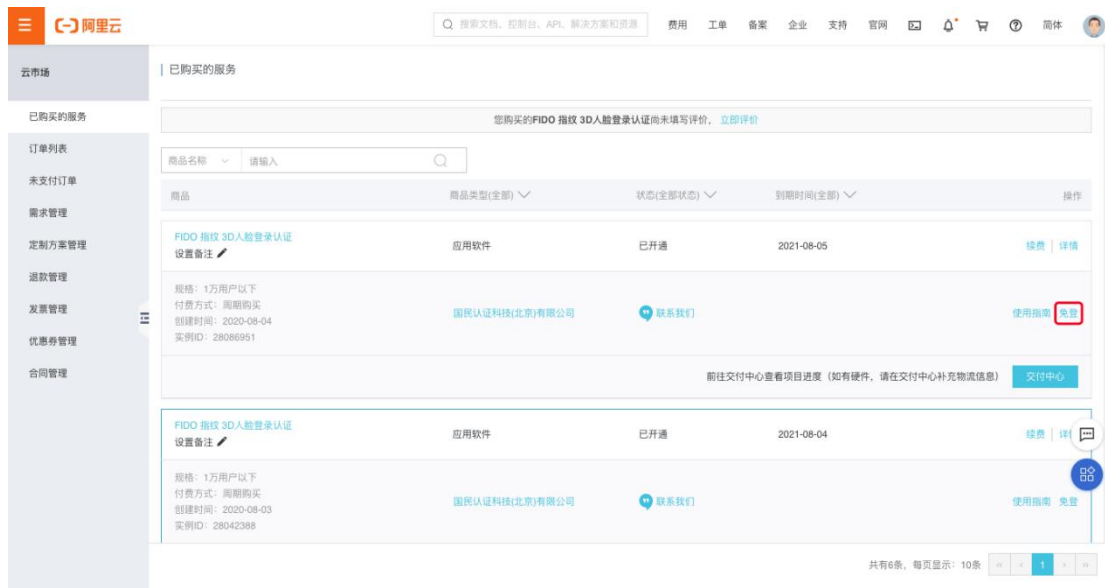


1:购买成功，进入管理控制台



2: 进入管理控制台后，点击免登，进入服务管理页面



3: 确定



4:进入管理页面



5:获取账号标识和 secret

通过控制台右上角菜单，选择账号信息



点击账号信息

开发者

账号标识:2TFodgJMN2a0EcBIF7caJIOQ

API DevSecret:lhHwYmzVnRTDw7UJHThkn0x

账号标识

查看 重置 secret

6:对接平台需要选择对应的服务, 通过点击增加服务按钮添加

服务	状态	授权次数	已用次数	授权时间
OTP认证	正常	1000	0	2020-04-16 08:47:20
OTP注册	正常	100	0	2020-04-16 08:47:20
FIDO注册	正常	100	2	2020-04-13 17:14:25
FIDO认证	正常	1000	6	2020-04-13 17:14:25

7:集成 FIDO SDK 的 APP 需要在平台登记, 用户增加应用调用的安全性, 通过增加应用按钮增加

应用名称	应用类型	应用标识	授权时间	操作
localhost	web	localhost	2020-04-16 14:05:57	编辑
ddd	android	ddd	2020-04-13 18:47:21	编辑
direct	android	android:apk-key-h...	2020-04-13 18:46:22	编辑

需要注意应用标识的填写, 应用标识的生成参考帮助

应用

一、Android app 应用标识

格式: android:apk-key-hash=<sha1_hash-of-apk-signing-cert>

备注: <sha1_hash-of-apk-signing-cert>为手机.apk签名证书的 hash 值

获取 FacetId 方式:

- 使用 keytool 或 openssl 生成<sha1_hash-of-apk-signing-cert>

```
keytool -exportcert -alias <alias of key->keystore -path of keystore | openssl sha1 -binary | openssl base64 | sed 's/=//g'
```

