=authorization_code
&code=CODE
&redirect_uri=REDIRECT_URI
```

其中 CLIENT_GENRATED_JWT 的生成规则：

- 使用 HS256 签名，使用 CLIENT_SECRET 作为签名密钥

- Payload 中，使用 CLIENT_ID 作为 iss，使用基座 issuer 作为 aud

参数	是否必须	说明
client_id	是	第三方应用的唯一标识
client_assertion_type	是	固定值：urn:ietf:params:oauth:client-assertion-type:jwt-bearer
client_assertion	是	客户端使用 CLIENT_SECRET 生成的 JWT
code	是	填写上一步获取的 code 参数
grant_type	是	填写为 authorization_code
redirect_uri	是	授权后重定向的回调链接地址，开发者平台中对应的配置项为：登陆后返回 code 页面地址，和认证请求的 uri 保持一致

2.client_secret_post 认证方式提交

```
POST /oauth2/token HTTP/1.1
Host: edu-org.bsedu.org.cn

client_secret=CLIENT_SECRET
&client_id=CLIENT_ID
&grant_type=authorization_code
&code=CODE
&redirect_uri=REDIRECT_URI
```

参数说明：

参数	是否必须	说明
client_id	是	第三方应用的唯一标识

client_secret	是	第三方应用的密钥
code	是	填写上一步获取的 code 参数
grant_type	是	填写为 authorization_code
redirect_uri	是	授权后重定向的回调链接地址

3.1.3.2. 返回说明

正确时返回的 JSON 数据包格式如下:

```
{
  "id_token": "ID_TOKEN",
  "access_token": "ACCESS_TOKEN",
  "expires_in": "3600",
  "token_type": "Bearer",
}
```

参考示例如下:

```
{
    "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbXIiOlsicHdkIl0sImF1ZCI6InN1aXRlMTIzIiwiYXV0aF90aW1lIjoxNzAxNjk4Mjc3LCJjbG
llbnRfaWQiOiJzdWl0ZTEyMyIsImV4cCI6MTcwMTcwMTg5MywiaWFOIjoxNzAxNjk4MjkzLCJpZHAiOiJodHRwczovL2xvZ2luLWRhaWx5LWN1YmUuem
plZHUuY29tL29hdXRoMi9hdXRob3JpemUiLCJpc3MiOiJodHRwczovL2xvZ2luLWRhaWx5LWN1YmUuemplZHUuY29tIiwianRpIjoiNDg2YzRmMDktMz
JhMiOONjlhLTk2ZDctNjM2ZmJhNzkzNGZlIiwibmJmIjoxNzAxNjk4MjkzLCJzY29wZSI6Im9wZW5pZCIsInN1YiI6InVpZF82NTVmMDFjZWMwYzJiYT
FhYWIzMDRlYjQifQ.XcqaqcHhVqvJcDCOQdaFiafr_Kz9LKgb8lyLZkUMINUBSOJeeMOHNLPHbjTnpZ3tNPBA4ksWupt6T6ggYj6-
KMQClQa9PLtCrQkzi2AFPOOR-
t7R1g8pqA3Ks7k8cq7pKtOhQAhJA6bJgEQeoi9jmiPkvsw7bMU502IqehOAaeRkOnxcVSwhxtRs6FI_Ma1r7fC1OQVxqed3NOkidLrhtvlpG7VUDVSXG
xYah-OCkLiCpSH1PfQXKBahlCy1OYDeQBwi-
```

htC1UrSiJshSIzUqiDcHXaCFhXEu_hdsbE_fWsr1eqr_li2tQeYxq6vx6aEkPWdxiyZV4RZ8VFqO_iH1w",
