



小米消费级物联网 安全基线

2024

前言

近年来，随着科技的发展，以及消费者对智能生活日益增长的消费升级需求，物联网（IoT）设备市场也开始蓬勃发展。从产品数量来看，根据 Omdia 的研究，到 2023 年底全球物联网设备安装量接近 380 亿台，预计到 2030 年将达到 820 亿台。从 IoT 技术支出来看，IDC 的数据显示，2022 年全球物联网总支出规模约为 7,300 亿美元，预计到 2027 年将接近 1.2 万亿美元，五年复合增长率（CAGR）为 10.4%。从市场价值来看，智次方研究院的洞察显示，智能物联迈入 2.0，“通感智值一体化”融合提速，产业将启动新一轮强势增长，预计 2023 年将增长至接近 5.9 万亿元人民币，增幅 9.5%。从 IoT 设备所产生的数据来看，IDC 的预测指出，随着物联网设备的持续增长，这些设备正在产生惊人的数据量，预计到 2025 年，IoT 设备数据将达到 79.4ZB。

IoT 市场如此迅猛的增速，意味着物联网设备将迅速进入人们的日常生活并广泛应用于各种场景。不同于传统家电，消费级物联网设备具有感知物体、信息传输、智能处理的特点，其本质是互联网在用户各种生活场景的延伸，因此在方便人们生活的同时，也不可避免的会收集、传输、存储、处理大量的用户个人信息甚至个人敏感信息。国内外的监管机构与国际标准化组织也相继发布了针对 IoT 产品的安全与隐私法律法规和标准规范；与此同时，消费者对 IoT 设备的安全与隐私保护能力的要求也越来越高。

随着 IoT 设备数量和随之产生的数据急速增长，用户和监管机构对产品的安全与隐私保护关注度也日益提高，企业如何保证物联网设备的安全与隐私，让用户和监管机构放心和信赖，成为企业亟需解决的问题。

小米智能终端安全实验室根据多年的安全测试经验积累、并结合国内外法律法规和标准规范，制定了本基线指南。本指南旨在提供一个开放、便捷、可落地的知识库，帮助广大消费级物联网设备企业应对以上安全和隐私挑战。相关企业在设计和开发消费级物联网终端产品时，可以对照此指南，提前规避一些基本的安全与隐私风险，快速提升产品的安全与隐私保护能力。

范围

本基线主要描述了针对消费级物联网终端设备的安全基线要求。

规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ETSI EN303645 《消费级物联网信息安全基本要求》

Cyber Security for Consumer Internet of Things: Baseline Requirements

GB/T35273-2020 《信息安全技术 - 个人信息安全规范》

Information security technology—Personal information security specification

Regulation (EU) 2016/679 《通用数据保护条例》

General Data Protection Regulation

使用指南

使用本安全基线时，建议先通过附录 A 确定产品的安全等级，再根据产品的安全等级在附录 B 中查找对应需要满足的安全基线要求条目。在正文内容中，各安全要求的标题旁也会标注其适用的安全等级。

目 录

01 设备硬件

1.1 物理调试接口	2
1.1.1 调试接口默认关闭 [高 中]	2
1.1.2 PCB 板上调试接口丝印 [高]	3
1.1.3 调试接口默认关闭信息输入 [高 中]	3
1.1.4 调试接口打印敏感数据 [高 中]	3
1.2 本地数据存储 [高 中]	3
1.3 芯片间通信 [高]	3
1.4 安全启动 [高]	4
1.5 防物理拆除 [高]	5
1.6 防强电磁攻击 [高]	6
1.7 智能门锁锁体、锁芯及门卡 [高]	6
1.8 设备唯一标识防篡改 [高]	7

02 设备软件

2.1 软件更新	10
2.1.1 固件升级包完整性与合法性 [高 中 低]	10
2.1.2 防固件降级 [高]	10
2.1.3 软件更新失败后恢复机制 [高 中]	10
2.1.4 局域网 OTA 升级 [高 中 低]	11
2.1.5 第三方组件更新 [高 中]	11
2.1.6 设备线刷防护 [高]	11
2.2 服务与端口最小化 [高 中 低]	12
2.3 代码库管理 [高 中 低]	12
2.4 正式版本组件管理 [高 中 低]	12

03 设备 OS

3.1 通用 OS	16
3.1.1 Bootloader 启动 [高 中]	16
3.1.2 用户账户密码（有登录 UI） [高中低]	16

3.1.3 防暴力破解 [高中低]	16
3.1.4 验证输入数据 [高中低]	17
3.1.5 特权功能接口 [高中]	17
3.2 嵌入式 Linux OS	17
3.2.1 串行端口绑定 SHELL [高中]	17
3.2.2 系统默认账户密码 (无 UI 登录) [高]	18
3.2.3 基础文件系统权限 [高中]	18
3.2.4 外部存储的程序和脚本 [高中]	18
3.2.5 地址空间布局随机化 [高中]	18
3.2.6 基址随机加载保护 [高中]	19
3.2.7 栈 Cookie 防溢出 [高中]	19
3.2.8 栈不可执行 [高中]	19
3.2.9 删除调试符号表 [高中低]	19
3.3 Android	19
3.3.1 通用 Android 版本 [高中低]	19
3.3.2 Android ADB 鉴权方案 [高中]	20
3.3.3 Android Webview 版本限制 [高中]	20

04 设备通信

4.1 通用通信	22
4.1.1 密钥生成与用途限制 [高中]	22
4.1.2 通信传输安全保护 [高中低]	23
4.1.3 通信双向认证 [高中低]	23
4.1.4 防重放 [高中]	24
4.1.5 非授权通信协议限制 [高中低]	24
4.1.6 未绑定状态的受控指令限制 [高中低]	25
4.1.7 系统配置防泄漏 [高中]	25
4.1.8 敏感指令来源限制 [高]	25
4.2 以太网和无线网络	26
4.2.1 以太网通信信道保护 [高中低]	26
4.2.2 HTTPS 证书校验 [高中低]	26
4.2.3 Wi-Fi 接入点口令 [高中]	26
4.2.4 Wi-Fi 接入点用途 [高中]	27
4.3 蓝牙	27
4.3.1 蓝牙协议版本 [高中低]	27
4.3.2 蓝牙配对 [高中低]	27
4.3.3 蓝牙广播 [高中低]	27

4.3.4 蓝牙控制指令合法性校验 [高 中 低]	28
4.3.5 蓝牙敏感信息通信 [高]	28
4.3.6 芯片原厂未鉴权指令防护 [高 中 低]	28
4.3.7 蓝牙广播防追踪机制 [高 中 低]	29
4.3.8 蓝牙 Mesh 协议 [高 中 低]	29
4.4 Zigbee	29
4.4.1 Zigbee 协议版本 [高 中 低]	29
4.5 Sub 1G 射频	30
4.5.1 射频通信数据包序列号长度 [高 中 低]	30
4.5.2 通信密钥硬编码 [高 中]	30
4.5.3 通信频率 [高]	30

05 数据安全和隐私

5.1 加密与哈希算法 [高 中 低]	32
5.2 随机数生成函数 [高 中]	32
5.3 日志上报 [高 中 低]	32
5.4 跨境网络请求 [高 中 低]	33
5.5 服务端数据存储安全 [高 中 低]	33
5.6 服务端数据删除功能 [高 中 低]	33
5.7 恢复出厂设置 [高 中 低]	33

06 业务逻辑

6.1 设备可绑定状态 [高 中 低]	36
6.2 绑定确认 [高]	36
6.3 防重复绑定 [高 中 低]	36
6.4 强绑定关系 [高]	36
6.5 设备分享权限及鉴权 [高]	37
6.6 密码输入防偷窥 [高]	38
6.7 指纹识别解锁 [高 中]	38
6.8 人脸识别解锁 [高 中]	38
6.9 报警事件管理 [高 中 低]	39
6.10 设备传感器说明 [高 中 低]	39
6.11 设备日志安全监控 [高 中 低]	39
6.12 安全设置指南 [高]	40
6.13 演示模式 [高]	40

术语和定义.....	41
缩略语.....	45
附录 A 产品安全等级	46
附录 B 产品安全等级与安全要求对应表	48
附录 C 敏感信息定义与举例	51
附录 D 硬件选型重点关注	53
附录 E 修订记录	54



01

设备硬件

1.1 物理调试接口

1.1.1 调试接口默认关闭【高中】

消费级物联网设备（下文简称“设备”）存储或生成密钥的 MCU/SoC 和控制设备关键功能的 MCU/SoC 应关闭用于功能调试目的调试接口，减少不必要的物理调试接口暴露，以避免出厂后的调试指令控制篡改、芯片内置 flash 数据读写等非必要的控制和信息传输，具体要求如下：

- PCB 设计：在设备 PCB 设计时应仅保留实际开发测试过程中需要的物理调试接口，非必要的物理调试接口不应从芯片引脚引出。
- 设备固件：设备正式版本固件默认关闭 UART、JTAG、SWD、ADB 等调试接口。如因售后问题分析等原因需开启调试接口，应按需经过认证鉴权后开启或对设备进行特殊操作后才能使用。

常见的 MCU/SoC 调试接口关闭 & 鉴权方式：

- 永久关闭：根据 MCU/SoC 的芯片技术手册，在芯片 efuse 烧录对应的安全配置字段，一次性永久关闭调试接口。
- 鉴权开启：根据 MCU/SoC 的芯片技术手册，在芯片 efuse 烧录一机一密密码，维修线刷时由售后人员登录账号密码从云端拉取设备刷机密码，在线刷工具输入并验证该密码正确后才可进行线刷。如上述云端鉴权方案无法实现，应采取安全的调试接口鉴权 / 加密方案，如使用私有 USB Dongle 串接使用进行鉴权加密等。调试接口鉴权开启方案应经过安全评估。

低安全等级设备还可采用以下鉴权方式：

- 飞线通联：调试接口从芯片引出到 PCB 上的调试接口节点，且节点不与设备外部的物理接口连接，需要调试时使用导线焊接到 PCB 的调试节点使调试接口电路通联。
- 特殊操作：根据设备传感器的能力，设置一定的特殊操作开启接口调试能力，如特殊按键组合、设备倾斜通电等。

1.1.2 PCB 板上调试接口丝印 [高]

设备应去除 PCB 板上的调试接口丝印 (如明显的 TX、RX、UART、JTAG、SWD、ADB)，以防止逆向工程。

1.1.3 调试接口默认关闭信息输入 [高中]

调试接口因某些特定需要而开启后，默认不应开放调试接口的信息输入，防止设备固件被篡改或本地存储的敏感信息被读取。

1.1.4 调试接口打印敏感数据 [高中]

调试接口因特定需要而开启后，log 输出的信息中不应包含用户与设备敏感信息 (敏感信息包含敏感安全参数如 key、token，和个人敏感信息如 password、Wi-Fi 密码等，详见附录 A 个人敏感信息)，如需输出完整数据流日志，需要将此类信息遮蔽展示 (如：password: *****)。

