IoT设备身份认证

IoT设备身份认证(ID²)

IoT设备身份认证(ID²)

什么是IoT设备身份认证(ID²)

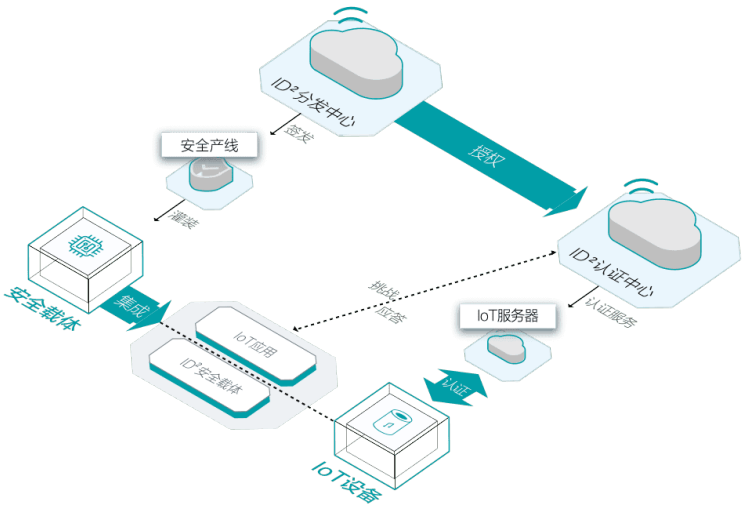
IoT设备身份认证ID²（Internet Device ID），是一种物联网设备的可信身份标识，具备不可篡改、不可伪造、全球唯一的安全属性，是实现万物互联、服务流转的关键基础设施。

- 产品特点、系统架构等介绍详见产品详情

相关概念

- IoT：物联网 IoT(Internet of things)。
- IoT设备：通过网络协议连接到物联网的设备。

产品架构



核心能力

- 身份标识：是身份信息的唯一标识。

- 身份认证：通过身份信息的标识来认证是否是一台合法的设备。
- 加密/解密：按照特定的计算方式（加密算法）将明文加密成为更加安全的密文，或者将密文解析为原始的明文。

开通使用ID²

您可以通过直接、间接的方式使用ID²提供的身份认证、加解密服务。

直接方式

- 通过ID²的控制台创建的产品，默认已开启ID²服务。

间接方式

- 通过物联网平台，创建产品时勾选ID²服务。请参见通过物联网平台使用ID²
- 通过其他业务平台，创建产品时勾选ID²服务。请参见通过其他业务平台使用ID²。

说明：通过物联网平台、其他业务平台创建产品时，如果启用了ID²服务。您可以在ID²的控制台看到相应的产品。但是通过ID²控制台创建的产品，在物联网平台、其他业务平台上不可见。

ID²的售卖方式

请参见ID²的计费方式与收费项,ID²提供两种形态：

- 软件：ID²认证授权。
- 软硬一体：ID²-安全芯片，安全芯片中已经烧录了ID²。

ID²的关联系统

ID²面向智能设备/物联网设备的生产厂商提供设备标识和认证服务，需要芯片/模组厂商的支持，为此ID²专门为芯片/模组厂商提供了入驻、烧录系统。如果您是芯片/模组厂商，可以通过ID²的关联系统完成与ID²的对接。

