

阿里云

IoT设备身份认证 我是芯片厂商或模组厂商

文档版本：20210518

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.芯片厂商入驻流程	05
2.芯片厂商或设备厂商对接流程	15
3.申请ID ² 烧录许可证	17
4.自主验证	20
5.产线审核	22

1.芯片厂商入驻流程

安全芯片接入平台（以下简称接入平台）为安全芯片厂商提供了流程化的芯片接入系统，提供相关验证工具、SDK、文档模板，保障安全芯片可以高效、高质量的接入阿里云IoT安全生态。本文为您介绍芯片厂商入驻流程。

接入平台需使用阿里云账号登录。如果您还未申请阿里云账号，请访问[阿里云官网](#)申请账号。

安全芯片接入流程



步骤一：芯片企业入驻

1. 登录[安全芯片接入平台](#)。
2. 在入驻页面填写企业的真实信息，单击**确认提交**。

安全芯片接入平台

test_per****@aliyun.com

欢迎安全芯片厂商加入ID²大家庭，为了给您的企业提供更完善的服务，我们需要您提交如下信息，并点击确认。

* 企业名称：请输入企业名称 0/30

* 企业法人代表：请输入企业法人代表 0/30

* 载体类型：请选择载体类型

* 联系人：请输入联系人 0/30

* 联系电话：请输入11位手机号码

* 联系地址：请输入联系地址 0/50

企业灯牌：请输入企业灯牌 0/30

* 电子邮箱：请输入电子邮箱 0/30

* 企业简介：请用150个以内文字，简单描述您的企业在芯片行业的实力，例如企业规模、销售渠道等。 0/150

确认 取消

说明

3. 如果您已经在ID²的控制台入驻过烧录者角色，接入平台会自动跳过这一步。

4. 通知您的阿里云IoT接口人，阿里云IoT会在3个工作日内进行入驻审核，请您耐心等待。



5. 入驻信息审核通过后，当您再次进入接入平台时，会显示审核通过页面，表明您已经成功入驻。单击进入管理平台开始安全芯片的接入流程。



步骤二：新增芯片型号

- 1.在左侧导航栏选择芯片接入管理 > 芯片列表，单击新增芯片。
- 2.在新增芯片页面填写安全芯片的相关信息，可参照本文下方的《附录：安全芯片信息填写指南》，填写完成后单击提交。

安全芯片接入平台

test_per****@aliyun.com

芯片接入管理

芯片列表

产线列表

下载列表

芯片列表 > 新增芯片

1 填写芯片信息

2 获取验证工具并验证

3 提交验证报告

* 芯片型号:

请填写芯片型号

0/30

* 芯片类型:

请选择芯片类型

* 芯片内核:

请选择芯片内核

* 芯片主频:

最低值

0/10

KHz

~

最高值

0/10

KHz

* 接口类型:

请选择接口类型,支持多选

* RAM大小:

请填写RAM大小

0/10

KB

* EEPROM大小:

请填写EEPROM大小

0/10

KB

* FLASH大小:

请填写FLASH大小

0/10

KB

* 算法资源:

请选择算法资源,支持多选

* 安全工作温度:

请选择安全工作温度

* 存储寿命:

请选择存储寿命

* 软件平台:

请填写软件平台,如XXXCOS_1.0, Linux_4.0等

0/30

* 安全资质:

请选择安全资质

* 芯片价格 [10万片起]:

请填写芯片价格,如: 8.01

元/片

* 芯片价格 [50万片起]:

请填写芯片价格,如: 8.01

元/片

* 芯片价格 [100万片起]:

请填写芯片价格,如: 8.01

元/片

提交

3.单击获取验证工具并验证。下载Demo App、安全功能测试工具，进行芯片验证。

说明

请参考安全功能测试工具压缩包内的ID²测试工具使用说明和ID²固定密钥验证进行验证。

安全芯片接入平台

test_per****@aliyun.com

芯片接入管理

芯片列表

产线列表

下载列表

芯片列表 > 新增芯片

1 填写芯片信息

2 获取验证工具并验证

3 提交验证报告

请下载Demo App、安全功能测试工具，进行芯片验证，您也可以返回芯片列表

Demo App

点击下载

安全功能测试工具

点击下载

下一步

返回列表

4.单击下一步，在提交验证报告页面，分别单击下载验证日志模板和下载验证报告模板。填写模板信息后，分别单击验证日志和验证报告后的重新上传，上传验证日志和验证报告。



单击提交审核。提交审核后，请通知您的阿里云IoT接口人并等待审核。审核通过后，芯片接入完成。



5.验证日志和验证报告全部上传之后，您需要等待阿里云IoT的审核，请通知您的阿里云IoT接口人。审核通过后，芯片即完成了接入流程。

步骤三：新增产线

您可以新增多条产线，每条产线需要选择一款芯片进行产线的烧录验收。验收审核过后，该产线可以为其他芯片提供烧录。

步骤四：产线烧录

经过以上流程，芯片和产线已经达到了阿里云IoT安全芯片的准入标准且认证通过。
请参考[申请ID²烧录许可证文档](#)，在[物联网设备身份认证](#)中申请烧录许可证进行芯片的正式烧录。

附录：安全芯片信息填写指南

芯片类型

类型	说明
AP	高性能应用处理器（如ARM Cortex-A系列芯片），具有一定的硬件算法能力。

类型	说明
AP-TEE	高性能应用处理器（如ARM Cortex-A系列芯片），且具有TrustZone或等同TrustZone安全属性。
MCU	中等性能中等功耗的M系列芯片，支持轻量级安全操作系统（如ARM Cortex-M系列新品）。
MCU-TEE	安全MCU，具有硬件加密引擎并具有一定的安全存储能力（如ARM Cortex v8-M），可确保密钥不出硬件。
Secure Element	具有高安全计算环境和高安全存储环境。
SIM	符合GSM系列规范且封装为SIM类型的SE芯片。
TPM	可信模块。
其他	其他符合安全芯片定义的芯片。

芯片内核

类型	说明
51系列	嵌入式51内核单片机，主要有51核和加强版251核。
ARM Cortex-A系列	具有高处理性能，主要面向手机、平板、车机、无人机等。
ARM Cortex-M系列	具有安全加密引擎CryptoEngine，可进行安全隔离加解密运算，并能存储一定长度的密钥。
ARM Cortex-R系列	ARM Cortex-R系列芯片。
ARM SecurCore系列	具有安全内核的安全芯片，如SC000。
Intel x86	具有SGX安全能力的芯片。
RISC-V	RISC-V内核系列，C*Core系列。

类型	说明
MIPS	MIPS内核。
其它	其它。

芯片主频

安全芯片的主频由芯片厂商自主填写，关键信息有：

- 最低正常工作主频率。
- 最高正常工作主频率。

类型	说明
低频	工作最高主频<40 MHz。
中频	工作最高主频<256 MHz。
高频	工作最高主频>256 MHz。

接口类型

芯片接口类型主要有：

- 传统接口
- 主流接口
- 未来支持接口

类型	说明
ISO7816	传统接口，主要用于接触式智能IC卡行业。
ISO14443	传统接口，主要用于非接触式IC卡行业。
SWP	传统接口，主要用于NFC扩展IC卡行业，以NFC-SIM电信卡居多。
UART	传统接口，串口。
I ² C	主流接口。