1.2 本地数据存储 [高中]

- 储存加密：设备应将敏感信息加密存储在存储芯片 (flash、nand、emmc 等)，加密方案可通过采用集成具备数据加密能力的安全芯片、TEE 或操作系统分区加密来实现。
- 防篡改：设备用于存储保护、传输保护和鉴权的公私钥、证书等需要防止被篡改的敏感信息，除加密存储外，应存储在设备不可被外部篡改的分区内，如 flash 只读分区、安全芯片或 TEE 中。

1.3 芯片间通信 [高]

门锁等对设备芯片间通信保密性和完整性要求高的产品，设备芯片间通信 (包括但不限于 UART/IIC/SPI/USB 等协议) 传输的所有信息应进行加密。

- 1) 一芯一密 / 一机一密：设备关键芯片应通过芯片间设备每次上电时协商一芯一密密钥，若部分关键芯片能力不支持密钥协商，可预置一机一密密钥。

- 2) 芯片加密通信：关键芯片之间完成密钥协商后，芯片间的所有通信都应经过鉴权和加密，不应执行未加密的指令。采用对称 / 非对称加密均可。
- 3) 密钥保护：关键芯片之间的通信密钥应被加密保护以防止被芯片外部读取
- 4) 芯片通信防重放攻击：关键芯片间通信应使用防重放机制，可通过加密的帧计数器或加密的时间戳校验。
- 5) 敏感信息最小化：关键芯片间传输的敏感信息应最小化和摘要化。如传输指纹 / 掌纹 / 指静脉及人脸的摘要能够满足需求，就不应传输指纹 / 掌纹 / 指静脉及人脸原图。

可参考以下方案：

- 宜采用安全芯片（SE）或可信执行环境（TEE）来确保加密密钥的安全性，并结合安全芯片真实与伪数据融合发送的机制，以防止攻击者通过硬件通道嗅探得到协商密钥以及芯片指令。国内外已有多家成熟的安全芯片厂商可供选择，也可选用支持 OP-TEE、ARM Trustzone 或 Android Trusty TEE 等成熟 TEE 方案的 SoC 作为设备主芯片，并在 TEE 内实现敏感信息加解密和密钥管理等功能。

注：OP-TEE 请参考：<https://www.trustedfirmware.org/projects/op-tee/>，ARM Trustzone 请参考：<https://www.arm.com/technologies/trustzone-for-cortex-a>，Android Trusty TEE 请参考：<https://source.android.com/docs/security/features/trusty?hl=zh-cn>

- 对于未集成安全芯片和不支持可信执行环境的设备，设备关键 MCU 之间首次上电后宜互相协商通信密钥（芯片间通过串口 ECC 生成公私钥对，计算临时密钥，生成随机数和挑战值，验证挑战值，验证通过后使用 LTK 做鉴权密钥），并存储在外部没有访问权限的存储分区（协商密钥方案对硬件能力要求较高，厂商可根据实际情况评估）。

1.4 安全启动 [高]

设备芯片宜支持安全启动（SecureBoot 原理如图），启动时对固件（U-Boot、Kernel、Rootfs）或 Flash 关键分区（如固件程序所在分区）进行合法加载校验，确存储芯片中的系统合法性和完整性校验通过后才能正常启动。

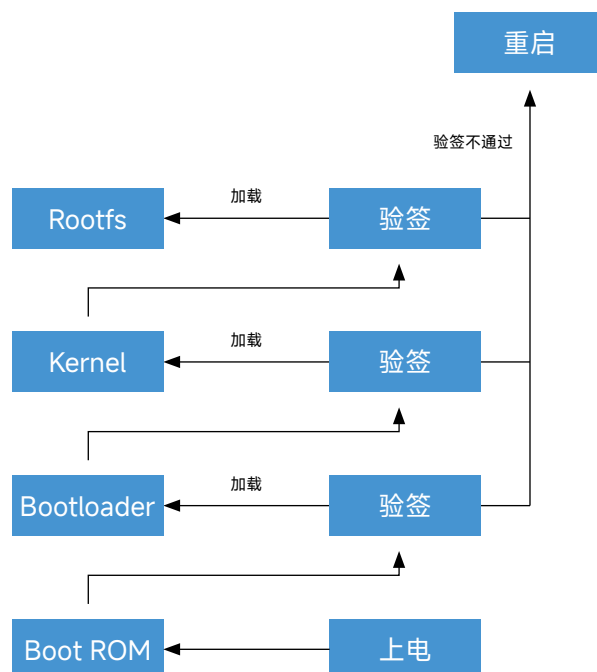


图 1 - 安全启动

1.5 防物理拆除【高】

高安全等级设备（仅门锁，门铃，室外摄像机）应具备在受到暴力移除或拆卸时的防护或预警机制：

- 外壳防拆除：设备不应暴露可以将设备部分或全部拆除的螺丝孔或卡扣，设备室外外壳宜采用一体式结构设计。如因业务需要必须暴露螺丝或卡扣的，应采用非常用类型固定螺丝来固定设备，并使用高强度环氧树脂等结构胶对外壳螺丝封胶防护，以防止设备从室外不使用破坏性工具即可被拆除。
- 电子组件结构防护：设备具有控制功能的电子组件（包括但不限于 MCU，接口，线路）应具有足够强度的结构保护，如把此类电子组件设计在设备的室内部分，防止设备室外外壳被拆除后直接暴露。
- 拆除警报：如设备传感器具备检测设备被拆解的能力，应发出警报铃声，记录并上报拆除事件至设备管理员。

1.6 防强电磁攻击〔高〕

高安全等级设备（仅门锁、保险箱）应在芯片外加装电磁防护罩，以防止强电磁脉冲（EMP）攻击造成的设备逻辑或运行异常，进而导致逻辑错误，设备宕机或电路烧毁（门锁 / 保险箱类 设备遭遇强电磁攻击后可导致非授权开锁）。

1.7 智能门锁锁体、锁芯及门卡〔高〕

智能门锁的开锁传动机构应具备结构防护措施，以防止攻击者通过敲击门锁面板进行异常开锁，或在破坏门锁外面板后，通过转动开锁传动机构的方式绕过锁芯进行劫持开锁，以及通过控制开锁电机电平实现开锁的风险。不同锁体和插芯结构的智能门锁应分别符合以下锁芯及锁体要求：

- 锁芯要求：智能门锁产品应采用真插芯，并宜使用 C 级锁芯，以防止锁芯被暴力开启或使用专用工具（如已有专业开锁工具）进行开锁。
- 锁体要求：
 - 半自动锁体 / 全自动锁体：应将开锁电机和离合组件放置于锁体内部，锁体外部应仅暴露锁芯和方轴套，且不应暴露离合器、离合块。
 - 机械锁体：背包电机的门把手传动方钢的外露部分应设计为不可轻易物理转动的圆柱体。
- 锁体硬件安全：

需使用内置游离式离合器从而做到防技术开启和被暴力破解。锁芯密钥量（> 30000（GA-T 73-2015-5.7.2 C 级）；> 30000（GA374-2019- 5.12.3 B 级））、互开率（≤ 0.01%（T-T73-2015-5.7.2 C 级））均符合或高于国家标准中锁芯的最高安全标准。
- 门卡：

支持门卡开锁方式的智能门锁应使用 CPU 卡作为开锁门卡，不应使用易被嗅探、破解复制的 ID 卡或 M1 卡开锁。

注：CPU 卡是指具备以下特征的卡片：动态数据加密的智能卡，内置微处理器（CPU），拥有独立的操作系统和内存，可以存储复杂的数据和程序。

表 1 - 门卡安全性

卡类型	优点	缺点	推荐
CPU 卡	安全性高，用户空间大， 读取速度快	价格稍贵	推荐使用
ID 卡	价格便宜	容易复制，安全性低	不应使用
M1 卡	可读可写	易被嗅探、破解并复制， 价格稍贵	不应使用

1.8 设备唯一标识防篡改 [高]

设备唯一标识符指用于识别或验证设备身份合法性的唯一标识符，如 SN、IMEI、Device ID 等，设备唯一标识被篡改可导致设备伪造，导致隐私泄露等风险。设备端应把设备唯一硬件标识存储在设备不可被篡改的存储区域，如

- 中、低安全等级产品可通过一次性编程把三元组烧录在模组或 MCU 的 efuse 作为唯一标识（对于小米模组，无需厂商额外配置；对于厂商自采模组，厂商需联系原厂将三元组烧录在自采模组或 MCU 的 efuse 中）。
- 高安全等级产品，使用安全芯片或 TEE 存储等技术防止被篡改。

The background of the slide is a light blue gradient. It is decorated with a repeating pattern of faint, orange-outlined icons representing various electronic devices. These icons include smartphones, tablets, laptops, desktop monitors, speakers, and other peripherals, arranged in a scattered, overlapping manner.

02

设备软件

2.1 软件更新

2.1.1 固件升级包完整性与合法性 [高中低]

设备固件升级（OTA 远程或本地升级）前应先对固件包进行完整性哈希得到固件包摘要，再使用公私钥方式对摘要进行合法性签名和验签，确认升级包完整性与合法性再进行更新，以防止固件包被篡改或替换。

固件升级包完整性哈希应采用安全的哈希算法（详见 5.1 加密与哈希算法），完整性凭据应在设备与服务端的加密通信通道内传输。

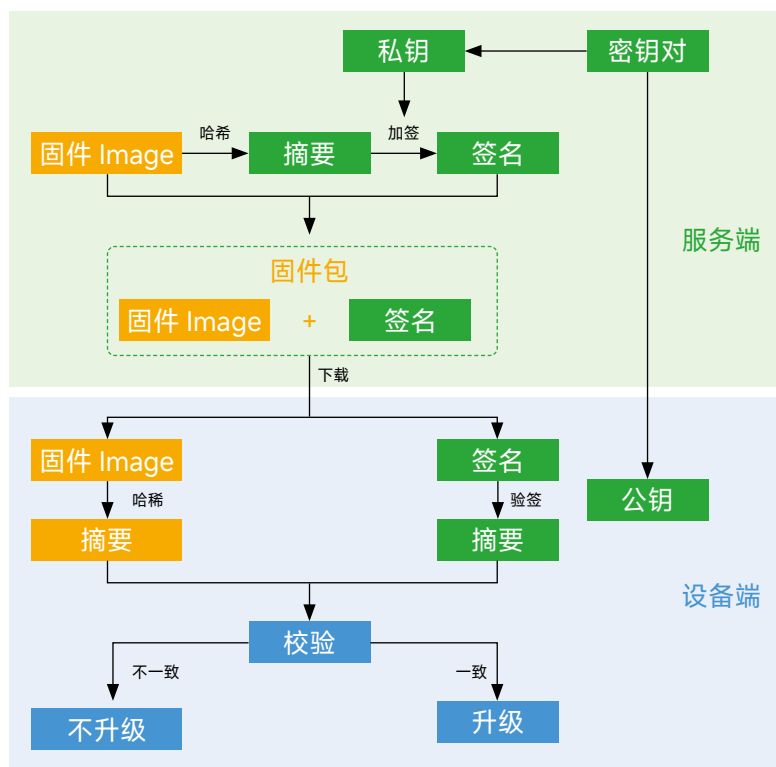


图 2 - 固件升级包合法性与完整性校验

2.1.2 防固件降级 [高]