"id_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbXIiOlsicHdkIl0sImF0X2hhc2giOiJTQVF1TjFuaXJXZmw3NEVMWjQ5eGJRIiwiYXVkIjoic3VpdGUxMjMiLCJhdXRoX3RpbWUiOjE3MDE2OTgyNzcsImV4cCI6MTcwMTcwMTg5MywiaWF0IjoxNzAxNjk4MjkzLCJpZHAiOiJodHRwczovL2xvZ2luLWRhaWx5LWN1YmUuemplZHUuY29tL29hdXRoMi9hdXRob3JpemUiLCJpc3MiOiJodHRwczovL2xvZ2luLWRhaWx5LWN1YmUuemplZHUuY29tIiwianRpIjoiYTI3Y2FmZTgtNTMzZS00MmZmLTg3MDYtZmYwNjU2ZDkxNTViIiwibmJmIjoxNzAxNjk4MjkzLCJub25jZSI6IjQxYzcxZWJhLWFmNDQtNGMxYi05NzBiLWE2MGFjMmNjNTE1YSIsInNpZCI6Ijk4M2E4YzYwZGYxNjRlZGE4OWZhMmJjMGJhZjc5ODA1Iiwic3ViIjoidWlkXzY1NWYwMWNlYzBjMmJhMWFhYjMwNGViNCJ9.All9iMzodvj0r4-o_a-F_7oqukgyEP18WKkKp944KMtKdZVKQyiJb_B-WSRPbDMNZMtokBw9Q-LCN4-Puweola-GSSpjQ-QyA1bT91jQc3rLo66dhS-D0n5tPiXRGtgGOA-uqsvFvV63onj5QSSk03tEGcOS8rrrkqWogBE2WLjoAdq1o1yoTPbfSo_31hP-hBKzwptKe2oLYbQvrhdLBa-EvVtsARWo2es_9-O_JqZWykFi8MwB1WpVvGSG5keSfTfrFU-790YbDpCVr0BiskkKr67phRUOlNIxbk9Ql8VVBRVeqT6FZuf6gY2kVWVLyMMiqu6wRZRMOASFbHmJfw",
"token_type": "Bearer ",
"expires_in": 3600
}

返回字段	描述
id_token	安全令牌 id_token
access_token	网页授权接口调用凭证
expires_in	access_token 接口调用凭证超时时间，单位（秒）
token_type	token 类型为 Bearer

错误时会返回 JSON 数据包如下（示例为 authorization_code 无效错误）：

{"error": "invalid_code"}

id_token和access_token都是jwt，可以通过解码查看其负载信息，只有sub标识了用户相关的uid。
id_token:

{
"amr": [
"pwd"
],
"at_hash": "6glziVZ_q93eYXqCeNt_5Q",
"aud": "suitevysrsk5s7ue3hdlt",
"auth_time": 1702437804,
"exp": 1702441509,
"iat": 1702437909,
"idp": "https://edu-org.bsedu.org.cn/oauth2/authorize",
"iss": "https://edu-org.bsedu.org.cn",
"jti": "7935006a-6914-4a63-b64d-17f9cc61c1f1",
"nbf": 1702437909,
"nonce": "4ccefbd5-3dd5-44c5-bf4e-595e29e53e16",
"sid": "a1e13196e8bb2ab1074a5f092dbf846f34b7d2bb2e1cd2937168aee47a239384d586fdee4269d5 77e5577c443450fa72",
"sub": "uid_x675d08622889e726be8835cf87a0794165afc3efc05b5145cb49d668d2eff599337b2b06f
3ce5e24e80740423ec74111e8a16318d22e280fc3e0958de1a8016227e8fbc9b09618c9570088be 848ed0e1"
}

access_token:

{
"amr": [

"pwd"
],
"aud": "suitevysrsk5s7ue3hdlt",
"auth_time": 1702437804,
"client_id": "suitevysrsk5s7ue3hdlt",
"exp": 1702441509,
"iat": 1702437909,
"idp": "https://edu-org.bsedu.org.cn/oauth2/authorize",
"iss": "https://edu-org.bsedu.org.cn",
"jti": "ce6e7cbb-378b-4a1a-a92b-0d79ce1dc0fb",
"nbf": 1702437909,
"scope": "openid",
"sub": "uid_x675d08622889e726be8835cf87a0794165afc3efc05b5145cb49d668d2eff599337b2b06f
3ce5e24e80740423ec74111e8a16318d22e280fc3e0958de1a8016227e8fbc9b09618c9570088be 848ed0e1"
}

3.1.4. 基于 AccessToken 的用户信息请求