类型	说明
SPI	主流高速接口。
USB	传统接口，主要用于USB通讯类产品。
I ³ C	未来接口，I ² C的演进接口。

存储空间

存储空间分为两类：

- 易失性存储RAM。
- 非易失性存储ROM，EEPROM，FLASH。

存储空间按照可用性划分，如下表格。

易失性存储说明：

类型	说明
低端	可用空间大小 <16 KBytes。
中端	可用空间大小 <64 KBytes。
高端	可用空间大小 >64 KBytes。

非易失性存储说明：

类型	说明
低端	可用空间大小 <128 KBytes。
中端	可用空间大小 <512 KBytes。
高端	可用空间大小 >512 KBytes。

安全算法

类型	说明
随机数	真随机数协处理器。
MD5	MD5摘要算法。
SHA-1	SHA-1摘要算法。
SHA-2	SHA-256、SHA-384、SHA-512摘要算法。
SHA-3	SHA3摘要算法。
SM3	国密摘要算法SM3。
3DES	3DES-112、3DES-168对称算法。
AES	AES-128、AES-256对称算法。
RSA	RSA1024~RSA2048非对称算法。
ECC	椭圆曲线算法，通常为256位。
SM2	国密椭圆曲线算法，算法长度256位。
SM4	国密对称加密算法。
SM7	国密对称加密算法。
SM9	国密非对称数字标识算法。

工作温度

类型	说明
消费级	芯片稳定工作温度区间 -25°C~+85°C。

类型	说明
工业级	芯片稳定工作温度区间 -40℃~+125℃。

存储器可靠性

类型	说明
消费级	可靠存储10年，可重复擦写10万次以上。
工业级	可靠存储10年，可重复擦写50万次以上。
车规级	可靠存储10年，可重复擦写100万次以上。

芯片封装

由芯片厂商自行填写，常用的安全芯片封装规格有QFP，QFN，DFN等，如QFN8，QFN32等。

系统软件平台

类型	说明
TPM	无
Native C Platform	无
JavaCard Platform	JC2.1/JC2.2/JC302/JC304/JCxxx
Global Platform	GP2.1/GP2.2/GP2.3/GP2.x
MultiApplication Platform	无
FreeRTOS	无
Linux	无
AliOS	无

类型	说明
自定义类型	无

安全资质

类型	说明
ICA L1	支持至少一种硬件安全算法和一定安全抗攻击能力。
ICA L2	等同于FIPS140- 2 L2。
ICA L3	等同于CC EAL4+， 商密二级。
ICA L4	等同于CC EAL5+， 商密三级。

2.芯片厂商或设备厂商对接流程

本文档介绍芯片厂商烧录ID²的流程。

芯片厂商或设备厂商烧录ID²流程图



步骤一：申请ID²烧录许可证

操作项	适用范围
申请ID ² 烧录许可证	芯片厂商或模组厂商烧录ID ² 前的准备工作。

步骤二：设备端适配

请根据ID²的载体类型，选择最适合您的操作文档。

操作项	适用范围
使用AliOS Things对接ID ² -SE	芯片厂商
使用第三方OS对接ID ² -SE	芯片厂商
使用AliOS Things对接ID ² -KM	模组厂商
使用第三方OS对接ID ² -KM	模组厂商

步骤三：烧录ID²

请根据ID²的载体类型，选择最适合您的操作文档。

操作项	适用范围
烧录ID ² 到芯片	芯片厂商
烧录ID ² 到模组	模组厂商

步骤四：自主验证

操作项	适用范围
自主验证	已经对接完服务端、设备端的ID ² 用户。

步骤五：产线审核

操作项	适用范围
产线审核	已经完成烧录对接和产线验证，申请产线烧录ID ² 的资质。

3. 申请ID²烧录许可证

本文介绍申请ID²烧录授权许可证的流程。

请您注册阿里云账号并完成个人实名认证后，再进行下面的操作。建议您使用阿里云账号申请入驻。

请单击下面的链接了解详细内容：

- [阿里云账号注册流程](#)
- [个人实名认证](#)

