

IoT设备身份认证

用户指南

用户指南

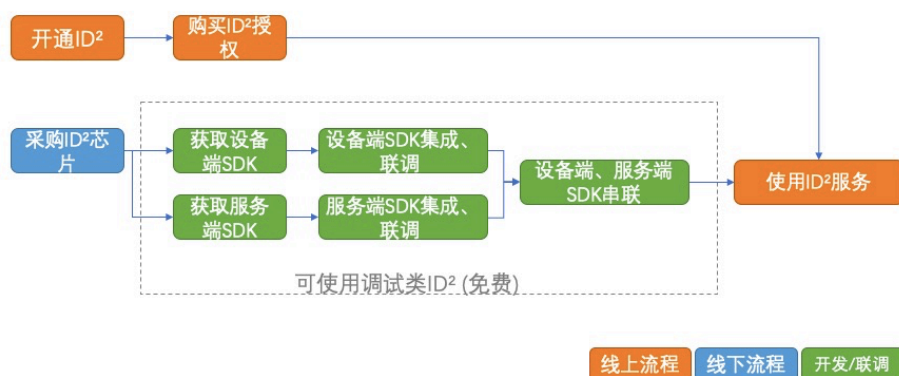
ID²使用指南

一、概述

ID²管理控制台是芯片厂商和设备厂商对ID²、产品、许可证等进行规模化管理的控制台。以下使用指南将指导设备厂商完成从企业入驻到ID²芯片使用的全部流程。

- ID²管理控制台：登陆ID²管理控制台

ID²使用流程



说明：

1. 已通过实名认证、企业认证的阿里云用户，默认为入驻审核通过，不用再次申请入驻。
2. 如果使用预置ID²，请先购买“ID²授权” 购买ID²授权(请先使用阿里云账号登录)。
3. 如果使用预烧ID²的SE安全芯片或SIM卡，需要线下采购ID²芯片或SIM卡申请获取支持ID²的安全芯片/SIM;如果使用软沙箱方案，则无需采购ID²芯片或SIM卡。

ID²开放平台需要使用阿里云账号登录，如果还没有阿里云账号，请先申请阿里云账号。

二、创建产品

进入ID²开放平台后，默认显示产品列表，您需要点击“新增产品”来创建产品。



在“创建产品”页面填写产品的真实信息，点击“确认”完成创建。其中，“产品型号”由用户自定义，不同产品型号之间的ID²授权不可串用。

创建产品

● 产品型号

0/30

芯片厂商

0/100

芯片型号

0/100

创建并购买 ID²

创建产品

1. 产品列表中的ProductKey是使用ID²服务时，调用服务端接口的必要参数。



三、购买ID²授权

建议您“先创建产品，然后再购买授权”。

创建产品的方式：进入管理控制台,点击左侧菜单栏的“使用管理->产品管理”在点击页面右上角的“创建产品”。

以下两种购买方式没有任何区别：

购买方式1：通过产品详情页的 购买按钮，进行购买。或直接点击购买ID²授权 (请先使用阿里云账号登录)进行购买。

购买方式2：通过ID²管理控制台的“购买授权”进行购买



四、使用ID²

设备端使用文档请参见：设备端对接指南

服务端使用文档请参见：服务端对接指南

使用调试类ID²

完成ID²的对接可以按照ID²管理控制台左侧菜单栏“调试服务->ID²”的指引，完成服务端、客户端的调试。了解更详细的对接说明请参见：快速入门

1. 服务端调试

1.1 获取服务端的SDK

ID²提供的服务端SDK，可以通过以下链接下载：

Java SDK

Node JS SDK

服务端SDK的对接，请参见：服务端对接指南

1.2 获取授权

调试管理->服务端调试 页面，已经提供了供您调试用的productkey。

在调试对接阶段，您可以使用这个productkey进行ID²服务端、设备端的集成，并通过服务端、设备端的验证助手进行验证。

1.3 服务端接口验证

为了验证您服务端对接是否已经完成，您可以在服务端调用 verify 接口。接口返回 code 值为 200 表示服务端接口调试成功。

2. 设备端调试

为了简化调试，针对设备端使用了SE的载体类型，提供了一个轻量化的调试SDK。通过该开源地址，您可以在集成了SE芯片的设备上，对ID²接口进行适配和自主调试。下载：[ID² SDK开源地址](#)