三方应用在上一步获取到的 token 中， id_token 只有 sub 字段是和用户相关的，如果还需要用户名等其他的用户信息，可以通过 access_token 从 /oauth2/userinfo 接口请求用户信息。

通过 access_token 获取用户信息：

GET 方式请求：

GET /oauth2/userinfo HTTP/1.1
Host: edu-org.bsedu.org.cn
Authorization: Bearer ACCESS_TOKEN
参数说明：

参数	是否必须	说明
ACCESS_TOKEN	是	上一步拿到的 access_token

POST 方式请求：
POST /oauth2/userinfo HTTP/1.1
Host: edu-org.bsedu.org.cn
access_token=ACCESS_TOKEN
参数说明：

参数	是否必须	说明
ACCESS_TOKEN	是	上一步拿到的 access_token

验证接口 token 和请求方式之后返回用户信息：


```
{
"sub": "uid_x675d08622889e726be8835cf87a0794165afc3efc05b5145cb49d668d2eff599337b2b06f
3ce5e24e80740423ec74111e8a16318d22e280fc3e0958de1a8016227e8fbc9b09618c9570088be 848ed0e1",
"uid": "uid_x675d08622889e726be8835cf87a0794165afc3efc05b5145cb49d668d2eff599337b2b06f
3ce5e24e80740423ec74111e8a16318d22e280fc3e0958de1a8016227e8fbc9b09618c9570088be 848ed0e1",
"name": "张三",
"email": "",
"nationalCode": "CN",
"orgId": "c_0001",
"staffId": "ou_123",
```

"eduId": "550e8400-e29b-41d4-a716-446655440000",
"mobile": "158****1111",
"orgUserInfo": [
{
"name": "管理员1",
"orgId": "c_0001",
"orgName": "第一小学",
"staffId": "ou_123"
}
]
}

其中各字段含义为：

	字段名	格式	说明
1	sub	string	用户数字识别号，唯一标识
2	uid	string	用户 uid,即用户数字识别码
3	name	string	用户姓名
4	email	string	邮箱
5	nationalCode	string	国家编码
6	orgld	string	用户当前登录的组织 id
7	staffld	string	用户在当前登录的组织内的员工 id
8	eduid	string	上海市教育服务号
9	mobile	string	掩码手机号
10	orgUserInfo	[]	用户所在组织及用户员工 id 列表，只有认证请求中的 scope 包含了

			orgInfo 时，才会有该信息
11	orgUserInfo.name	string	用户所在组织内名称
12	orgUserInfo.orgId	string	用户所在组织 id
13	orgUserInfo.orgName	string	用户所在组织名称
14	orgUserInfo.staffId	string	用户所在组织的员工 id

可根据获得的这些用户信息，新增或更新第三方应用中此用户的数据。

3.2. 用户登出

3.2.1. 登出流程

用户登出可分为主动登出和被动登出两种情况。

用户在某第三方应用里面点击登出，这种情况为主动登出。在这种情况下，第三方应用应先让用户在本应用内登出，然后给“认证中心”发送一个结束会话的请求，告知“认证中心”此用户已登出。再由“认证中心”告知其他已登录的第三方应用，此用户已登出的消息。此时其他第三方应用的情况为被动登出。

3.2.2. 主动登出

主动登出请求方式如下,请使用页面重定向等方式引导用户调用此接口:

/oauth2/endSession? id_token_hint=ID_TOKEN&post_logout_redirect_uri=POST_LOGOUT_REDIRECT_URI&state=STATE

请求示例

https://edu-org.bsedu.org.cn/oauth2/endSession?id_token_hint=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbXIiOlsicHdkIl0sImF0X2hhc2giOiJ6Tjk3Zm1kMmc3OFVFSjFXNkd4U1J3IiwiYXVkIjoic3VpdGV2eXNyc2s1czd1ZTNoZGx0IiwiYXV0aF90aW1lIjoxNzAyNDM4NjA2LCJleHAiOj