步骤一：申请开通产线烧录管理或芯片入驻管理

1. 登录[物联网设备认证](#)。
2. 在左侧导航栏选择扩展服务 > 我的服务。
3. 单击芯片入驻管理或产线烧录管理后，填写信息。

 说明 阿里接口人请填写与您联系的阿里云IoT小二姓名，如果没有可以不填。

4. 单击确定，提交申请并等待审核。
5. 当您通过审核后，即可看到芯片入驻管理或产线烧录管理页面。

步骤二：下载产线烧录SDK

1. 在左侧导航栏选择扩展服务 > 芯片入驻管理 > 工具列表。
2. 在工具列表页面下载配套相应产线的SDK。

 说明 目前SDK支持SE（安全芯片）、TEE、Secure MCU、软件沙盒等载体类型，包含Java和C两种编程语言的SDK。

3. 下载产线SDK并解压。

ID² SDK Release Package包括以下文件。

文件	说明
sdk-lib	ID ² SDK的库文件。
sdk-sample	示例代码。
genkeypairs.jar	用于生成产线公私钥对的工具。

步骤三：生成产线公私钥

在安装有Java环境的PC机上运行公私钥对生成程序，并获取keypairs.txt文件中的公私钥对。

```
java -jar genkeypairs.jar > keypairs.txt
```

公私钥对信息如下图所示。

```
1 Generate key pair:
2 pubKey:
3 MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQkiGzEhCZEFUzbGHCE
4 privKey:
5 MIICdQIBADANBgkqhkiG9w0BAQsF3zwwC
```

注意 请务必妥善保存密钥，产线烧录环节会使用pubKey拉取ID²。

步骤四：获取ID²烧录许可证

- 1. 在左侧导航栏选择扩展服务 > 产线烧录管理。
- 2. 在产线烧录管理页面，单击产线管理页签。
- 3. 单击新增产线。
- 4. 在新增产线对话框，填写产线信息后，单击确定提交。

新增产线

产线名称

请输入产线名称

芯片型号

请输入芯片型号

载体类型

请选择载体类型

操作系统类型

请选择操作系统类型

操作系统版本

请输入操作系统版本

确定

取消

参数	说明
产品型号	实际的产品或设备的型号。
芯片型号	芯片的完整型号。
载体类型	SE、TEE、KM等。
操作系统类型	按照设备实际运行的操作系统信息来填写。
操作系统版本	按照设备实际运行的操作系统信息来填写。

- 5. 在左侧导航栏选择扩展服务 > 产线烧录管理。
- 6. 单击新增许可证，打开新增许可证弹窗，填写信息后，单击确定提交。

新增许可证

产线

ID2测试产线2

公钥

请填写厂商公钥

0/2048

密钥类型

RSA-1024

申请配额

请填写申请配额，不大于100万

备注

请输入备注

0/100

确定

取消

参数	说明
产线	从已经创建的产品中选择。
公钥	厂商公私钥对中的公钥。 公私钥对生成方法，请参见 步骤三：生成产线公私钥 。
密钥类型	根据实际产品密钥类型选择。
申请配额	填写要烧录的ID ² 数量，单次烧录不超过100万个。

4. 自主验证

本文介绍如何使用设备端适配验证工具完成ID²全链路的调试验证。

前提条件

- 已在设备端上集成安全SDK。获取安全SDK，请访问[ID² Client SDK](#)。
- ID²数据已烧录到设备上。若还未完成烧录，请参考[烧录ID²到芯片](#)。
- 已获取ID²认证授权。购买ID²认证授权，请访问[ID²认证授权-预付费](#)。

步骤一：使用设备端适配验证工具验证ID²

完成ID²设备端适配后，可以通过ID²设备端适配验证工具验证ID²的设备认证和解密功能。设备端适配验证工具适用于不同的载体（如TEE，SE，MCU），流程如下图。



1. 获取设备端调试工具。
2. 编译生成自主验证的固件（id2_app）。
3. 将自主验证的固件烧录到设备。

调试结果如下图。

```
===== ID2 Validation Json Message =====
{
  "reportVersion": "1.0.0",
  "sdkVersion": "2.0.0",
  "date": "Aug 26 2019 17:02:06",
  "testContent": [
    {
      "api": "id2_client_get_id",
      "args": {
      },
      "result": "000F[REDACTED]9100"
    },
    {
      "api": "id2_client_get_challenge_auth_code",
      "args": {
        "challenge": "55B8[REDACTED]33DC",
        "extra": "abcd1234"
      },
      "result": "2-2-BC[REDACTED]mazr+kyHiAPbviICs6//C4i/ciSU6rEupdmisx"
    },
    {
      "api": "id2_client_get_timestamp_auth_code",
      "args": {
        "timestamp": "1512022279204",
        "extra": "abcd1234"
      },
      "result": "3-2-B0EF[REDACTED]2FS72To//C4i/ciSU6rEupdmisx"
    }
  ]
}
```