设备 OTA 升级、SD 卡升级等用户版本支持的固件更新功能，应拒绝旧版固件更新，以防止旧版本可能存在的历史 BUG 或安全风险重新暴露被利用。特殊需求下（如：测试、维修等），可以经过鉴权后开启调试接口线刷或经过鉴权的开启降级 RPC 指令等方式对固件验签后刷机。

2.1.3 软件更新失败后恢复机制 [高中]

设备软件更新时可能遇到断电等特殊情况，导致设备升级失败。因此设备应具备 OTA 双分区备份机制，保障升级失败时能恢复到可用软件版本，防止升级失败损害设备可用性。

2.1.4 局域网 OTA 升级 [高中低]

设备应默认关闭局域网 OTA 升级能力，如需开启应满足 2.1.1 固件升级包完整性与合法性要求，以防止攻击者通过局域网对设备进行恶意固件 OTA 升级。

2.1.5 第三方组件更新 [高中]

设备制造商在产品开发过程中应维护产品软硬件的第三方商用及开源组件清单，并将其用于持续监测已识别的软硬件组件的相关安全。

设备使用到的第三方软件 / 库 / 开源代码应使用最新版本，不应使用老旧或已停止维护的版本，不应使用无 licence 或来源不明的代码或库，如特殊需求不能使用最新版本，应经过安全评估。在明确安全漏洞的情况下，应及时更新到最新修复版本。

注：软件 / 库漏洞可前往：<https://www.cvedetails.com/product-list.php> 查询。

2.1.6 设备线刷防护 [高]

设备正式出厂版本应关闭线刷功能，如售后等强需求需要支持线刷，应对线刷过程进行鉴权。

设备线刷主要分为 IAP (In Application Programming)、ISP (In System Programming) 和 ICP (In Circuit Programming)，根据设备支持的不同线刷方式，应满足以下两项要求之一：

- IAP 线刷：此类设备的系统在线刷时仍在运行，设备具备对线刷固件进行验证的能力。因此，支持 IAP 线刷的设备 MCU/SoC 应具备安全更新机制，如设备对线刷传入的固件包进行签名验证，或封装专用的 USB Dongle 对 MCU/SoC 的 IAP 过程进行数据加密或签名验证，仅允许验证通过的固件通过线刷刷入，以避免 MCU/SoC 固件逻辑被篡改的风险。
- ICP/ISP 线刷：通过线刷工具直接刷写存储芯片，设备的线刷工具应具备完善的对线刷操作人员的鉴权机制，如：设备的调试接口默认关闭，线刷时需使用线刷工具与设备鉴权打开调试接口进行线刷。这类线刷工具生成调试接口鉴权密钥的算法不应是纯本地的，应结合向云端请求获取到的设

备相关信息共同生成调试接口鉴权密钥。

2.2 服务与端口最小化 [高 中 低]

- 高风险服务与非必要端口：设备应默认关闭 FTP、SSH、Telnet、HTTP、ADB 等高风险管理服务或信息数据服务，如需开启应经过安全评估，也应关闭非数据交互与控制实现所必要的 IoT SDK 控制服务端口。
- 设备端口协议：设备局域网端口应使用 IPv4 协议，互联网如非业务必要应关闭 IPv6 协议，防止局域网端口在 IPv6 协议开放导致可被互联网访问；设备互联网端口应按照业务功能需求选择使用 IPv4 或 IPv6 协议，如设备无 IPv6 协议使用需求应关闭 IPv6 协议，防止非预期的互联网 IPv6 访问。

注：Android 系统在开放端口时会默认同时在局域网和互联网开放，对于仅需要在局域网开放的端口应更改为仅在局域网开放。

2.3 代码库管理 [高 中 低]

设备相关代码库不应在未经允许的情况下上传至 Github、Gitee 等公用代码仓库或百度网盘等公开、半公开服务，防止源代码泄露。

2.4 正式版本组件管理 [高 中 低]

设备应严格区分使用的小米 SDK、设备固件的版本类型，正式固件应基于用户或 Release 版本编译，不应使用开发调试或 Debug 版本编译正式版本，防止开发调试或 debug 版本中存在的特权接口、调试和产测等功能引入安全风险；同时设备使用的三方组件不应有 6 个月未处置的高危与严重漏洞。

针对高安全等级产品，用户或 Release 版本固件中不允许存在产测代码，以避免留存后门等相关风险。如产线产测完成，应通过上位机或设备自身清除产测代码（如图 4- 清除产测代码）

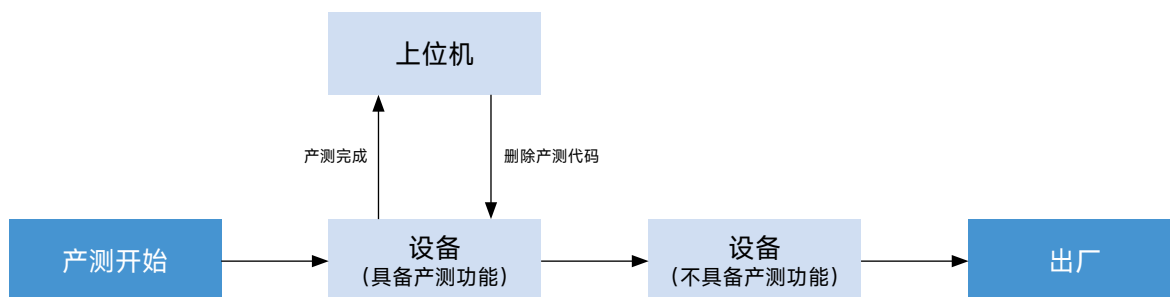


图 4 - 清除产测代码

通用方案：用户或 Release 版本判断方式：

- 通用模组版本可在获取小米 IoT 模组页面查看。

注：小米 IoT 开放平台模组页面请参考：<https://iot.mi.com/new/doc/tools-and-resources/module?keywords=1.0.0>

- 二次开发模组版本可在申请模组资源后在对应 Gitlab 链接内的 Release Note 查看，未在 release note 中的版本为非正式版本。

注：如 ESP32 GitLab：<https://partner-gitlab.mioffice.cn/miot/bsp/miot-esp32-sdk>

- 非小米 SDK/ 模组的组件版本请与对应供应商确认或在 SDK 代码库官网确认。

The background of the slide is a light beige color with a repeating pattern of various electronic devices. These include smartphones, tablets, laptops, smart speakers, and other IoT devices, all rendered in a simple, orange-outlined icon style. The devices are scattered across the entire background, creating a textured, thematic effect.

03

设备 OS

3.1 通用 OS

3.1.1 Bootloader 启动 [高中]

设备 Bootloader 不应在系统启动前预留中断时间，Delay 需设置为 0，防止通过修改启动参数进入 Shell 界面获得设备控制权。

当设备操作系统引导加载程序（Bootloader/U-Boot）在启动中发生异常，设备应自动重启，避免暴露操作系统引导和加载控制台（Console）界面，防止攻击者通过错误植入进入控制台界面并获得篡改设备启动参数的权限，进而控制设备。

3.1.2 用户账户密码（有登录 UI）[高中低]

对具有用户注册 / 登录界面的设备，如果用户注册 / 登录设备的用户账户 / 管理后台预置了默认密码，则该密码应为随机生成且一机一密的高强度密码，并在用户首次登陆时强制要求修改默认密码；如果设备不为用户注册 / 登录设备的用户账户 / 管理后台预置默认密码，则设备应要求用户注册或首次登录时自行设置高强度密码。

门锁开锁密码：针对门锁开锁密码，锁端和插件端均应支持弱密码检测（至少应保证检测相同数字和连续递增、连续递减数字密码。）

注：高强度密码：长度为 10-14 位，包含大写字母、小写字母、符号和数字其中三类字符的密码。

3.1.3 防暴力破解 [高中低]

- 通用品类：需要在设备端登录密码的设备（如路由器、门锁、电视、投影仪、带屏音箱等），其登录密码应具备防暴力破解机制，如验证码等人机交互机制、登录验证失败递增等待时间和登录验证失败超过一定次数锁定账号等。锁定账号后，用户通过身份认证后应重置设备端密码，不应以明文形式直接展示原始密码，防止密码泄露或同一账号下多设备撞库等情况。用于累计登录验证失败次数的计数器应严格计算，防止通过按取消键可绕过计数等情况。
- 门锁品类：未授权的所有技术认证手段（包含但不限于数字钥匙、PIN 钥匙、生物钥匙）在 5min 内连续错误输入次数累计之和达到 5 次后，锁端应给出报警提示信息，同时锁端应自动进入无效输入状态且至少持续 90s。

3.1.4 验证输入数据 [高 中 低]

设备应验证通过用户界面或 API 接口输入的数据，以防止设备执行外部恶意攻击代码。

数据验证方法包括但不限于：过滤超出处理范围的数据、过滤和转义非预期的数据类型，及部署 Fuzz 工具检测程序是否存在输入数据验证不足而出现的潜在漏洞等。

3.1.5 特权功能接口 [高 中]

设备应默认关闭可直接修改设备固件或配置的特权接口（如工厂 OTA、未公开功能接口、调试后门等），如业务强需求需要在出厂后的版本仍保留特权功能接口，应参照以下方案制定严格的鉴权加密方案，并经过安全评估。

- 1) 开启调试接口鉴权，方式可参考 1.1.1;
- 2) 维修线刷鉴权，方式可参考 2.1.6;
- 3) 设备芯片间通信特权指令：

对于永久关闭了调试接口的 MCU/SoC，在售后返厂等业务场景，如需通过设备正常的片间通信协议发送特权指令开启厂测等功能，特权指令鉴权加密方案应满足要求：

- 应与设备进行鉴权后加密通信传输特权指令，相关鉴权加密和特权指令应封装在工厂上位机内，防止泄露。
- 鉴权过程应进行鉴权失败次数统计，5 分钟内鉴权失败超过 5 次应临时禁止该鉴权，等待 1.5 分钟或设备重新上电后才能再次允许鉴权，防止爆破。

3.2 嵌入式 Linux OS

3.2.1 串行端口绑定 SHELL [高 中]