E3MDI0NDIyMjUsImlhdCI6MTcwMjQzODYyNSwiaWRwIjoiaHR0cHM6Ly9lZHUtb3JnLmJzZWR1Lm9yZy5jbi9vYXV0aDIvYXV0aG9yaXplIiwiaXNzIjoiaHR0cHM6Ly9lZHUtb3JnLmJzZWR1Lm9yZy5jbiIsImp0aSI6ImI1ZWM2MzVjLTYyNGQtNDg5Ny05NGI4LWUzYjllMDAwMzA4YyIsIm5iZiI6MTcwMjQzODYyNSwibm9uY2UiOiJmY2FkZTVhOS05ZDA1LTQyNDMtYWY0Ni05NjZiMDg0Y2FhY2UiLCJzaWQiOiJhMWUxMzE5NmU4YmIyYWIxMDc0YTVmMDkyZGJmODQ2ZjM0YjdkMmJiMmUxY2QyOTM3MTY4YWVlNDdhMjM5MzgOZDU4NmZkZWU0MjY5ZDU3N2U1NTc3YzQ0MzQ1MGZhNzIiLCJzdWIiOiJ1aWRfeDY3NWQwODYyMjg4OWU3MjZiZTg4MzVjZjg3YTA3OTQxNjVhZmMzZWZjMDViNTE0NWNiNDlkNjY4ZDJlZmY1OTkzMzdiMmIwNmYzY2U1ZTI0ZTgwNzQwNDIzZWM3NDExMWU4YTE2MzE4ZDIyZTI4MGZjM2UwOTU4ZGUxYTgwMTYyMjdlOGZiYzliMDk2MThjOTU3MDA4OGJlODQ4ZWQwZTEifQ.eCxWIuY7Mj6-6WMAlyHOi2Rw-4YFy5EdjRyo51MYVA7KI3fT4hS0g7kBIWE5Hv8giqIV8ToapLN78RuiQFZO9rD8SJjFk_YEDXG7eJpZVIIbtW0m9cRA8OEZCtg3wTb4R1vIoRXv4ldChtdyNSy7rjbU_SzA2jHNKMMbovGiqzG64iaffyLUKDe3Z0aiht2aV2lxBGfHc66gW9hNdiOZVlrq9T3o9U6zVF38k5sBt6_MLAGE5e_udX6FcOPCGVKtzFtP3LTXb1RD8su2WM7mvbW0d6fS1wFzv0FoRmfuwgWX1J9BtrVhQPIZNSJNBkUPJMKO7sGBHtkxfzb9mq-T5g&post_logout_redirect_uri=https%3A%2F%2Fclient.sh.cn%2Fphp%2Findex.php&state=123

参数说明：

参数	是否必须	说明
id_token_hint	是	登录过程中获取到的 id_token
post_logout_redirect_uri	是	登出后重定向的回调链接地址，请使用 urlencode 对链接进行处理，需要和应用配置的回调地址一致，开发者平台中对应的配置项为：主动注销后重定向页面地址
state	否	重定向后带上 state 参数，开发者可以填写 a-zA-Z0-9 的参数值，最多 128 字节

3.2.3. 被动登出

在被动登出的情况下，第三方应用需在开发者平台配置应用的登出回调地址。使用同一登录态登录的用户主动注销时，基座会回调其他应用的登出回调地址，应用根据参数登出指定的用户。

基座从服务器端发起请求，请求的地址为第三方应用指定的登出回调地址，参数为 logout_token。

请求方法：

POST BackChannelLogoutUri HTTP/1.1
Host: edu-org.bsedu.org.cn
logout_token=LOGOUT_TOKEN

请求示例：

GET BackChannelLogoutUri HTTP/1.1
Host: edu-org.bsedu.org.cn
logout_token=eyJhbGciOiJSUzI1NiIsImtpZCI6ImFkMWU3YmE2YjMwOTNmMGE1YjMzNjQ3Y2JlZWNlNDU3IiwidHlwIjoiSldUIn0.eyJuYmYiOj
E1NzEzMjM2OTgsImV4cCI6MTU3MTMyMzk5OCwiaXNzIjoiaHR0cHM6Ly9pZC5wZGVkdS5zaC5jbiIsInN1YiI6IjE0NjgyIiwiYXVkIjoiMTAuNj
YuMTA0LjMwIiwiaWF0IjoxNTcxMzIzNjk4LCJqdGkiOiI2M2YwY2YxMWE3MDQ1NDdiZDRjZjFhZGJjMzY4NjdiMSIsInNpZCI6ImViMzMzYTAzMm
UwNDY0OTVhYzc3YTgwZjQ5NGQ2MWY5IiwiZXZlbnRzIjp7Imh0dHA6Ly9zY2hlbWFzLm9wZW5pZC5uZXQvZXZlbnQvYmFja2NoYW5uZWwtbG9nb3
V0Ijp7fX19.beScsTlZBklNTG_SK7hCeCG0U9A30a0xNUjxgZW3KWtOB6iHQEXdyfqFs9oKwjOOrhYr3GjApYisGyTDgWTOhW_Hn76oaCyTLLXqI wIM35-