步骤二：在服务端验证调试结果

1. 登录[物联网设备身份认证](#)。
2. 选择扩展服务 > 设备端验。
3. 在设备端适配验证页面单击验证调试结果，将设备端生成的调试结果粘贴在验证调试结果对话框。
4. 单击验证，开始设备端适配验证。
5. 验证完成后，在完成验证对话框查看验证结果。

步骤三：在设备端解密

1. 获取服务端生成的密文。
请在步骤二：在服务端验证调试结果描述的完成验证对话框中复制密文。
2. 在设备端导入密文。

```

/* Copyright (C) 2017-2019 Alibaba Group Holding Limited
*/

#include "id2_dev.h"

/* Hex String, getting from id2 console */
#define ID2_CIPHER_DATA "44444444444444444444444444444444"

int main(int argc, char *argv[])
{
    int ret;
    uint32_t cipher_len = 0;
    char *cipher_data = ID2_CIPHER_DATA;

    if (argc >= 4) {
        if (strcmp(argv[1], "set_data") == 0) {
            cipher_data = argv[2];
        }
    }

    ret = id2_client_unit_test();
    if (ret < 0) {
        ID2_DBG_LOG("id2 client unit test fail!\n");
        return -1;
    }

    cipher_len = strlen(cipher_data);

    ret = id2_client_generate_authcode();
    if (ret < 0) {
        ID2_DBG_LOG("id2 client generate authcode fail!\n");
        return -1;
    }

    cipher_len = strlen(cipher_data);
    if (cipher_len > ID2_ID_LEN * 4) {
        ret = id2_client_decrypt_data(cipher_data, cipher_len);
        if (ret < 0) {
            ID2_DBG_LOG("id2 client decrypt data fail!\n");
            return -1;
        }
    }

    return 0;
}

```

3. 在设备端进行解密验证。

- i. 重新编译生成固件 (id2_app)。
- ii. 烧录固件到设备。
- iii. 运行固件，进行解密验证。

```

"args": {
  },
  "result": "000F .....9100"
}, {
  "api": "id2_client_get_challenge_auth_code",
  "args": {
    "challenge": "5588 .....33bc",
    "extra": "abcd1234"
  },
  "result": "2-2-C4B .....Eco2//C4i/cisU6rEupdmisx"
}, {
  "api": "id2_client_get_timestamp_auth_code",
  "args": {
    "timestamp": "1512022279204",
    "extra": "abcd1234"
  },
  "result": "3-2-C4B .....rp8+a//C4i/cisU6rEupdmisx"
}]
}

<LS_LOG> id2_client_cleanup 579: [id2_client_cleanup enter.]
<LS_LOG> id2_client_generate_authcode 186: =====>ID2 Client Generate AuthCode End.

<LS_LOG> id2_client_decrypt data 202: ===== ID2 Client Test Decrypt Start.
<LS_LOG> id2_client_init 556: [id2_client_init enter.]
<LS_LOG> ID2 Client Version: 0x00020000
<LS_LOG> ID2 Client Build Time: Aug 27 2019 10:18:30
<LS_LOG> -----
<LS_LOG> CONFIG ID2_DEBUG is defined!
<LS_LOG> CONFIG ID2_OTP is defined!
<LS_LOG> CONFIG ID2_KEY_TYPE: ID2_KEY_TYPE_AES
<LS_LOG> -----
<LS_LOG> id2_client_get_id 606: [id2_client_get_id enter.]
<LS_LOG> id2_client_get_id 649: ID2: .....
<LS_LOG> id2_client_decrypt 700: [id2_client_decrypt enter.]
<LS_LOG> id2_log_hex_dump 99: id2 cipher input: [length = 0x0020]
<LS_LOG> id2_log_hex_dump 109: 85 C8 1E C6 21 94 E5 44 1F C0 09 EC AA 16 BE
<LS_LOG> id2_log_hex_dump 109: BC AE 76 B0 3E 86 AA EA B7 67 37 FD 95 D2 4E 05
<LS_LOG> id2_log_hex_dump 99: id2 cipher output: [length = 0x0020]
<LS_LOG> id2_log_hex_dump 109: 30 30 30 46 46 46 46 46 45 41 45 44 46 44 46 34
<LS_LOG> id2_log_hex_dump 109: 31 33 37 44 39 31 30 30 08 08 08 08 08 08 08 08
<LS_LOG> id2_sym_cipher 154: id2 cipher pkcs5 unpadding.
<LS_LOG> id2_client_decrypt data 262: =====>ID2 client Test Decrypt Pass.