设备端的集成和完整对接（包含硬件适配、ID²业务对接），我们提供了统一的设备端安全SDK，支持多种载体类型（SE、SIM、KM、TEE等），请参见：[设备端 对接指南](#)

如果您底层硬件适配过程中遇到问题，请您使用钉钉搜索群(群号：23147118)或扫描页面最下方的二维码获取技术支持。

问题反馈

如果您在调试对接阶段，遇到任何问题且现有文档没有解决您的问题，请您使用钉钉搜索群(群号：23147118)或扫描下方二维码加入钉钉群获取技术支持。



Scan the QR Code to Join the Group

服务端对接指南

服务端SDK获取

您需要下载并集成适合您业务平台的服务端SDK。我们提供的SDK：

Java SDK

Node JS SDK

购买ID²授权

如果您还没有购买ID²授权，请先购买ID²授权。购买ID²授权

AccessKey生成

1. 您需要在阿里云账号下生成AccessKey，该账号必须与ID²管理控制台、购买ID²授权的账号保持一致。
 2. AccessKey生成帮助文档：[AccessKey生成](#)
-

接口调试（基于sample code）

接口说明，参见官网文档：[服务端API手册](#)

依赖包安装：参考sample code中的Readme，安装依赖包及SDK

参数填充：

- ID2参数：使用设备端调试所用的ID²
- authCode参数：使用设备端接口生成的有效authCode
- productKey参数：从ID²开放平台的产品列表中获取

运行sample code。

服务端API手册

更多服务端API信息，请参见[服务端API手册](#)

设备端对接指南

适配设备端的安全SDK

设备端安全SDK是打包集成了阿里云IoT在设备端的安全框架和安全组件，通过统一的OSA和HAL接口，以便适配到不同的系统和平台。目前已经支持Android，Linux，AliOS Things，如果您希望在更多的设备类型上集成和使用这套安全SDK，请与我们联系。

IoT设备端安全SDK V1.0 核心能力

- ID²的设备端SDK。
- 轻量化安全连接协议iTLS,基于ID²进行双向认证和会话密钥的协商，提供兼容mbed TLS的接口。
- SecureStorage (SST) 基于ID²设备主密钥派生出存储密钥，加密保护敏感数据。
- DevicePasswordManagement (DPM) 基于ID²主密钥派生的共享密钥，提供基于时间戳的动态密码服务。
- 设备端烧录 (Prov) SDK，用于集成到设备烧录程序中，在产线生产阶段，提供设备密钥的预制和预制结果检测功能。

设备端 安全SDK下载

设备端SDK	版本号	发布时间	适用环境	下载链接
安全SDK	V1.0	2019-04-23	Android: armv5 armv7 armv8	下载
安全SDK	V1.0	2019-04-23	Linux: x86 x64	下载
安全SDK	V1.0	2019-04-23	AliOS Things: 3060 3080	下载

对接ID²的接口

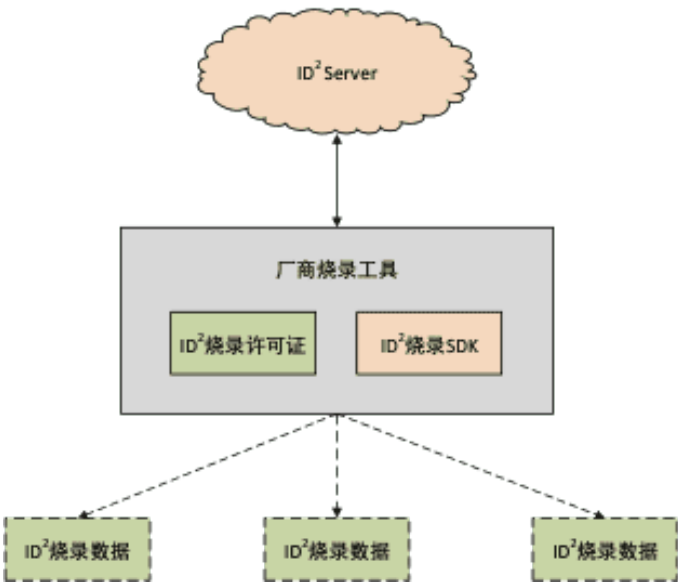
完成IoT设备端安全SDK的适配后，可以对接和验证ID²的接口。ID²设备端接口说明参见：[设备端对接 API](#)