N7Jy2I4mw_IXfrliPnEk3F5U9tGvle6-sooFNbd_cwubHTFKp0AYXJJ2FVTxIbsKWYJGi0Gu4JfWYa3IhXXE6fpszx0PtjDdAEb5-19hbb W8-
J5gXS43jUnaQCaf0DEiAPmgj-k_8_lYeVQYM7dNvqA3WThFpC3tK7WvHV7IFIY77h360XFAdkKfojogAPIWnVRWWP3_l2AOnrMwciZkZ53osa n9nc5o3aMwE_5Ec-g

logout_token 是一个 jwt，解析后内容如下：

{
  "aud": "suitevysrsk5s7ue3hdlt",
  "events": {
    "http://schemas.openid.net/event/backchannel-logout": {}
  },
  "exp": 1702448803164,
  "iat": 1702448205,
  "idp": "https://edu-org.bsedu.org.cn/oauth2/authorize",
  "iss": "https://edu-org.bsedu.org.cn",

"jti": "cf086125-fd34-471c-990f-251c2978ac80",
"nbf": 1702448203,
"sid": "a1e13196e8bb2ab1074a5f092dbf846f34b7d2bb2e1cd2937168aee47a239384d586fdee4269d577e5577c443450fa72",
"sub":
"uid_x675d08622889e726be8835cf87a0794165afc3efc05b5145cb49d668d2eff599337b2b06f3ce5e24e80740423ec74111e8a16318d22e280fc3e0958de1a8016227e8fbc9b09618c9570088be848ed0e1"
}
需要先判断这个 logout_token 的有效性，然后让 sub 字段指定的用户登出。

3.3. APP 端接入说明

基座提供的统一身份认证功能，如需应用于手机或平板上 App 中，请在用户点击“登录”按钮时，在 App 中用 WebView 控件加载如下页面：
https://edu-org.bsedu.org.cn/oauth2/authorize?client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&response_type=code&scope=SCOPE&state=STATE
（参数及说明详见技术规范接口说明章节）
后续用户登录流程与上文中描述的一致。
最后把经过基座认证的用户身份信息及 id_token 信息通过 js 函数调用形式，从 WebView 内部传递给 App。这样就在 App 中完成了用户身份的认证。
同时拿到的 id_token 用于用户登出过程。
当然 APP 端也可以应用于 Window 电脑应用程序。

4. 数字基座应用开发规范

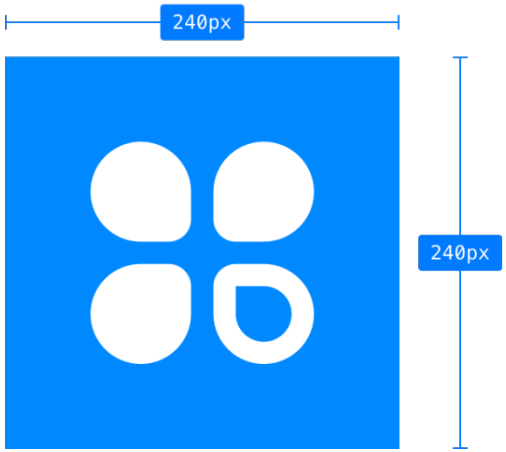
4.1. 教育数字基座应用 Logo 设计规范

4.1.1. 要求概述

- 简洁明了、表达准确、避免使用文字、不要使用照片；
- 为了更好的使用「面型」图标，避免使用「线型」图标，便于应用 Logo 在各种场景下保证清晰、可读；
- 建议使用纯白颜色填充，以保证在彩色背景下足够突出；
- 如 ISV 有自己的品牌图形，应当使用扁平化或剪影的方式呈现，以便在应用 Logo 缩小后易于识别；
- 为避免在浅色底上的可阅读型以及视觉统一性，请勿使用黑色、白色、浅灰色作为图标背景色；
- 图标不能有任何的压缩、拉伸、模糊。

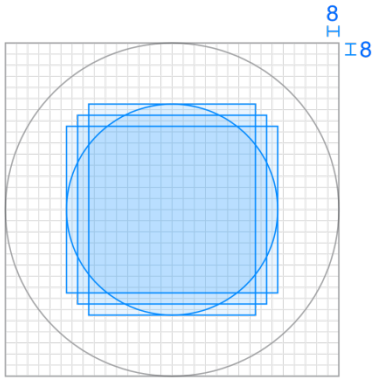
4.1.2. 切图要求

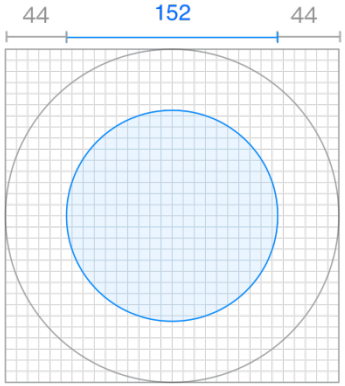
应用 Logo 输出实际尺寸为：240*240px，直角 PNG/JPG，纯色不透明背景，不超过 2M



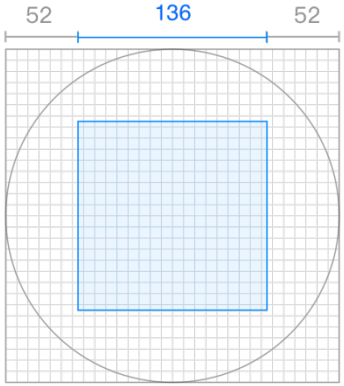
4.1.3. 栅格系统

- 为统一应用 Logo 视觉体量，请确保背景容器内图形尺寸处于圆形、方形、矩形的栅格区域内；
- 单位栅格尺寸为 8*8px。

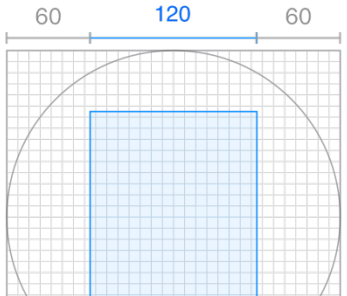


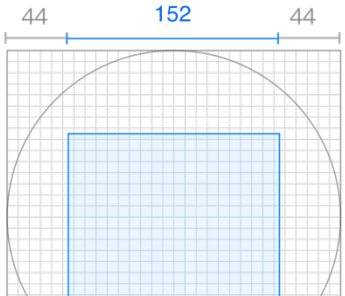


圆形区域152*152



方形区域136*136





4.1.4. 背景颜色

- 二方、三方应用可使用自己的品牌色；
- 一方应用与功能入口图标背景色，从以下色板选取；
- 不可使用渐变、纯白、纯黑色，应当为单一的纯色背景。