设备不应将系统 SHELL 绑定在 UART 等串行调试接口，防止通过接线获取设备控制权。如有特殊需要，需满足 3.2.2 要求。

3.2.2 系统默认账户密码（无 UI 登录）[高]

嵌入式 Linux 系统默认用户（如 root、admin 等）需设置高强度密码，并保证一机一密，不应在代码中为所有设备写入相同密码或空密码。

注：高强度密码：长度 10-14 位，包含大写字母、小写字母、符号和数字其中三类字符的密码。

3.2.3 基础文件系统权限 [高中]

设备嵌入式 Linux 的基础文件系统（如 /etc/ 等存有启动项的目录）应使用只读文件系统（如 squashfs、cramfs），以防止攻击者在篡改运行状态的操作系统。

注：由于 squashfs 不具备 flash 坏块处理机制，如果 NAND flash 设备的 OTA 等功能对坏块处理能力要求较高，可使用 UBI 文件系统，并且把设备根目录配置为只读，也满足安全要求。

3.2.4 外部存储的程序和脚本 [高中]

设备嵌入式 Linux 操作系统默认不应运行外部存储（SD 卡、U 盘、网络存储等）中程序或脚本。如有特殊需要，应进行公私钥签名验证，以防止系统被植入恶意软件或脚本。

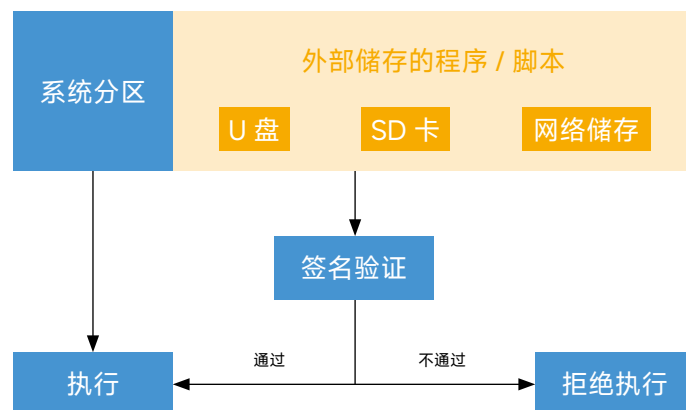


图 5 - 外部程序和脚本签名验证

3.2.5 地址空间布局随机化 [高中]

嵌入式 Linux 系统的设备应开启地址空间布局随机化（ASLR）保护措施，以防止缓冲区溢出。

开启方法：在 `/etc/sysctl.conf` 中添加 `kernel.randomize_Va_space = 2` (Kernel $\geq 2.6.12$) 参数 2 代表除了库与栈外，堆也进行随机化保护，但需要注意，ASLR 不负责代码段以及数据段的随机保护，该项工作需要通过编译器 PIE 实现，参见：3.2.6

3.2.6 基址随机加载保护 [高中]

应用应开启 PIE 应用基址随机加载保护选项。

开启方法：gcc 编译参数 `-pie -fPIE`（注意大小写），同时需要系统 ASLR 支持，参见：3.2.5

3.2.7 栈 Cookie 防溢出 [高中]

在编译 Linux 程序代码时，应开启 Linux 程序的 CANARY 栈溢出保护选项。

开启方法：添加 gcc 编译参数 `-fstack-protector-all`

3.2.8 栈不可执行 [高中]

在编译 Linux 程序代码时，应开启 Linux 程序的 NX 栈不可执行保护选项。

开启方法：添加 gcc 编译参数 `-z noexecstack`

3.2.9 删除调试符号表 [高中低]

在编译 Linux 程序代码时，需使用 Strip 函数删除调试符号表，以提升逆向分析难度并减少程序体积。

3.3 Android

3.3.1 通用 Android 版本 [高中低]

通用 Android 设备应使用 8.0 及以上安全稳定版本，并在明确安全漏洞的情况

下及时更新到最新修复版本。

注：软件 / 库漏洞可前往：<https://source.android.com/docs/security/bulletin?hl=zh-cn>

3.3.2 Android ADB 鉴权方案 [高 中]

ADB (Android Debug Bridge) 是一种多功能命令行工具，包含客户端、守护进程、服务器三大组件，可以用来操作 Android 设备。

开启 ADB 需保障客户端与服务端通过密钥协商的方式，建立安全通信连接后访问目标设备。

3.3.3 Android Webview 版本限制 [高 中]

为避免被 v8 引擎漏洞影响，应当升级至最新的 Webview 版本（根据相关公开 CVE 漏洞信息，建议升级至 117 及以上版本）。

部分产品可能存在兼容性问题，则至少应按照下表升级到该安卓版本发布时对应的 Webview 版本。

表 2 - Android Webview 版本限制

安卓版本	Webview 版本	发布日期
8.0 (API level 26)	Chromium 63	2017-08
8.1 (API level 27)	Chromium 68	2017-12
9.0 (API level 28)	Chromium 69	2018-08
10 (API level 29)	Chromium 75	2019-09
11 (API level 30)	Chromium 81	2020-09
12 (API level 31)	Chromium 93	2021-10
12L (API level 32)	Chromium 93	2022-03
13 (API level 33)	Chromium 101	2022-08
14 (API level 34)	Chromium 120	2023-05

注：当前建议使用的最低版本为 117 版本。建议使用的最低版本要求将随安卓版本更新而更新。

04

设备通信

4.1 通用通信

4.1.1 密钥生成与用途限制 [高中]

- 密钥生成：设备不应该使用硬编码在代码中的密钥用于鉴权或传输被保护的关键安全参数，应采用一机一密 PSK 或通过 PSK 密钥结合设备 SN、MAC、salt 等其他信息导出等方式生成密钥，防止通过固件逆向得到批量设备的传输安全保护或鉴权密钥。

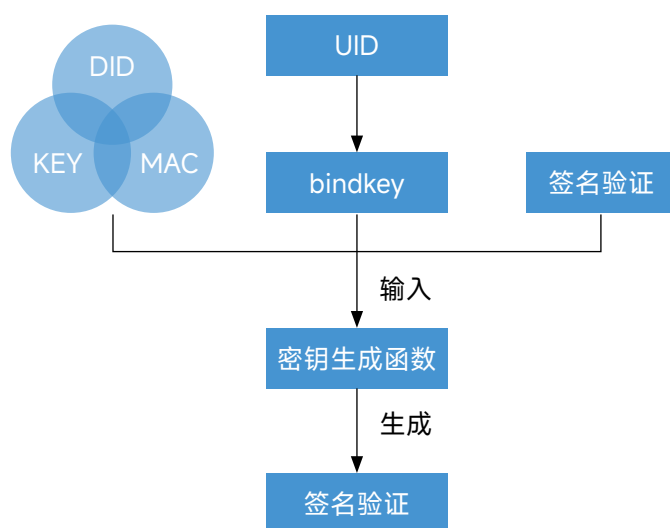


图 6 - 密钥生成

- 密钥用途：设备传输加密或鉴权的密钥应避免用于多种用途，如设备与 APP 在首次连接时的绑定鉴权密钥应仅用于绑定鉴权目的，鉴权通过后的传输会话密钥应使用绑定鉴权密钥结合随机数等其他信息导出的长期密钥来进行推衍。

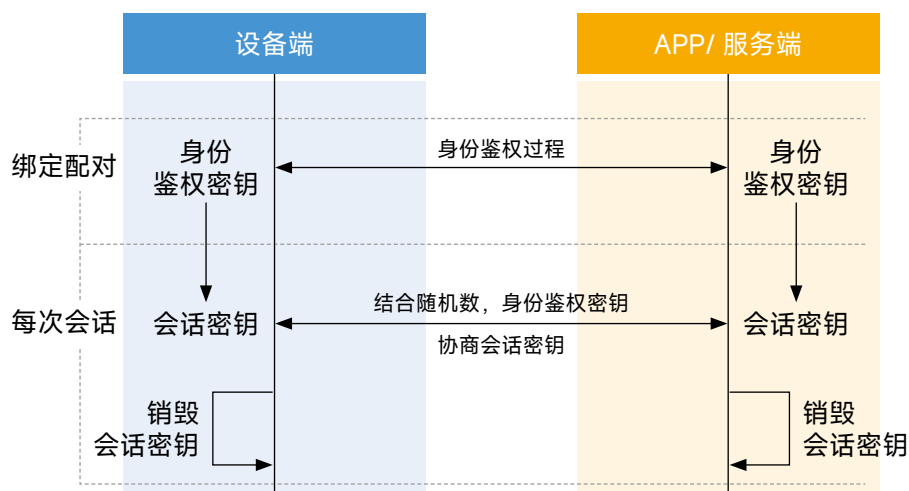


图 7 - 密钥用途

4.1.2 通信传输安全保护 [高中低]

- 通信信道保护：传输敏感信息字段的设备应对与其他设备、应用和服务端通信的信道进行加密和完整性保护，并在会话结束时及时销毁会话密钥。针对不同通信方式的加密方案可参考 4.2, 4.3, 4.5。通用方案：模组 /SDK 的控制信令通道已默认进行了加密。使用最新版本的模组 /SDK 即可满足此要求。
- 敏感信息加密：设备应对与其他设备、应用和服务端通信中传输的个人敏感信息、特殊类型的个人信息和关键安全参数字段（如身份证号、私钥和密码等）使用额外的安全加密算法进行加密传输。

注：加密算法的安全性可参考 5.1 加密与哈希算法；敏感信息、个人敏感信息、特殊类型的个人信息、关键安全参数等详细定义见：敏感信息定义

4.1.3 通信双向认证 [高中低]

设备通信时应在数据传输之前进行双向认证，验证双方真实身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制。设备应使用以下列举的米家标准双向认证通信协议，如因特殊原因需使用非标准协议的，应经过安全评估。



图 8 - 安全芯片

- 设备验证服务端：

以太网设备通过米家 OTS 协议（基于 TLS/DTLS）与服务端通信时会先向 CA 校验服务端证书是否合法。

蓝牙设备通过米家蓝牙安全认证协议绑定流程中的 OOB 信息验证服务端 / APP 是否合法。
- 服务端验证设备：

中、低安全等级设备：服务端通过校验设备的身份标识信息如三元组，判断设备身份是否合法。

高安全等级设备：服务端通过验证设备安全芯片或 TEE 中存储的设备唯一证书判断设备身份是否合法。

4.1.4 防重放 [高中]