产线烧录SDK使用指南

ID²产线烧录SDK

1，ID²产线烧录SDK介绍

ID²产线烧录SDK是由阿里开发和维护，提供给合作厂商，用于集成到厂商烧录工具，用于将ID²烧录数据拉取到PC端。



ID² 烧录SDK Release Package：

目录	说明	备注
inc	头文件	
lib	库文件, 许可证和日志配置文件	log.conf: 配置日志路径和级别 licenseConfig.ini:烧录许可证和私钥
sample	示例代码	SDK的接口使用示例，可用于调试和测试
genkeypairs.jar	RSA1024公私钥对生成工具	
ReleaseNotes.txt	发布说明	

2，产线烧录SDK 接口说明：

2.1 ds_stat_t ds_init(ds_cfg_t *cfg)

功能：初始化烧录SDK，只需启动时做一次

参数：指定烧录工具支持同时烧录的设备数和许可证文件路径

返回：成功 - DS_STATUS_OK；失败 - 参考错误码

2.2 ds_stat_t ds_create_dev(ds_dev_t *dev)

功能：创建烧录数据的句柄

参数：数据的句柄

返回：成功- DS_STATUS_OK；失败- 参考错误码

2.3 ds_stat_t ds_get_rec_num(ds_dev_t dev, uint32_t *num)

功能：获取record的数量

参数：dev -数据的句柄; num – record数量

返回：成功- DS_STATUS_OK；失败- 参考错误码

2.4 ds_stat_t ds_get_rec(ds_dev_t dev, uint32_t rec_idx, void _rec, uint32_t _size)

功能：通过dev句柄获取知道index对应的record数据和record的大小

参数：当rec == NULL时，size返回指定index的record的大小

当rec != NULL时，rec返回指定index的record数据

返回：成功- DS_STATUS_OK；失败- 参考错误码

2.5 ds_stat_t ds_set_dev_prov_stat(ds_dev_t dev, ds_dev_prov_stat_t prov_stat)

功能：烧录工具通过dev句柄设置的烧录状态

参数：烧录状态

返回：成功- DS_STATUS_OK；失败- 参考错误码

2.6 void ds_destroy_dev(ds_dev_t dev)

功能：注销烧录数据

2.7 void ds_cleanup(void)

功能：对应ds_init,用于烧录退出时的清理操作

ID² Client SDK对接SE/MCU

ID² Client SDK对接SE/MCU

代码模块关系

ID² Client SDK各个部件的关系如下：

抱歉，请登录内网获取此图片权限。

场景一：SE安全芯片厂商基于《ID² 安全应用指令规范》来实现的情况下，仅需要根据SE芯片去适配SE驱动层的接口(se_open_session/se_transmit/se_close_session)，接口实现参见：《SE芯片驱动API文档》。

场景二：SE/MCU芯片厂商自定义的通讯规范（并不遵循ID²安全应用指令规范），可以直接通过实现SE硬件抽象层的接口完成和SE芯片的通信。接口实现参考：《IROT硬件抽象层接口文档》

配置选项说明

SE芯片厂商在移植好SE芯片驱动后，需要根据SE芯片所支持的算法类型做配置，以确保正确的代码执行流程

ID2模块配置

security/include/id2/id2_config.h

配置项	支持的选项	备注说明
CONFIG_ID2_KEY_TYPE	ID2_KEY_TYPE_AES ID2_KEY_TYPE_3DES ID2_KEY_TYPE_RSA ID2_KEY_TYPE_SM1 ID2_KEY_TYPE_SM4	选择ID2服务使用的SE芯片的密码算法类型
CONFIG_ID2_HASH_TYPE	ID2_HASH_TYPE_SHA256 ID2_HASH_TYPE_SM3	选择ID2服务的散列算法 注：SM3是由SE芯片来计算的，而SHA256是通过icrypto算法库来实现的。因此SM3必须由SE芯片支持

SE驱动配置

se_driver/chip_config.h

配置项	支持的选项	备注说明
CONFIG_CHIP_TYPE	CHIP_TYPE_SE_STD_CMD	符合ID2安全应用指令规范的命令
	CHIP_TYPE_SE_MTK_CMD	厂商自己实现的SE命令(MCU等)
CONFIG_CHIP_KEY_TYPE	ID2_KEY_TYPE_AES ID2_KEY_TYPE_3DES ID2_KEY_TYPE_RSA ID2_KEY_TYPE_SM1 ID2_KEY_TYPE_SM4	选择SE芯片对应的密码算法 注：该配置必须和上面 CONFIG_ID2_KEY_TYPE的选择 保持一致。