4.1.5. 安全补充

- 应用 Logo 需原创，无法律风险；
- 应用 Logo 不允许出现禁限售、低俗等非法字符和图案，如“黄赌毒、枪支、烟草等”；不能涉及政治倾向、政治色彩；
- 应用 Logo 不允许出现红点、NEW、HOT 等标签；
- 不要使用二维码作为小程序 Logo；
- 教育数字基座团队拥有应用图标上传的审核权以及最终解释权。

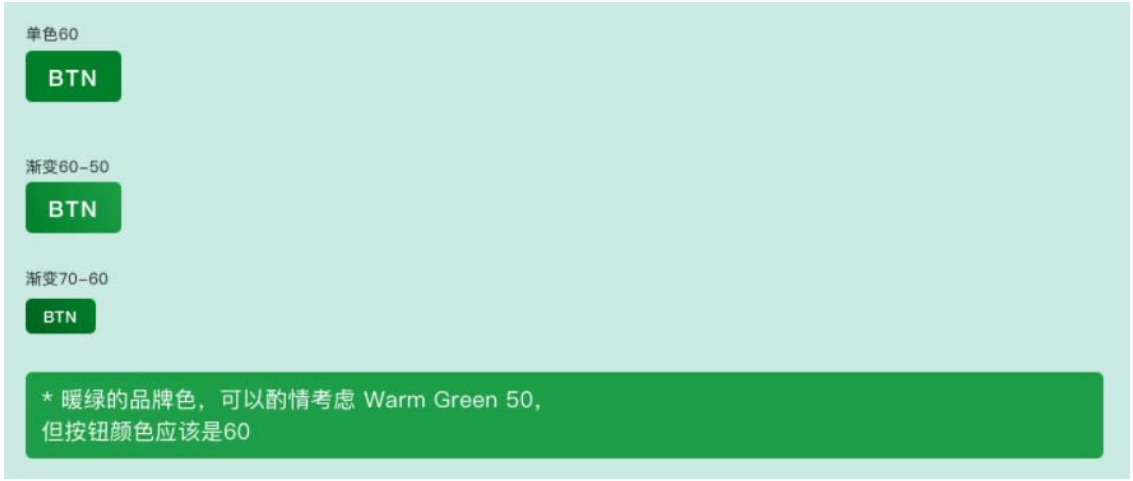
4.2. 视觉色彩设计规范（以下为参考视觉色彩，最终以教育局公布为准）

4.2.1. 教育-前台（学生）应用设计规范

（1）色彩设计规范

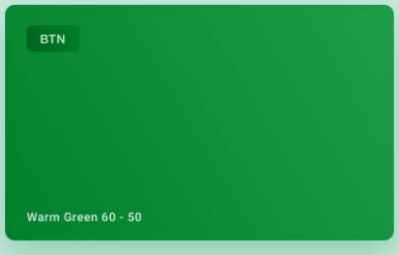

Warm Green 100 18 # 001B09
Warm Green 90 15 # 002E0F
Warm Green 80 11 # 004717
Warm Green 70 7.5 # 006221
Warm Green 60 acs 5 H 140 S 100 B 50 # 00802A
Warm Green 50 6 # 1E9E48
Warm Green 40 8.5 # 3EBC67
Warm Green 30 12 # 69D58C
Warm Green 20 16.5 # A3F3BD
Warm Green 10 19.5 # D0FFE0

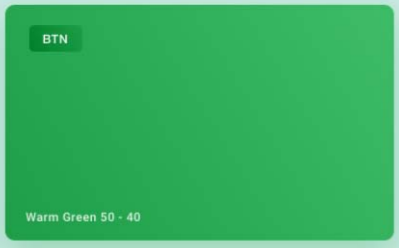
（2）按钮渐变


单色60
BTN
渐变60-50
BTN
渐变70-60
BTN
* 暖绿的品牌色，可以酌情考虑 Warm Green 50，
但按钮颜色应该是60

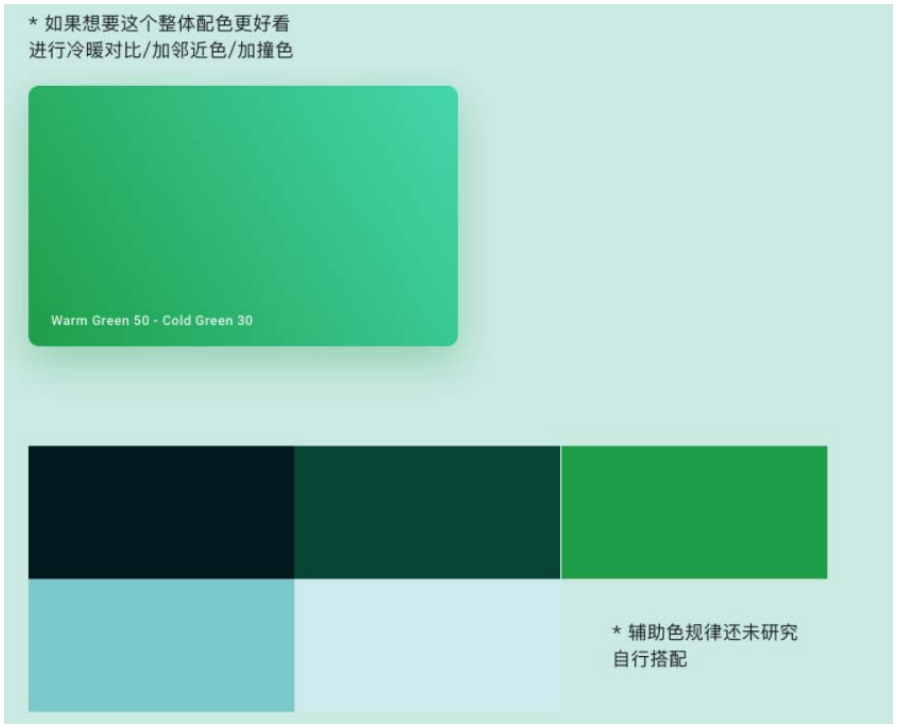
（3）卡片渐变

当按钮60–50渐变时，卡片渐变50–40，从左下角往右上角斜度渐变
当按钮70–60渐变时，卡片渐变60–50
卡片阴影为当前2色中最大数值（如卡渐变为50–40，则选50），参数：alpha 30%，x=0，y=12，blur=32





* 可以酌情选择 50–30或60–40的渐变，跨度不超过20，比如导航


* 如果想要这个整体配色更好看
进行冷暖对比/加邻近色/加撞色
Warm Green 50 · Cold Green 30
* 辅助色规律还未研究
自行搭配

（4）导航栏渐变

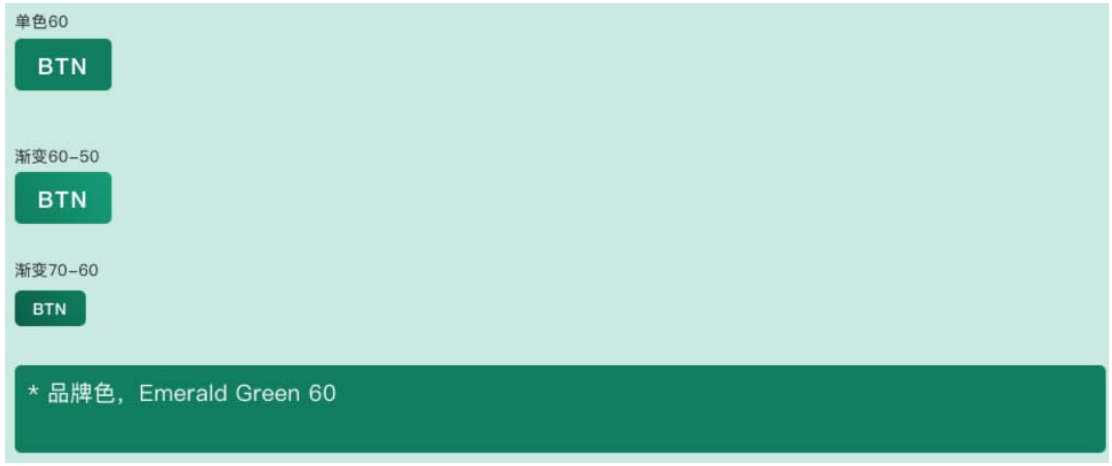

导航栏渐变
前台用户使用产品
中后台工具型产品

4.2.2. 教育-后台（开发者）应用设计规范

（1）色彩设计规范

Emerald Green 100	18		# 031A14
Emerald Green 90	15		# 062C22
Emerald Green 80	11		# 094535
Emerald Green 70	7.5		# 0C5E48
Emerald Green 60	acs 5	H 164 S 87 B 49	# 117E61
Emerald Green 50	6		# 169C78
Emerald Green 40	8.5		# 2CBA95
Emerald Green 30	11.5		# 4BD6B1
Emerald Green 20	16		# 9BF1DA
Emerald Green 10	19		# CCFFF2

（2）按钮渐变



（3）卡片渐变

当按钮60–50渐变时，卡片渐变50–40，从左下角往右上角斜度渐变
当按钮70–60渐变时，卡片渐变60–50
卡片阴影为当前2色中最小数值（如卡渐变为50–40，则选40），参数：alpha 30%，x=0，y=12，blur=32

* 可以酌情选择 50–30或60–40的渐变，跨度不超过20，比如导航中

（4）导航栏渐变

5. 运营规范

我们一直致力于为教育行业提供绿色、健康的生态环境，努力打造一个教育行政部门、企事业单位、教育机构与个人用户之间交流和服务的优质平台，给予用户更多的选择和便利，进一步推动上海市宝山区数字化转型并创造更多的社会价值。

5.1. 运营规范概述

教育数字基座平台的良好可持续发展有赖于教育数字基座平台运营者及广大教育数字基座生态合作伙伴的共同努力与支持，以下运营规范的内容有助于运营者更加清晰地了解教育数字基座的运营规则，期望我们一起创建并维护运营者、用户、平台等各方共建共享共生乃至共赢的生态体系。

5.2. 注册规范

- 教育数字基座入驻主体向平台提供的联系方式和主体信息必须真实有效。
- 教育数字基座服务提供者应按照协议的要求提供相应的审批、备案等资质文件材料，以此保障平台和其他用户的安全、稳定。
- 为保证服务质量和平台的良性发展，入驻教育数字基座时应避免批量注册、重复提交相似功能的应用或服务。
- 教育数字基座生态合作伙伴提供的所有内容信息不得违反国家法律法规、违反公序良俗或侵害第三方权益。小程序的名称、icon、简介、描述等信息不得含有政治敏感、色情、暴力血腥、恐怖内容及国家法律法规禁止的其他违法内容。