设备通信应使用滚动码或计数器机制，当请求操作计数大于设备计数才准许设备执行该操作指令，以防止他人通过抓包重放控制请求来对设备进行非授权的控制。

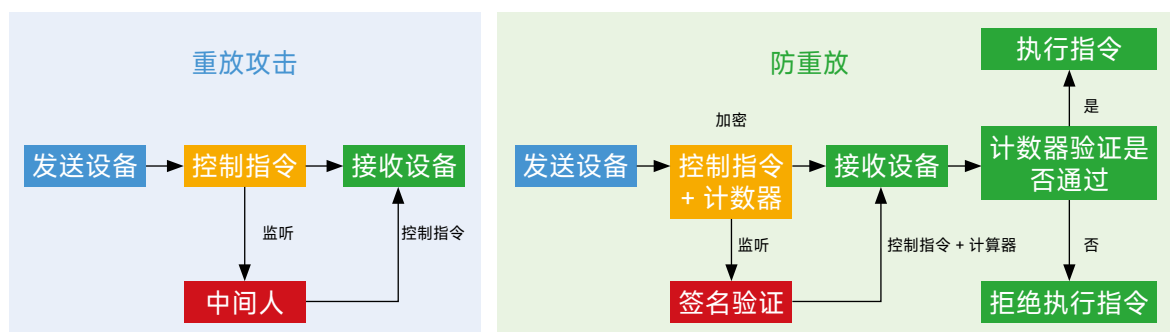


图 9 - 重放攻击和防重放

不同通信协议下的防重放可参考以下方案：

- ZigBee：设备应开启 Zigbee 协议帧计数器（framecounter）。开启方法为设置 nwkAllFresh 为 TRUE。
- 射频：设备使用滚动码方式进行通信，参考 keeloq、DST40、Hitag2 等业界成熟方案。

注 1：滚动码被用于设备通信身份验证，防止重放攻击。请参考：https://ww1.microchip.com/downloads/en/Appnotes/Atmel-2600-AVR411-Secure-Rolling-Code-Algorithm-for-Wireless-Link_Application-Note.pdf

注 2：业界成熟方案包括 Keeloq：<https://blog.csdn.net/kangweijian/article/details/43491047>；DST40：https://en.wikipedia.org/wiki/Digital_signature_transponder；Hitag2：<https://blog.csdn.net/spenghui/article/details/71930428>

- Wi-Fi：采用 HTTPS TLS1.2+ 传输协议默认支持的数据包序列号计数器防重放功能。
- 蓝牙：采用米家蓝牙认证协议默认支持的帧计数器和加密功能，或采用标准 BLE SM（Security Manager）模块的数据包计数器（packetCounter）和链路层加密。

4.1.5 非授权通信协议限制 [高中低]

设备与 APP、服务端、其他设备以及工厂 / 售后维修工具通过无线或有线通信

使用的通信协议应经过安全评估，不应使用非授权通信协议，以防止非授权协议存在安全漏洞或后门影响设备通信安全。

设备如因业务需要连接第三方 APP / 服务器，应对第三方 APP / 服务器提交安全评估和测试，并对第三方服务器通过安全调查问卷等方式进行审核，审核通过后应把设备与第三方服务器间的数据传输处理情况加入到设备 / APP 的隐私政策中。

4.1.6 未绑定状态的受控指令限制 [高中低]

设备在未绑定时无法判断控制指令来源合法性，应拒绝执行除配网相关指令外的其他指令，防止设备配置被篡改或隐私信息泄露。

4.1.7 系统配置防泄漏 [高中]

设备在网络接口及设备调试接口中应实现系统配置等安全相关信息的最小化输出，防止攻击者利用非必要输出的信息中的特定配置或版本可能存在的安全漏洞绕过通信认证。

- 网络接口：在通信认证通过前返回的信息不应包含非绑定过程必要的设备安全相关信息。
- 调试接口：设备调试接口打印的日志中不应包含设备安全相关信息。

注 1：设备安全相关信息包括：1) 设备系统配置相关信息：设备配网协议、配置选项、内核版本和软件版本等。2) 设备登录认证失败的提示信息：如用户登录失败，应提示用户名或密码错误，而不是具体的错误原因如密码错误、密码长度错误等。绑定过程中必须进行的加密算法协商、配网协议协商等参数通过网络接口披露应经过安全评估

注 2：绑定过程中必须进行的加密算法协商、配网协议协商等参数通过网络接口披露应经过安全评估

4.1.8 敏感指令来源限制 [高]

高安全等级设备的敏感受控指令应仅支持通过蓝牙 /NFC 等近场通信协议经过严格的指令完整性、合法性和权限验证再执行，防止攻击者从互联网远程向设备下发非预期的敏感控制指令。如业务强需求需从互联网下发此类指令，则指令下发的通信加密鉴权方案应经过安全评估。

4.2 以太网和无线网络

4.2.1 以太网通信信道保护【高中低】

设备应使用加密的传输协议对通信进行加密，应采用 TLS (1.2+) 传输协议的安全加密套件。避免因使用 MQTT、HTTP 等明文传输协议或包含的 SHA1、CBC 等弱加密套件而导致信息泄露或通信内容被篡改的风险。

注：TLS 加密套件的安全性可在 <https://ciphersuite.info/cs/> 查询，推荐使用 Recommend 和 Secure 类型的加密套件。

4.2.2 HTTPS 证书校验【高中低】

设备使用 HTTPS 协议时，应对所有字段（域名、有效期等）进行严格的证书校验，完成设备对服务端的验证，不能忽略证书检查导致证书被替换的风险。

- Linux 系统

设备应严格验证服务端证书合法性，不应使用如下参数跳过证书验证或忽略证书验证错误。

表 3 - Linux 工具 / 库 HTTPS 校验配置

工具 / 库	参数使用建议
curl	不应使用 -k 参数
wget	不应使用 --no-check-certificate 参数
libcurl	应将 CURLOPT_SSL_VERIFYPEER 和 CURLOPT_SSL_VERIFYHOST 设置为 True

- Android 系统

设备应用使用 SSL 加密通信服务应严格校验服务端和客户端证书，不应信任任意证书，不应忽略异常事件（如 return 空或者 null）；如需自定义 SSLx509 TrustManager，重写 checkServerTrusted 方法，方法内必须严格判断服务端的证书校验，以防止通信内容被劫持导致通信数据泄漏或被篡改。

4.2.3 Wi-Fi 接入点口令【高中】

设备使用 Wi-Fi Direct 接入点与控制应用连接的功能应严格评估必要性，如确

有必要，设备端 Wi-Fi Direct 接入点口令不应使用固定密码或空密码，应遵循一机一密或者每次使用真随机生成密码，并显示在屏幕上（带屏设备）或在绑定时由用户提前设置并存储（无屏设备），以防止 Wi-Fi 被非法接入。

4.2.4 Wi-Fi 接入点用途 [高中]

设备建立的 Wi-Fi 接入点应只允许接入此 Wi-Fi 接入点的其他设备与本设备进行通信，不应令接入的设备访问本设备之外的网络（如家庭网或互联网），以防止攻击者通过此 Wi-Fi 接入点向家庭网络渗透。

4.3 蓝牙

4.3.1 蓝牙协议版本 [高中低]

蓝牙设备应使用 4.2 及以上版本的蓝牙协议，以防止设备在绑定阶段泄露蓝牙连接层密钥，从而导致隐私泄露或设备伪造的风险。

4.3.2 蓝牙配对 [高中低]

- 物理按键确认：有物理按键的蓝牙设备在配对绑定过程中应要求用户在设备端按下物理按键进行绑定确认，或在设备端按下物理按键后再开启绑定窗口，以避免设备在用户不知情的情况下被他人绑定的风险。
- 配对模式：如果采用的不是米家蓝牙安全认证协议或米家蓝牙标准认证协议，应使用安全的蓝牙配对模式：
 - 设备在配对过程中应正确上报设备 IO 能力，如设备是否支持数字输入 / 输出能力，是否支持按键等。
 - 如果由于需要兼容不同按键 / 显示等交互能力的设备而支持 Just Work 配对模式的（如电视），应符合本项要求中物理按键的要求。

4.3.3 蓝牙广播 [高中低]

部分设备通过蓝牙将传感器采集的数据进行广播传输，通过蓝牙网关解析广播

内容进行设备联动，或根据广播数据作为控制指令，从而影响其他设备。此类设备的蓝牙广播应使用安全的通信协议，并使用绑定时产生的 beaconkey 对广播数据内容进行加密。

4.3.4 蓝牙控制指令合法性校验【高中低】

设备执行蓝牙控制指令前应对指令来源合法性进行校验，如使用绑定时验证控制端身份，每次连接时身份验证通过后应与控制端协商会话密钥，使用会话密钥加密传输控制指令，防止指令被篡改。

4.3.5 蓝牙敏感信息通信【高】

设备在使用 BLE 与控制应用（安卓）通信时，应对敏感信息内容本身进行应用层加密，以防止用户使用 BLE 将手机与其他智能设备配对进行数据传输时，手机上的所有应用都可以访问这两个设备间传输的数据。

In contrast to **Classic Bluetooth**, Bluetooth Low Energy (BLE) is designed to provide significantly lower power consumption. This allows Android apps to communicate with BLE devices that have stricter power requirements, such as proximity sensors, heart rate monitors, and fitness devices.

Caution: When a user pairs their device with another device using BLE, the data that's communicated between the two devices is accessible to **all** apps on the user's device.

For this reason, if your app captures sensitive data, you should implement app-layer security to protect the privacy of that data.

注：风险描述参见 Android 开发文档中有关引入蓝牙 BLE 的相关内容，<https://developer.android.com/guide/topics/connectivity/bluetooth-le>

4.3.6 芯片原厂未鉴权指令防护【高中低】

设备使用蓝牙芯片厂商提供的 OTA 例程指令前应判断控制应用的蓝牙绑定状态，只有在绑定状态下才可执行 OTA 指令。防止因例程中可能支持未授权指令控制设备的逻辑，从而导致设备拒绝服务（例如芯片重启、切换工作空间、进入 DFU 升级模式等等）的风险。

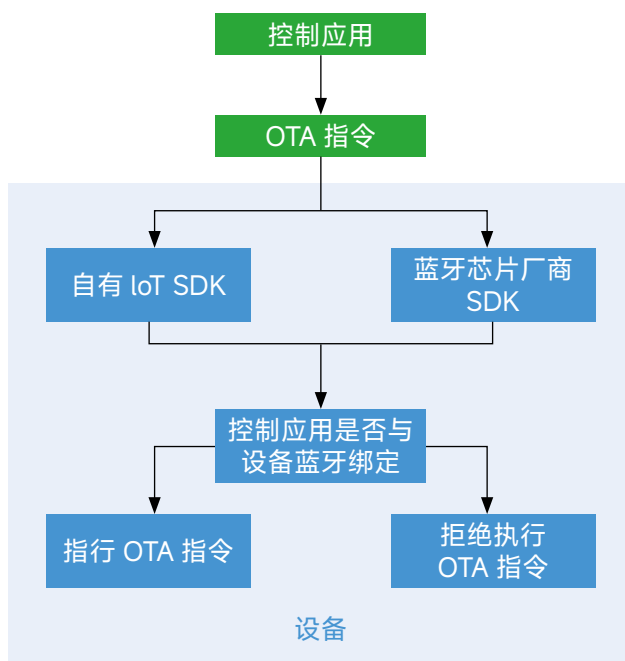


图 10 - 芯片原厂未鉴权指令防护

4.3.7 蓝牙广播防追踪机制【高中低】

设备宜使用随机蓝牙 MAC 地址，并对蓝牙广播内容进行加密；如需通过 Beacon 信标广播可识别身份的信息，应定时变换设备蓝牙 MAC 地址并同时变换广播 Payload，以防止他人通过部署足够多的探测设备对广播内容进行分析，通过固定的 MAC 地址或固定的广播 Payload 跟踪设备的移动轨迹。