系统	功能	适用人群
ID²芯片厂商入驻	ID²的芯片/模组对接	芯片/模组商
ID²烧录系统	申请可以烧录的ID²，并将ID²烧录到芯片/模组中	芯片/模组商

ID²安全芯片

ID²安全芯片-规格

ID²安全芯片是集成了ID²安全能力的芯片。

安全芯片规格如下：

规格	标准版-恩智浦A71CL	标准版-紫光同芯 IOT60	国密版-复旦微 FM1280
起订量	6000片	3000片	3000片
CPU	SmartMX（Secure_MX51）	32位ARM内核SC000	32位ARM内核SC000
FLASH容量	20KB E2PROM	256KB~320KB	512KB
RAM容量	6KB	13~20KB	17.5KB
算法	对称算法： AES（128，192 and 256bits）、 DES（3DES） 非对称算法： RSA 可达2048bits 摘要算法： SHA-1、SHA-224、SHA-256	对称算法： DES/TDES、SM1、SM4 非对称算法： RSA、ECC、SM2 摘要算法： SHA-1、SHA-256、SM3	对称算法： TDES、AES、SM1、SM4、SSF33 非对称算法： RSA、ECC、SM2 摘要算法： SHA-1、SHA-224、SHA-256、SM3
外设	两个时钟 CRC16 真随机数发生器 DES，AES协处理器，RSA协处理器 安全传感器Reset	真随机数发生器 CRC引擎：16-bit CRC-CCITT DMA：数据拷贝和数据比较 3个通用定时器/计数器，1个ETU定时器	工作时钟：最高频率32MHz 真随机数发生器 1个24-Bits定时器，2个32Bits的计时器TIMERA和TIMERB CRC：支持CRC32和CRC16运算功能 看门狗模块
接口	I2C接口 SPI接口	USB接口 ISO/IEC 7816 从/主接口 UART接口 SPI主/从接口 I2C接口 PWM接口 键盘 GPIO	ISO/IEC 7816接触接口 ISO/IEC 14443-A接口 SPI接口 I2C接口
封装	SOP8	Wafer QFN32	DFN12 SOP8
ICA 安全认证	SE L1 载体L2	无	SE L3 载体L3

国际/国内 安全认证	无	无	CC EAL5+
ID² INSIDE商标	有	无	有

功能特性

ID²为IoT设备的身份标识、认证提供了以下核心服务：

身份唯一标识

为每个IoT设备提供唯一的标识信息，防止设备被篡改或仿冒。

iTLS安全协议

兼容TLS，在保障安全性的同时大幅减少IoT设备的资源消耗。

安全烧录

与合作伙伴的安全产线对接，确保密钥安全烧录到各种安全等级的载体上。

ID²的管理控制台，支持以下功能：

1，调试ID²

在正式使用ID²之前，建议您通过调试ID²完成服务端、IoT设备端的对接。这里为您提供了10个免费的调试用ID²。调试用ID²：仅供调试阶段使用，不能够在实际的业务环境中进行身份标识和认证。调试工具：在服务端调试过程中，ID²管理控制台为您提供了“设备端”的authcode生成助手，帮助您完成ID²的对接。在设备端调试过程中，ID²管理控制台模拟“服务端”的authcode验证助手，帮助您完成ID²的对接。

2，创建和管理产品

ID²管理控制台为每个产品都分配了唯一的“ProductKey”，请您妥善保管ProductKey。

3，ID²的使用统计

ID²管理控制台提供了统计和查询工具，帮助您了解某个产品/设备使用ID²进行认证的情况。包括ID²的调用次数、调用失败的次数统计。

产品优势

与现有的设备身份认证相比，IoT设备身份认证ID²具有以下优势：

支持多种安全等级的载体

提供支持SE、SIM、TEE、secure MCU、软件沙箱等多种安全等级载体。

易于适配

不依赖于物联网设备的操作系统和通信协议，能够快速完成适配。

高安全性

ID²提供了数据加解密的能力，

富认证

支持在线认证、代理认证、广播认证、离线认证

稳定可信

服务可用性99.9%

使用限制

使用ID²的前提条件

使用ID²之前，请您务必了解以下信息：

序号	说明
1	ID²是一款能够独立运行的面向IoT系统的安全产品，也可以与物联网平台搭配一起使用。
2	（推荐）搭配物联网平台使用ID²，可以获得轻量

	级安全连接(iTLS/iDTLS)。如果您需要对接物联网平台，请查看如何对接物联网平台
3	ID²是基于产品型号进行授权的，您可以在ID²管理控制台创建多个产品，但是产品之间的ID²授权额度不能共享、不能交叉使用。
4	同一个产品型号下所有的ID²，有效期必须一致。请在购买时按实际的生命周期选择相应年限的有效期。例如，产品A已经购买了1年期的ID²，那么产品A续费时只能续费1年期的ID²
5	支持的Region：目前仅支持中国-华东2区(上海)，其他Region会陆续支持。
6	基础版ID²的限制：每个ID²每天认证次数限制为10次。尽管现在超出认证次数后不会做限制，但是强烈建议您控制认证调用量。过高的、频繁的、超标的调用量在未来会受到严格的控制。