- 宝山区教育局有权拒绝入驻主体提交的从事或为从事违法行为、非法活动提供便利、协助等不合理的教育数字基座生态合作伙伴。
- 应用平台的基本信息描述应准确反应其核心功能，并实时更新。

5.3. 认证规范

- 需遵守《教育数字基座平台认证服务协议》及相关认证规则。
- 申请企业版支付宝账号，并通过商家实名认证。

5.4. 入驻规范

- 申请入驻：以认证企业的主/子管理员的账号，登录教育数字基座合作伙伴管理后台，在对应的合作伙伴类型下提交入驻申请；
- 合作审批：提交企业资质、服务案例，审核资质，签订合作协议；
- 人员授权：进入人员管理，添加负责教育数字基座业务的人员并设置职位；
- 上线合作：完成人员培训，正式开展业务。

以下特殊情况不接受入驻申请

- 因一类违规被终止合作的部署服务商、销售服务商禁止二次引入，其法定代表人或者股东参股公司禁止引入；
- 其他违反法律、法规及教育数字基座规定的情况。

5.5. 行为规范

以下行为严重违规并影响教育数字基座用户体验，还可能给其他运营者、用户及平台带来损害，一经发现将根据违规程度采取相应的处理措施。

- 应用平台的页面内容中，不得存在诱导类行为，包括但不限于诱导分享、诱导添加、诱导关注、诱导下载等；如不得要求用户分享、添加、关注或下载后才可操作；不得含有明示或暗示用户分享的文案、图片、按钮、弹窗、浮层等；不得通过利益诱惑诱导用户分享、传播；不得使用

夸张言语来胁迫、引诱用户分享；不得强制或诱导用户添加教育数字基座应用。

- 不得存在恶意刷量、刷单等行为。
- 不得在用户不知情或用户未进行任何触发操作的情况下跳转其他应用平台。
- 不得滥用模板消息，包括但不限于利用模板消息骚扰用户活动或进行广告营销。
- 不得滥用客服消息，向用户发送与咨询无关的任何文案、图片。
- 不得通过教育数字基座实施多级分销欺诈行为，发布分销信息诱导用户进行添加、分享或直接参与。
- 不得以奖励或其他方式，强制或诱导用户将消息分享至朋友圈的行为。奖励的方式包括但不限于：实物奖品、虚拟奖品（积分、信息）等。
- 未经同意不得以教育数字基座的名义进行夸大或者虚假推广。
- 未经宝山区教育局书面许可不得利用其他教育数字基座账号、个人账号和任何功能或第三方运营平台进行推广或互相推广。
- 不得有恶意篡改功能行为，不得有目的性的对应用平台的功能或文字进行篡改，违反应用平台功能的原本用途或意义。
- 应合法、合规、正当、善意地使用教育数字基座提供的各项功能、接口和能力等，使用时应遵循与宝山区教育局签署的相关协议规则。

5.6. 内容规范

教育数字基座生态合作伙伴的服务内容需要遵守《教育数字基座平台服务协议》、相关法律法规的规定。用户发送内容如涉及违反相关规定，一经发现将根据违规程度对入驻账号采取相应的处理措施，包括但不限于：

5.6.1. 侵权或侵犯隐私类内容

（1）主体侵权

- 擅自使用他人已经登记注册的企业名称或商标，侵犯他人企业名称专用权及商标专用权。

- 擅自使用他人名称、头像，侵害他人名誉权、肖像权等合法权利。
- 此类侵权行为一经发现，将对违规账号予以注销处理。

（2）内容侵权

- 未经授权发送他人原创文章，侵犯他人知识产权。
- 未经授权发送他人身份证号码、照片等个人隐私资料，侵犯他人肖像权、隐私权等合法权益。
- 捏造事实公然丑化他人人格，或用侮辱、诽谤等方式损害他人名誉。
- 未经授权发送企业商业秘密，侵犯企业合法权益。
- 首次出现此类侵权行为将对违规内容进行删除处理，多次出现或情节严重的将对违规账号予以一定期限内封号处理。

5.6.2. 色情及色情擦边类内容

- 散布淫秽、色情内容，包括但不限于招嫖、寻找一夜情、性伴侣等内容。
- 发送以色情为目的的情色文字、情色视频、情色漫画的内容，但不限于上述形式。
- 长期发送色情擦边、性暗示类信息内容，以此来达到吸引用户的目的。

5.6.3. 暴力内容

- 散播人或动物被杀、致残以及枪击、刺伤、拷打等受伤情形的真实画面。
- 出现描绘暴力或虐待儿童等内容。
- 出现吸食毒品、自虐自残等令人不安的暴力画面内容。
- 无资质销售仿真枪、弓箭、管制刀具、气枪等含有杀伤力枪支武器。

- 出现以鼓励非法或鲁莽使用方式等为目的而描述真实武器的内容。

5.6.4. 赌博类内容

发送组织聚众赌博、出售赌博器具、传授赌博（千术）技巧、方式、方法等内容。

5.6.5. 危害平台安全内容

- 发送钓鱼网站等信息，诱使用户上当受骗蒙受损失。
- 发送病毒、文件、计算机代码或程序，可能对微信消息发送服务的正常运行造成损害或中断。

5.6.6. 涉黑类内容

发送替人复仇、收账等具有黑社会性质的信息；雇佣、引诱他人从事恐怖、暴力等活动；拉帮结派，招募成员，对社会秩序构成潜在危害的内容。

5.6.7. 非法物品类内容

包括但不限于买卖发票；出售假烟、假币、赃物、走私物品；违法办证刻章、代办身份证、信用卡、办理手机复制卡等信息；交易人体器官等内容。

5.6.8. 广告类内容

- 欺诈虚假广告类：以骗取钱财为目的的欺诈广告（例如网赚、中奖类信息）；虚假夸大减肥、增高、丰胸、美白效果但明显无效的保健品、药品、食品类广告；推广销售假冒伪劣商品的广告。