备注: <alias of key->是 keystore 中 key 的别名, -path of keystore->为 keystore 存放位置, 再同'android.apk-key-hash'拼接成最终 FacetId

- 在 Android 应用程序中获取

```
try {  
    PackageInfo info =  
        getPackageManager().getPackageInfo(packageNames, PackageManager.GET_SIGNATURES);  
    // packageNames 为应用程序证书, 签名后的应用名  
    byte[] cert = info.signatures[0].toByteArray();  
    InputStream input = new ByteArrayInputStream(cert);  
    CertificateFactory cf = CertificateFactory.getInstance("X.509");
```

8:企业账号可以通过用户中心查看注册的用户和停用

用户名	创建时间	操作
12345678	2020-04-16 18:53:10	停用
1234567	2020-04-16 15:25:37	停用
1234567	2020-04-16 15:21:55	停用
12344	2020-04-16 14:15:56	停用
zhaoyf	2020-04-13 18:45:09	停用

9:对于购买包年的用户，系统默认开通除了一键登录外的所有服务，授权次数为最大值



The screenshot shows a web interface for service management. The left sidebar contains navigation options: 服务信息 (Service Information), 应用信息 (Application Information), and 用户中心 (User Center). The main content area is titled '可用服务' (Available Services) and contains a table with the following data:

服务	状态	授权次数	已用次数	授权时间
OTP注册	正常	1000000000	0	2020-08-03 16:55:25
PUSH注册	正常	1000000000	0	2020-08-03 16:55:25
PUSH认证	正常	1000000000	0	2020-08-03 16:55:25
OTP认证	正常	1000000000	0	2020-08-03 16:55:25
FIDO注册	正常	1000000000	0	2020-08-03 16:55:25
FIDO认证	正常	1000000000	0	2020-08-03 16:55:25
WECHAT认证	正常	1000000000	0	2020-08-03 16:55:25
WECHAT注册	正常	1000000000	0	2020-08-03 16:55:25

At the bottom of the table, there is a pagination control showing '1' page and a '跳至' (Jump to) field.

10:集成说明以及文档，点击集成说明



11: 即可查看并下载文档

全部文档 ^

平台简介 ^

入门指南

控制台介绍

AccessToken使用

OTP v

PUSH v

Webauthn v

FIDO UAF v

小程序使用说明

FIDO2 Key v

运营商一键登录 v

手机证书 v

认证平台简介

CMAS（国民认证在线身份认证平台）是经过考验的企业级线上认证平台，每天完成认证次数上亿。开发者集成后，可以使用指纹、人脸、OTP、PUSH等认证能力，提升用户体验和系统安全。同时，CMAS提供可视化的web端控制台，提供用户管理、统计分析认证效果。CMAS全面支持Android、iOS、Windows三大硬件平台和Web端。

认证方式

CMAS提供多种认证方式：FIDO指纹3D人脸、OTP（动态口令）、Webpush、Webauthn等。

FIDO指纹+3D人脸认证

利用用户自有终端设备（包括但不限于手机、平板电脑、笔记本电脑等）中的生物识别能力（包括但不限于指纹、3D结构光人脸识别、虹膜识别等）进行APP\应用登录认证等操作。这种认证方式支持Native应用和Web应用，安全性高、体验佳。
常用于高频的登录、支付等场景，工商银行、中国银行等使用此能力进行登录、转账。
开发者参考文档：[Bio API v1](#)

OTP（动态口令）

OTP认证即一次性验证码，验证码依赖用户种子数据、当前时间。
常用于高安全应用的二次验证，谷歌账户、Github账户均采用这种能力。
开发者参考文档：[OTP API v1 message](#)

WebPush

push认证，基于用户手机存储种子数据。当用户在其它平台进行登录认证时，可以通过推送告知用户，再进行确认。
开发者参考文档：[Push API v1 message](#)