```

5.产线审核

本文介绍产线审核流程。

1. 登录[安全芯片接入平台](#)，在左侧导航栏选择芯片接入管理 > 产线列表，然后单击新增产线。



2. 在填写产线信息页面中填写产线的实际信息，并选择一款芯片，填写芯片的相关测试数据，单击提交。

产线列表 > 新增产线

1 填写产线信息 2 获取烧录工具 3 提交产线报告

⚠ 小贴士：芯片型号、厂商公钥、密钥类型和测试配额，是用于测试产线的测试数据

• 产线类型：请选择产线类型

• 产线工厂名称：请填写产线工厂名称 0/30

• 产线资质：请选择产线资质

• 芯片型号：请选择芯片型号

• 厂商公钥：请填写厂商公钥 0/512

• 密钥类型：请选择密钥类型

• 测试配额：请填写测试配额 0/5

• 联系人：请填写 2/20

• 联系电话：请填写

提交 返回列表

3. 在获取烧录工具页面，下载产线SDK，进行产线烧录测试。测试完成后，单击下一步。如果您已经完成了烧录的测试，请跳过此步骤。

产线列表 > 新增产线

1 填写产线信息 2 获取烧录工具 3 提交产线报告

⚠ 小贴士：请下载相应的产线SDK，进行产线烧录测试。您也可以稍后从“下载列表”下载

产线 SDK for SE 点击下载

产线SDK for其它平台（如TEE、Secure MCU、软件沙盒等）点击下载

下一步 返回列表

4. 在提交产线报告页面，上传产线报告、产线Checklist和产线照片（产线照片非必传）。上传之后，请通知您的阿里云IoT接口人，并等待审核。

产线列表 > 新增产线

1

2

3

填写产线信息

获取校验工具

提交产线报告

小贴士:

1) 请将Checklist填好并盖章后，扫描为图片添加到产线报告的Checklist一栏
2) 产线报告需要相关责任人签字并加盖公司公章后视为合法有效
产线报告和Checklist必须上传，产线照片非必填，上传成功后，请点击“提交审核”等待小二审核

产线报告:

上传文件

下载产线报告模板

产线Checklist:

上传文件

下载Checklist模板

产线照片1:

上传图片

产线照片2:

上传图片

产线照片3:

上传图片

提交审核

返回列表

说明

- 请将Checklist填好并盖章后，扫描为图片添加到产线报告的Checklist一栏。
- 产线报告需要相关责任人签字并加盖公司公章后视为合法有效。
- 若您已上传产线审核相关信息但未提交审核，可稍后在产线列表页面，找到待审核的产线，单击其操作列的提交审核发起产线信息审核。

5. 审核通过后，产线列表页面中，该产线对应的审核状态列显示审核通过。产线即开启了ID²安全芯片的烧录资质。

产线列表

产线工厂名称:

芯片型号:

产线类型: 全部

审核状态: 全部

查询

新增产线

产线类型	产线工厂名称	芯片型号	厂商公钥	密钥类型/长度	测试配额	审核状态	申请时间	操作
SecureMCU	测试产线工厂	测试芯片	ssfd	3DES-112	100	审核通过	2018-03-27 17:01:29	查看详情