- 违法广告类：包括但不限于：贩卖毒品、窃听器、军火、人体器官、迷药、国家机密，信用卡套现，办证，非法刻章，性虐等。
- 广告推荐商品本身和教育数字基座账号所公示身份（包含注册及公示的主体资料及运营业务范围）无关，如：账号名称为心情语录，实际售卖减肥产品等。

5.6.9. 谣言类内容

发送不实信息，制造谣言，可能对他人、企业或其他机构造成损害的内容。

5.6.10. 搔扰类内容

过度营销，对用户造成搔扰的内容。

5.6.11. 其他涉及违法违规或违反相关规则的内容

5.7. 数据使用规范

(1) 获取或使用用户数据

- 未经用户明确同意，并向用户如实披露数据用途、使用范围等相关信息的情形下复制、存储、使用或传输用户数据。
- 要求用户共享个人信息（手机号、出生日期等）才可使用其功能，或收集用户密码或者用户个人信息（包括但不限于，手机号，身份证号，生日，住址等）。
- 向第三方显示用户微信号、名称、QQ、手机号、电子邮箱地址和出生日期等。
- 将用户微信号、名称、QQ、手机号、电子邮箱地址和出生日期等信息用于任何未经用户及教育数字基座平台授权的用途。
- 企图进行反射查找、跟踪、关联、挖掘、获取或利用用户微信号、名称、QQ、手机号、电子邮箱地址和出生日期等信息从事与教育数字基座账号所公示身份无关的行为。

(2) 地理位置数据使用

- 在采集、传送或使用地理位置数据之前未通知并获得用户同意的教育数字基座账号将会被拒绝。
- 使用基于地理位置的 API 用于车辆、飞机或其他设备的自动控制或自主控制的应用平台将会被拒绝。

- 使用基于地理位置的 API 用于调度、车队管理或应急服务的应用平台将会被拒绝。
- 地理位置数据只能用于应用平台提供的直接相关功能或服务，或者有授权的广告。

5.8. 支付规范

需遵守《教育数字基座电子商务服务协议》和《教育数字基座支付用户服务协议》。

5.9. 8. 内测规范

- 我们新的功能与接口都将以内测的形式发布出来，欢迎教育数字基座账号的运营者申请内测。
- 我们有权根据产品运营需要制定并修改针对内测名额的限定以及内测接口的使用规则。

5.10. 商标与商业外观

- 应用平台必须遵守商标、版权等知识产权法律法规以及教育数字基座关于知识产权使用的相关规则。
- 非商标所有权人或未经授权使用他人商标的教育数字基座帐号将会被拒绝。
- 使用他人商标、版权等涉及他人知识产权的内容需要在帐号申请时如实说明，并根据要求提供相关权利证书或授权证明。
- 非教育数字基座官方帐号，禁止在帐号名称、输出内容中出现与数字基座已有知识产权内容相同、相近似的字样，或者容易与已有数字基座产品设计主题、外观等相混淆的内容。
- 任何误导和暗示宝山区教育局是该帐号运营者，或者误导和暗示宝山区教育局以任何形式表示认可其质量、服务或与其存在合作关系，而并非宝山区教育局运营的教育数字基座帐号将会被拒绝。

5.11. 处罚和举报

教育数字基座平台已启用用户举报处理机制，我们会根据用户的举报，视违规程度予以不同程度的处罚措施。

5.12. 免责声明

宝山区教育局明确了解并同意关于教育数字基座平台服务，宝山区教育局不提供任何种类的明示或暗示担保或条件，包括但不限于商业适售性、特定用途适用性等。开发者对教育数字基座平台的使用行为必须自行承担相应风险。

六. 常见问题解答

当前仅补充核心常见问题，后续根据各厂商通用问题持续补充。

1. 应用在接入教育数字基座时，如何判断什么时候接入“随申办”？

教育数字基座作为上海市宝山区教育数字化转型工程，旨在推动教育服务更加优质均衡，教育治理更加科学高效。因此，在教育数字基座的应用中，若涉及到为上海市社会民众提供服务（如入学入园申报、教培机构查询和报名缴费等），均需接入“随申办”对应专区，为上海市民提供便捷数字化服务。

2. 接口联调过程中提示“无访问权限”

请检查是否申请对应的接口权限。

3. 通过模板发送工作通知接口返回正常，但是账号没有收到消息

- 扫码安装应用到测试组织；
- 测试的账号要在刚才安装应用的组织内；
- 传参要用刚才安装应用的组织 corpid 生成对应的 agentid；
- 要用刚才安装应用的测试组织下的用户作为信息接收人，传参时要用此人的 userid 和所在部门 id；

检查确认下传参信息是否都对应到同一个组织，和同一个用户。

4. 接口联调时提示“不存在的授权信息”

一般提示不存在的授权信息，有以下可能，①没有安装应用到对应的组织；②传参时的组织 corpid 和当前用户所在的组织 corpid 不是同一个，具体的

要根据报错码查看原因。查看报错码的地址如下。
https://open.dingtalk.com/document/orgapp-server/server-api-error-codes-1

5. 应用安装测试过程中提示“授权超时”

一般出现这种提示，需要检查开发者的服务端代码，或重启应用服务。

6. 应用联调时提示“应用不存在”

一般出现这种情况是因为没有配置免登 url。配置免登 url 即可解决问题。