

阿里云 IoT可信执行环境 TEE安全芯片

文档版本：20190819

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
	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。	 禁止： 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
<code>[]或者[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }或者{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 TEE安全芯片.....	1

1 TEE安全芯片

TEE安全芯片的规格描述如下：

特性	能力	基础版 – i.MX 6UL	标准版 – i.MX 8MMini	高级版（认证同款）- i.MX 6QP
适用场景	适用场景	TBOX,网关, 智能货柜, 二维码扫码终端, 工控安全设备, 智能音箱	车载娱乐系统, TBOX, 带屏网关, 智能货柜, 机器人, 工控, 汽车仪表盘	IVI, TBOX, 网关, 智能货柜, 二维码扫码终端, 工控安全设备
	架构	· ARMv7-A (Trustzone) · CSKY-A (TEE Extended)	ARMv8-A (Trustzone)	ARMv7-A (Trustzone)
	核心数量	单核	4核	4核
	加密引擎	· 无硬件加密引擎或少数算法支持 · 对称加密 (AES, DES) · 非对称加密 (RSA) · 摘要 (HASH, MD5, HMAC)	· 支持硬件加密引擎, 算法支持种类齐全 · 对称加密 (AES, DES) · 非对称加密 (RSA, ECC) · 摘要 (HASH, MD5, HMAC)	· 无硬件加密引擎或少数算法支持 · 对称加密 (AES, DES) · 非对称加密 (RSA) · 摘要 (HASH, MD5, HMAC)
	硬件防侧信道攻击	不支持	支持抗SPA/DPA攻击	支持抗SPA/DPA攻击
	真随机数	支持	支持	支持
	硬件隔离	· 内存安全隔离 · OTP/fuse 分区安全隔离 · 硬件安全配置	· 内存安全隔离 · OTP/fuse 分区安全隔离 · 硬件安全配置	· 内存安全隔离 · OTP/fuse 分区安全隔离 · 硬件安全配置
	硬件可信根	硬件密钥派生	硬件密钥派生	硬件密钥派生
	安全存储	可选	eMMC(RPMB)	eMMC(RPMB)
	安全启动	支持	支持	支持

特性	能力	基础版 – i.MX 6UL	标准版 – i.MX 8MMini	高级版（认证同款）- i.MX 6QP
	安全时钟	支持Secure RTC	支持Secure RTC	支持Secure RTC
	安全调试	JTAG禁用	JTAG授权调试/ JTAG禁用	JTAG授权调试/ JTAG禁用
	DDR	<=2G (DDR2, DDR3)	>=3G (DDR3, DDR4)	<=3G (DDR2, DDR3)
	存储类型	NOR, NAND, eMMC, SDCard	NOR, NAND, eMMC, SDCard	NOR, NAND, eMMC, SDCard
	外设	GPIO,SPI,I2C, USB,Ethernet	GPIO,SPI,I2C, USB,Ethernet, CAN,TSC, LCD	GPIO,SPI,I2C, USB,Ethernet, CAN,TSC,LCD



说明:

- 高级版为“获得GP全配置安全认证”的同款芯片。
- [详细了解TEE](#)