ALIBABA CLOUD

# 阿里云

## IoT设备身份认证

## 产品简介

文档版本：20220607

阿里云

# 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<br>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<br>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<br>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<br>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 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid` *Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

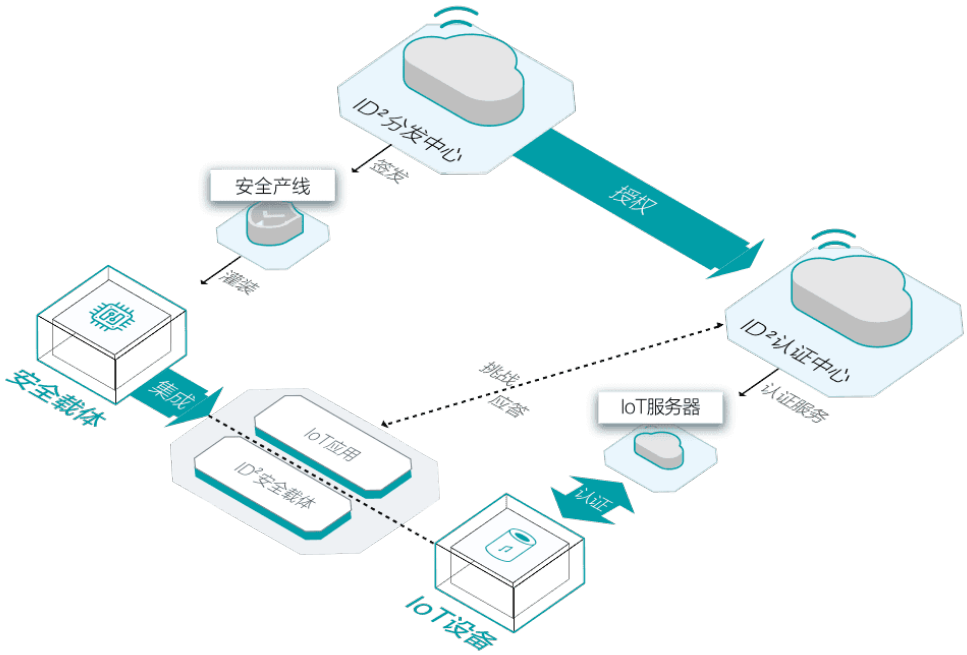
1.什么是IoT设备身份认证 05
2.ID²安全芯片规格 07
3.功能特性 09
4.产品优势 10
5.使用限制 11

# 1.什么是IoT设备身份认证

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。
- 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

- 设备身份标识：为每个IoT设备提供独立的身份标识，基于ID²提供双向身份认证服务，防止设备被篡改或仿冒。
- 安全连接：提供兼容TLS和DTLS的轻量级安全协议：iTLS/iDTLS。更适合物联网设备，在保障安全性的同时大幅减少IoT设备的资源消耗。
- 业务数据保护：基于设备可信根派生的密钥支持多种加密算法，为设备固件、业务数据、应用授权等敏感数据提供安全防护。
- 密钥管理：为IoT系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发。

## 产品特点

- 轻量化：使用ID²代替CA证书，即节省了存储空间又节省了网络资源的消耗。仅连接握手阶段就可以节省70%的网络资源消耗。
- 高安全：为IoT设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保IoT设备的合法性和数据的安全性。
- 广覆盖：适用于多种安全等级的IoT应用场景，支持不同安全等级的载体（SE、SIM、TEE、secure MCU、软件沙箱）。

## $ID^2$的关联系统

如果您是芯片/模组厂商，需要在您的芯片/模组中烧录$ID^2$，请使用以下系统。

| 系统 | 功能 | 适用人群 |
| --- | --- | --- |
| $ID^2$芯片厂商入驻 | $ID^2$的芯片/模组对接。 | 芯片/模组商 |
| $ID^2$烧录系统 | 申请可以烧录的$ID^2$，并将$ID^2$烧录到芯片/模组中。 | 芯片/模组商 |

# 2.ID²安全芯片规格

ID²安全芯片是集成了ID²安全能力的芯片。

安全芯片规格如下表。

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

| 规格 | 恩智浦A71CL（标准版） | 紫光同芯IOT60（标准版） | 复旦微FM1280（国密版） |
| --- | --- | --- | --- |
| ICA安全认证 | • SE L1<br>• 载体L2 | 无 | • SE L3<br>• 载体L3 |
| 国际或国内安全认证 | 无 | 无 | CC EAL5+ |
| ID² INSIDE商标 | 有 | 无 | 有 |

# 3.功能特性

$ID^2$为IoT设备的身份标识、认证、数据加密提供了以下核心服务。

## 设备身份认证

为每个IoT设备提供唯一的身份标识，基于$ID^2$提供双向身份认证服务，防止设备被篡改或仿冒。

## 安全连接

提供兼容TLS和DTLS的iTLS/iDTLS轻量级安全协议。该协议在保障安全性的同时大幅减少IoT设备的资源消耗，更适合IoT设备。

## 业务数据保护

基于设备可信根派生的密钥，支持多种加密算法。为设备固件、业务数据、应用授权等敏感数据提供安全防护。

## 密钥管理

对IoT系统中的设备、应用和业务使用的密钥提供集中管理，包括密钥生成、密钥销毁和端到端的密钥安全分发。

# 4.产品优势

$ID^2$具有轻量化、高安全、广覆盖的特点，适合在低功耗的物联网设备中使用。

## 轻量化

使用$ID^2$代替CA证书，既节省存储空间又可以降低网络资源消耗。仅在连接握手阶段即可降低70%的网络资源消耗。

## 高安全

为IoT设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保IoT设备的合法性和数据的安全性。

## 广覆盖

适用于多种安全等级的IoT应用场景，支持不同安全等级的载体（SE、SIM、TEE、secure MCU和软件沙箱）。

# 5.使用限制

本文介绍ID²的使用限制。

ID²是面向IoT系统且能够独立运行的安全产品，并且支持与物联网平台搭配使用。

推荐您搭配物联网平台使用ID²，即可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，并将认证方式选择为**ID²**。

使用ID²之前，请您务必了解以下使用限制。

| 限制项 | 描述 |
| --- | --- |
| 授权限制 | ID²基于产品型号授权，ID²管理控制台支持创建多个产品，但是产品之间的ID²授权额度不能共享。 |
| 有效期限制 | 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。<br>例如，产品A购买了1年期的ID²，那么续费时只能续费1年期的ID²。 |
| 地域限制 | 目前仅支持华东2（上海）。 |