4.3.8 蓝牙 Mesh 协议【高中低】

蓝牙 Mesh 设备应使用安全的通信协议与 Mesh 设备、网关及手机进行双向认证，对传输的敏感数据使用会话密钥加密。

注：米家的 Mesh SDK 已实现上述安全能力，接入米家产品按照指引接入即可符合此项要求。

4.4 Zigbee

4.4.1 Zigbee 协议版本【高中低】

Zigbee 设备应使用 Zigbee 3.0 协议栈版本，并使用官方 Install Code 方案，以防止攻击者利用旧协议版本的默认 TCLK 密钥进行攻击。

注：Zigbee 3.0 官方 Install Code 方案请参考：<https://zigbeealliance.org/solution/zigbee/>

4.5 Sub 1G 射频

Sub 1G 射频指工作在 315MHz，433MHz，769-935MHz 等 1GHz 以下频率的频段。此类频段一般没有通用的协议栈，需要自行设计开发组网、编解码和加密等功能。

4.5.1 射频通信数据包序列号长度 [高 中 低]

设备的射频通信数据包应使用四字节作为序列号变量空间，避免使用较短序列号长度，以防止通信内容可在短时间暴力破解的风险。

4.5.2 通信密钥硬编码 [高 中]

设备射频通信密钥应通过发射器和接收器配对交换生成，不应预置密钥在代码中。

4.5.3 通信频率 [高]

设备应使用跳频机制进行通信（硬件选型时可参考芯片厂提供的跳频能力），以防止因射频通信频点固定造成信道拥堵，导致设备无法正常通信。



05

数据安全与隐私

5.1 加密与哈希算法 [高中低]

- 加密算法：设备应使用安全的加密算法且密钥长度符合对应算法的最低要求（见下表），不应使用 DES、TDES、RC4 等不安全加密算法。
- 哈希算法：设备应使用 256 bit 以上的安全 hash 函数，如 SHA256，SHA512 等，不应使用已有安全风险的 hash 函数，如 MD5 或 SHA1。

表 5 - 安全的加密与哈希算法

算法	密钥 / 哈希值 长度 (bit 位)	其他要求
AES	128 / 192 / 256	
ECDH / ECDHE	256/384/512	安全曲线：curve25519
ECDSA	256/384/512	安全曲线：curve25519, secp256k1
RSA	2048 / 3072 / 4096	
DSA	Prime P: 2048 / 3072 / 4096	
	Prime Q: 256/384/512	
SM4	128	
SHA	256/384/512	

注：如由于产品 ECC 加密 / 签名库不支持以上曲线的，可使用 NIST P-256 曲线。

5.2 随机数生成函数 [高中]

设备系统及应用的身份认证、通信加密、本地数据加密等关键逻辑应使用真随机或强伪随机算法产生认证或加密所需的随机数。

表 6 - 安全的随机数生成函数

类型	生成方式	建议
真 / 强伪随机	● /dev/urandom ● 芯片支持的熵随机 (TRNG) 能力 ● uxRand() 函数	推荐
伪随机	● srand()、rand() 并使用 time(0) 为种子生成	不推荐

5.3 日志上报 [高中低]

设备、系统及应用打印的日志不应上传任何明文或加密的敏感信息（如 Wi-Fi SSID、密码、手机 IMEI、地理位置等敏感信息）。因业务需要确需上报使用的，应

经过安全评估审核通过，并在隐私政策中明示数据上报的范围、使用目的和存储方式等信息

5.4 跨境网络请求 [高 中 低]

设备或控制应用应识别当前用户所属国家或地区，根据不同国家或地区的隐私合规要求发送网络请求，以防止数据跨境传输带来的隐私风险。

表 7 - IoT 业务跨境合规参考

地区	可访问的服务器
中国大陆	仅可访问当地服务器
印度	
俄罗斯	
美洲（北美 & 南美）	仅可访问美国服务器
欧洲	仅可访问欧洲服务器 其中荷兰要求健康相关数据存储于荷兰本地服务器
其余地区	仅可访问新加坡服务器

5.5 服务端数据存储安全 [高 中 低]

通过设备采集的用户敏感信息（如视频、音频、图片、文档等）应加密存储于业务云端存储服务器。云端应具有访问控制机制，禁止未授权访问和使用用户信息。

5.6 服务端数据删除功能 [高 中 低]

物联网平台应向用户提供便捷的删除云端数据的功能，删除范围包括用户在使用设备及其关联服务过程中产生并存储在云端的个人信息。

5.7 恢复出厂设置 [高 中 低]

设备恢复出厂设置后应完全清除设备中所有用户数据、设置（如用户使用记录、设置、NFC 门卡、eSIM 卡记录等）。对于支持 SD 卡、硬盘等扩展存储的设备，应在说明书中提供扩展存储中的数据删除或复制方式，或恢复出厂设置时同时删除扩展存储中的数据。

06

业务逻辑

6.1 设备可绑定状态 [高 中 低]

未绑定设备在上电后 30 分钟仍未绑定的，应关闭待绑定状态，并在重新上电后重新进入绑定状态，避免设备始终允许接受绑定请求而被恶意绑定的风险。

6.2 绑定确认 [高]

室内高安全级别设备绑定时宜在产品能力允许的情况下，要求用户在设备端进行绑定确认（针对无实体按钮的设备使用场景，需要用户主动确认）。绑定确认时应设置超时断开链接机制，确保不被恶意绑定链接。

室外交通工具和室外高安全级别设备（如滑板车、门铃、门锁、室外监控摄像机）应使用 OOB 绑定方式，防止设备被恶意绑定。

门锁等其他带有“物理按钮”的高安防等级产品，应将绑定确认“物理按钮”放置在室内面板或安全区域。

6.3 防重复绑定 [高 中 低]

对于具备重置能力的设备，应被重置后才可再次接受绑定请求，以防止被其他用户重复绑定或恶意绑定控制。

6.4 强绑定关系 [高]

室外高安全级别设备应在云端将设备和账户建立强绑定关系，即云端记录设备 ID 与用户 ID 的绑定关系。设备绑定时应先验证云端记录，仅允许在云端没有绑定记录的设备的绑定请求，并且设备端重置不应清除云端绑定记录，仅当设备所有者（在云端有绑定记录的用户 ID）在控制端应用上主动解绑时才清除绑定关系，以防止设备重置后被非法绑定控制。若设备由于业务特殊原因无法采用云端强绑定关系，应经过安全评估，在设备端解除与用户 ID 的绑定关系时增加密码验证等保障措施。

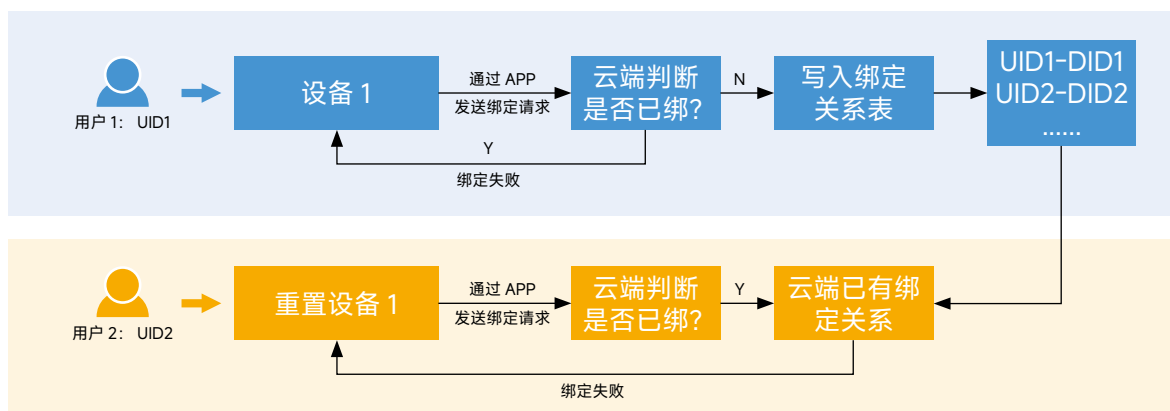


图 11 - 强绑定

6.5 设备分享权限及鉴权 [高]

- 对于具备访问权限分享的设备，应建立分享权限分级机制，用户在分享设备时能以被分享人所需的最低权限分享设备，防止被分享人权限过高可任意修改设备配置等风险。

权限分级可参考以下：

- 1) 设备所有者：即绑定设备的用户，具备最高权限，可访问设备的敏感及非敏感功能、修改设备所有设置、分享设备、解绑设备。
- 2) 设备管理员：被设备所有者通过设备分享授予权限，具备中等权限，可访问设备的敏感及非敏感功能、修改设备的非关键设置，可被设备所有者随时收回权限。
- 3) 设备使用者：被设备所有者通过设备分享授予权限，具备最低权限，可访问设备的非敏感功能，可被设备所有者随时收回权限。

- 服务端及被分享设备应对分享操作进行严格鉴权：

- 1) 服务端及设备端应分别对分享用户身份鉴权，仅允许设备所有者进行设备分享。
- 2) 分享中的过程通信应使用设备 /APP/ 服务端三者之间已有的安全通信信道加密通信。
- 3) 对于门锁等对用户人身安全、家庭安全、财产安全的保护起到关键作用的设备，应在分享过程中结合 OOB 二维码、PIN 码等认证方式，并应在设备端根据每个用户的独特信息生成不同鉴权密钥的方式验证每次连接的分享用户的权限。

6.6 密码输入防偷窥【高】

具备密码输入功能的室外高安全等级设备（如门锁）应具备防偷窥功能，如在验证密码时允许用户在正确密码前后增加一定位数的虚位密码。



图 12 - 虚位密码

6.7 指纹识别解锁【高中】

- 指纹识别算法应在设备端具备安全存储和安全运行环境的芯片内运行，防止指纹照片或特征在局域网或互联网传输造成用户敏感信息泄露。
- 指纹识别认假率 (FAR) 应小于 0.001%

注：认假率指未录入的指纹认证成功并实现解锁的概率，如果认假率过高，门锁的安全性就得不到保障。

- 指纹识别模块宜具备活体检测能力，如在指纹模块集成红外传感器等方式防止指纹假体解锁攻击。

6.8 人脸识别解锁【高中】

- 人脸识别算法应在设备端具备安全存储和安全运行环境的芯片内运行，防止人脸照片或特征在局域网或互联网传输造成用户敏感信息泄露。
- 人脸识别认假率 (FAR) 应小于 0.001%

注：认假率指未录入的人脸认证成功并实现解锁的概率，如果认假率过高，门锁的安全性就得不到保障。

- 人脸识别应具备活体检测能力，防止人脸照片等 2D 假体和三维头部模型等 3D 假体解锁攻击。

6.9 报警事件管理 [高中低]

- 部分设备具备感知事件并报警的功能应默认开启，对于可能威胁用户人身安全、家庭安全或重大财产安全的报警事件（如门锁被撬、触发烟雾报警等），设备应立即启动声光报警。本条内容对第二条范围内的场景不适用。
- 对于胁迫报警等部分特殊设计的安防场景，设备声光报警可能反而会威胁用户人身安全，此类报警事件不应触发设备端声光报警。例如在被歹徒胁迫开门时，用户可在门锁密码键盘输入提前设定好的特定报警密码秘密上报报警事件。
- 对于所有报警事件，除设备端本地响应外，应同时通过 WI-Fi/ 蓝牙 /Zigbee 网关、移动通信网络等通道上报该报警事件到云端。

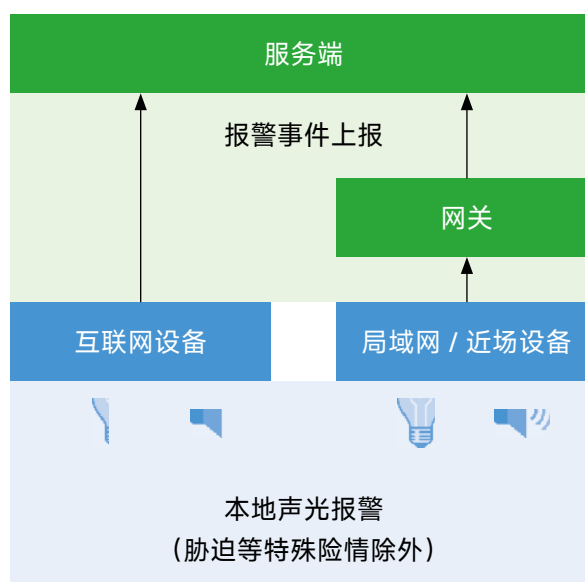


图 13 - 报警事件管理

6.10 设备传感器说明 [高中低]

设备应在说明书或隐私政策中清晰透明地声明设备所有的外部传感能力（如声光感应、环境感应等），防止在用户不知情的情况下收集用户个人信息。

6.11 设备日志安全监控 [高中低]

物联网平台应从设备端收集关键日志，应将此类设备日志用于安全监控。通过统计和分析日志信息发现异常，从而发现潜在的设备或物联网平台安全风险。同时，

日志在管理平台的存储时间应不少于 6 个月。

日志应包括但不限于以下内容：

- 用户登陆、通讯录管理、添加或删除管理用户、安全报警、系统开关机、核心配置变更等重要操作；
- 事件的日期和时间、用户、事件类型、事件操作结果及其他与审计相关的信息。

6.12 安全设置指南 [高]

设备应采取以下方式之一帮助用户简便地开启这些安全功能。安全设置指南指设备及关联服务（如 APP，WEB 等）为用户提供的用于设备的访问控制、身份认证、通信加密等安全功能的指南，以及用户如何检查这些设置是否已安全设置的文档或流程。可参考以下类型来实现：

- 默认设置：设备初始化时自动默认开启必要的安全功能。

例如：默认禁止不安全的通信加密套件。

- 软件引导：设备软件或控制应用通过配置向导、软件界面引导提示等提供相关安全功能开关和说明，或通过弹窗等形式引导用户开启。

例如：APP 中有开启和查看设备访问密码设置的指引或选项，或提示用户当前设备连接的 Wi-Fi 的加密方式不安全。

- 说明书：通过纸质或电子版产品安全设置指南告知用户开启产品安全功能的方式和步骤。

例如：在说明书中图文并茂地展示如何开启设备访问密码、设置管理密码等安全功能，以及用户设备中、SD 卡中的个人信息如何删除等。

6.13 演示模式 [高]

具有演示功能的设备，应禁止销售给用户。若具备演示功能等设备需要进行售卖，应通过返厂刷机或在线 OTA 等方式去除演示功能代码。

术语和定义

下列术语和定义适用于本文件

1 消费级物联网设备 Consumer IoT Device

网络连接设备（本文简称“设备”），该规范内消费级物联网终端设备指具有无线（Wi-Fi、BLE/Mesh、Bluetooth classic、Zigbee、NFC、RF 射频）、有线（RJ45）联网与组网能力，或具有固件逻辑更新能力的任意智能终端产品。

注 1：消费级物联网设备也通常用于商业环境，这些设备仍然被归类为消费级物联网设备。

注 2：消费级物联网设备通常可供消费者在零售环境中购买，消费级物联网设备也可以委托和 / 或专业安装。

2 用户 User

自然人或组织。

3 关键安全参数 Critical Security Parameter

与安全相关的秘密信息，这些信息被泄露或被修改后会危及智能家居安全性，如后台系统管理员认证信息、操作系统登录认证信息、网络设备认证信息等。

4 公共安全参数 Public Security Parameter

与安全相关的公共信息，其修改会损害安全模块的安全性，如验证软件更新的真实性 / 完整性的公钥、证书的公共组件。

5 敏感安全参数 Sensitive Security Parameters

公共安全参数和关键安全参数。

6 个人信息 Personal Data

与已识别或可识别的自然人有关的任何资料。

7 敏感信息 Sensitive Information

敏感信息为敏感安全参数与个人信息的统称。

8 调试接口 Debug Interface

制造商在开发过程中用于与设备通信的物理接口，或用于对设备的问题进行分类，如测试点、UART、SWD 和 JTAG 等。

9 逻辑接口 Logical Interface

利用网络接口通过信道或端口在网络上通信的软件实现。

10 网络接口 Network Interface

可用于通过网络访问消费者物联网功能的物理接口。

11 物理接口 Physical Interface

物理端口或空气接口（如无线电、音频或光学接口），用于与物理层的设备通信，如收音机、以太网端口、USB 等串行接口和用于调试的接口。

12 安全更新 Security Update

为了修复由制造商发现的或他人报告给制造商的安全漏洞的软件更新。

注：如果漏洞的严重程度需要更高的优先级修复，软件更新可以是纯粹的安全更新。

13 日志 Telemetry

来自设备的数据，可以提供信息，帮助制造商识别与设备使用有关的问题或信息。如消费者物联网设备向制造商报告软件故障，使他们能够识别和补救原因。

14 鉴权 Authentication Mechanism

用于证明实体真实性的方法：“实体”既可以是用户，也可以是机器。例如：认证机制可以是请求密码、扫描二维码或使用生物特征指纹扫描仪。

15 闪存 Flash

Flash 是存储芯片的一种，通过特定的程序可以修改里面的数据。FLASH 在电子以及半导体领域内往往表示 Flash Memory 的意思，即平时所说的“闪存”，全名叫 Flash EEPROM Memory。

16 Bootloader

在嵌入式操作系统中，BootLoader 是在操作系统内核运行之前运行，可以初始化硬件设备、建立内存空间映射图，从而将系统的软硬件环境带到一个合适状态，以便为最终调用操作系统内核准备好正确的环境。

17 U-Boot

U-Boot 是一个主要用于嵌入式系统的引导加载程序，可以支持多种不同的计算机系统结构，包括 PPC、ARM、AVR32、MIPS、x86、68k、Nios 与 MicroBlaze。

18 内核 Kernel

嵌入式内核是在嵌入式硬件和软件之间的抽象层，在 Linux 的术语中被称为“内核”，也可以称为“核心”。Linux 内核的主要模块（或组件）分以下几个部分：存储管理、CPU 和进程管理、文件系统、设备管理和驱动、网络通信，以及系统的初始化（引导）、系统调用等。

19 蓝牙信标 Beacon

蓝牙信标（Beacon）是建立在低功耗蓝牙协议基础上的一种广播协议。

20 地址随机化 ASLR

地址随机化（ASLR）是一种针对缓冲区溢出的安全保护技术，通过对堆、栈、共享库映射等线性区布局的随机化，通过增加攻击者预测目的地址的难度，以防止攻击者直接定位攻击代码位置，达到阻止溢出攻击的目的。

21 ID 卡 Identification Card

ID 卡全称为身份识别卡（Identification Card），是一种不可写入的感应卡，含固定的编号，主要有台湾 SYRIS 的 EM 格式、美国 HIDMOTOROLA 等各类 ID 卡。ID 卡与磁卡一样，都仅仅使用了“卡的号码”而已，卡内除了卡号外，无任何保密功能，其“卡号”是公开、裸露的，因此 ID 卡也被称作“感应式磁卡”。

22 M1 卡 M1 card

M1 芯片卡，是指飞利浦下属子公司恩智浦出品的芯片缩写，全称为 NXP Mifare1 系列，常用的型号包括 S50、S70，常见的样式包括卡式、钥匙扣式。

23 真插芯 Through-Lock Cylinder

智能门锁的真插芯是指锁芯直接固定在锁体结构上，利用锁芯上的拨片直接驱动锁体，使其实现开关效果的一种组合方式，直观表现为：使用钥匙时，钥匙与门面为垂直关系。

24 假插芯 Non-Through-Lock Cylinder

智能门锁的假插芯是将锁芯与锁体位置分离，锁芯转动时，利用齿轮箱和连接杆，将动力传送给锁体，从而实现锁体开关效果的一种新型组合方式，直观表现为：使用钥匙时，钥匙与门面为平行关系。

25 例程 Routine

例程是某个系统对外提供的功能接口或服务的集合，如操作系统的 API、服务等。

26. CarIoT 设备

可以直接连接小米汽车，且在小米汽车上或附近（非远程）使用的后装 IoT 设备，连接通道包括蓝牙、WiFi、有线以太网、蜂窝网等。

27. 控车 CarIoT 设备

可影响车辆财产安全和驾驶安全的 CarIoT 设备，如可控制车门车窗后备箱开关、可启动汽车或更改驾驶模式的设备。

缩略语

缩略语	解释和全称
API	应用编程接口 (Application Programming Interface)
ADB	安卓调试桥 (Android Debug Bridge)
AES	高级加密标准 (Advanced Encryption Standard)
ASLR	地址空间布局随机化 (ASLR)
DES	数据加密标准 (Data Encryption Standard)
DID	设备标识码 (Device ID)
EMMC	嵌入式的非易失性存储卡 (Embedded Multi Media Card)
FTP	文件传输协议 (File Transfer Protocol)
IoT	物联网 (Internet of Things)
IP	网络协议 (Internet Protocol)
JSAPI	JavaScript 应用编程接口 (JavaScript Application Programming Interface)
JTAG	联合测试工作组 (Joint Test Action Group)
MAC	介质访问控制地址 (Media Access Control)
MQTT	消息队列遥测传输 (Message Queuing Telemetry Transport)
NAND	与非门逻辑电路 (Not And)
NX	Stack 栈不可执行 (No Execute Stack)
OOB	带外数据 (Out of Band)
OTA	空中下载 (Over The Air)
PIE	位置独立的可执行文件 (Position Independent Executables)
PSK	预共享密钥 (Pre-Shared Key)
RSA	一种非对称加密算法，以此算法的三位共同提出者姓氏开头字母拼在一起而命名
RX	接收 (Receive)
SSH	安全外壳协议 (Secure Shell)
SWD	串行线调试 (Serial Wire Debug)
TCLK	信任中心链接密钥 (Trust Center Link Key)
TCP	传输控制协议 (Transmission Control Protocol)
TLS	安全传输层协议 (Transport Layer Security)
TX	发送 (transmit)
UART	通用异步收发传输器 (Universal Asynchronous Receiver-Transmitter)
UDP	用户数据报协议 (User Datagram Protocol)
UID	用户名 (User ID)
USB	通用串行总线 (Universal Serial Bus)
XML	可扩展标记语言 (eXtensible Markup Language)

附录 A 产品安全等级

根据产品的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）受到损害时对设备、用户及物联网平台可能造成的最大影响程度，把物联网产品分为高、中、低三个安全等级。设备安全等级判断的核心关注点及对应影响等级见下表：

安全属性	关注点	影响程度		
		低	中	高
保密性 Confidentiality	设备收集的个人信息敏感程度越高，保密性受到损害时对用户的影响越大			
	个人基本资料	√		
	个人教育工作信息	√		
	个人常用设备信息	√		
	个人通信信息		√	
	联系人信息		√	
	个人身份信息			√
	个人生物识别信息			√
	网络身份标识信息			√
	个人健康生理信息			√
	个人财产信息			√
	个人上网记录			√
	个人位置信息			√
	其他敏感信息			√
完整性 Integrity	综合设备或 APP 端可能发生的恶意篡改或其他完整性被破坏的情况下，对用户人身安全、财产安全、精神上可能带来的影响程度			
	影响轻微	√		
	影响有限		√	
	影响严重			√
可用性 Availability	在设备及相关服务完全不可用的情况下，对用户或在舆论上带来的影响程度			
	影响轻微	√		
	影响有限		√	
	影响严重			√

各类个人信息及敏感信息的定义及举例见附录 C

根据小米 IoT 平台中已接入的产品的类型及特点，梳理出产品安全等级划分表，供评估产品安全等级时参考使用。

产品安全等级划分参考		
产品安全等级	品类	产品
高安全等级	摄像头	摄像机、门铃、猫眼
	网关	路由器、网关、移动路由、Wi-Fi 信号放大器
	工作娱乐	音箱、电视、电视盒子、笔记本、Android 电纸书、运输机器人、故事机、词典笔、学习机
	安防	门锁、保险箱（需要区分是否链接网络，或可以通过蓝牙遥控，手机远程遥控等方式开锁）、智能门、防丢器
	穿戴	手环、手表
	出行	滑板车、自行车、行车记录仪
	清洁	扫地机器人
	其他类型设备参考	其他对 CIA 要求较高的产品，如： 1) 保密性 (C): 产品携带摄像头，或会持续监听用户语音指令（如小爱、Alexa、Google Assistant 等），或会采集用户个人敏感信息和特殊类型个人信息并可直接通过 Wi-Fi 或移动网络连接互联网的设备 2) 完整性 (I): 具有小爱等语音主控功能的设备，或产品本身具有交通工具属性 3) 可用性 (A): 在用户的家庭网络 /IoT 设备关系中扮演比较重要角色的设备，可用性收到破坏可导致家庭网络 /IoT 网络中断
中安全等级	健康检测	心电仪、体脂秤、睡眠检测仪、艾灸器、血压计、智能枕头、电热毯、跑步机、走步机、电暖器
	大家电	电热器
	出行	对讲机（可连接互联网）；儿童安全座椅
	办公	打印机
	其他	其他对 CIA 要求中等的产品，如： 保密性 (C): 会采集用户个人敏感信息和特殊类型个人信息，但无法直接连接互联网，需要使用蓝牙等近距离通信方式经过 APP/ 网关等上报数据的设备，如体脂秤、睡眠检测仪、心电仪、动感单车
低安全等级	家用电器	冰箱、空调、洗衣机、热水器、炒菜机、集成灶、抽油烟机、风扇、空气净化器、净水器、垃圾处理器、电磁炉、电饭煲、压力锅、微波炉、榨汁机、蒸烤箱、洗碗机 养生壶、新风机、空气检测仪、除湿机、空气炸锅、足浴器、集成灶、冲奶器、软水机、咖啡机、果蔬净化机、消毒柜、燃气传感器、凉霸、恒温酒柜、多功能料理锅等
	卫浴	晾衣架、浴霸、马桶、马桶盖、牙刷、毛巾架、干衣 / 鞋机等
	其他	耳机、灯、门窗传感器 / 窗磁 / 门磁 / 窗帘电机、温湿度计 / 温度传感器 / 天气传感器、开关、宠物喂食机、插座 / 插排、打印机、宠物玩具 / 宠物饮水机、加湿器、红外遥控器、机顶盒、收音机、智能鱼缸、管线机、智能种植器、杀菌灯、继电器控制模块、驱蚊器、叮咚机

附录 B 产品安全等级与安全要求对应表

不同安全等级的设备需满足的要求如下：

章节	标题		低	中	高	特殊说明
第一章 设备硬件	1.1 物理调试接口	1.1.1 调试接口默认关闭	○ *	●	●	*CarloT 设备
		1.1.2 PCB 板上调试接口丝印			●	
		1.1.3 调试接口默认关闭信息输入	○ *	●	●	*CarloT 设备
		1.1.4 调试接口打印敏感数据	○ *	●	●	*CarloT 设备
	1.2 本地数据存储			●	●	
	1.3 芯片间通信				●	
	1.4 安全启动				○ *	* 控车 CarloT 设备、智能门锁、摄像机
	1.5 防物理拆除				○ *	* 智能门锁、门铃、室外摄像机
	1.6 防强电磁攻击				○ *	* 智能门锁、保险箱
	1.7 智能门锁锁芯及门卡				○ *	* 智能门锁
	1.8 设备唯一标识防篡改				●	
第二章 设备软件	2.1 软件升级	2.1.1 固件升级包完整性与合法性	●	●	●	
		2.1.2 防固件降级			●	
		2.1.3 软件更新失败后恢复机制		●	●	
		2.1.4 局域网 OTA 升级指令		●	●	
		2.1.5 第三方组件更新			●	
		2.1.6 设备线刷防护	●	●	●	
	2.2 服务与端口最小化		●	●	●	
	2.3 代码库管理		●	●	●	
	2.4 正式版本组件管理		●	●	●	
第三章 操作系统	3.1 通用 OS	3.1.1 Bootloader 启动		●	●	
		3.1.2 用户账户密码（有登录 UI）	●	●	●	
		3.1.3 防暴力破解	●	●	●	
		3.1.4 验证输入数据	●	●	●	
		3.1.5 特权功能接口	○ *	●	●	*CarloT 设备
	3.2 嵌入式 Linux OS	3.2.1 串行端口绑定 SHELL		●	●	
		3.2.2 系统默认账户密码（无登录 UI）	○ *	○ *	●	*CarloT 设备
		3.2.3 基础文件系统权限		●	●	

章节	标题		低	中	高	特殊说明
		3.2.4 外部存储的程序和脚本		●	●	
		3.2.5 地址空间布局随机化		●	●	
		3.2.6 基址随机加载保护		●	●	
		3.2.7 栈 Cookie 防溢出		●	●	
		3.2.8 栈不可执行		●	●	
		3.2.9 删除调试符号表	●	●	●	
	3.3 Android	3.3.1 通用 Android 版本	○ *	●	●	*CarloT 设备
		3.3.2 Android ADB 鉴权方案	●	●	●	
		3.3.3 Android Webview 版本限制		●	●	
第四章 设备通信	4.1 通用通信	4.1.1 密钥生成与用途限制		●	●	
		4.1.2 通信传输安全保护	●	●	●	
		4.1.3 通信双向认证	○ *	○ *	●	*CarloT 设备
		4.1.4 防重放		●	●	
		4.1.5 非授权通信协议限制	●	●	●	
		4.1.6 未绑定状态的受控指令限制	●	●	●	
		4.1.7 系统配置防泄漏		●	●	
		4.1.8 敏感指令来源限制	○ *	○ *	●	*CarloT 设备
	4.2 以太网和无线网络	4.2.1 以太网通信信道保护	●	●	●	
		4.2.2 HTTPS 证书校验	●	●	●	
		4.2.3 Wi-Fi 接入点口令		○ *	○ *	* 依赖设备建立 Wi-Fi 热点进行连接控制 (如行车记录仪、运动相机等)
		4.2.4 Wi-Fi 接入点用途		○ *	○ *	
	4.3 蓝牙	4.3.1 蓝牙协议版本	●	●	●	
		4.3.2 蓝牙配对	●	●	●	
		4.3.3 蓝牙广播	●	●	●	
		4.3.4 蓝牙控制指令合法性校验	●	●	●	
		4.3.5 蓝牙敏感信息通信			●	
		4.3.6 芯片原厂未鉴权指令防护	●	●	●	
		4.3.7 蓝牙广播防追踪机制	○ *	○ *	○ *	* 控车 CarloT 设备
		4.3.8 蓝牙 mesh 协议	●	●	●	
	4.4 Zigbee	4.4.1 Zigbee 协议版本	●	●	●	
	4.5 射频	4.5.1 射频通信数据包序列号长度	●	●	●	
		4.5.2 通信密钥硬编码	○ *	●	●	*CarloT 设备
		4.5.3 通信频率			●	

章节	标题	低	中	高	特殊说明
第五章 数据安全 与隐私	5.1 加密与哈希算法	●	●	●	
	5.2 随机数生成函数		●	●	
	5.3 日志上报	●	●	●	
	5.4 跨境网络请求	●	●	●	
	5.5 云端存储安全	●	●	●	
	5.6 云端数据删除功能	●	●	●	
	5.7 恢复出厂设置	●	●	●	
第六章 业务逻辑	6.1 设备可绑定状态	●	●	●	
	6.2 绑定确认			●	
	6.3 防重复绑定	●	●	●	
	6.4 强绑定关系			○ *	* 室外设备
	6.5 设备分享权限及鉴权			●	
	6.6 密码输入防偷窥			●	
	6.7 指纹识别解锁		●	●	
	6.8 人脸识别解锁		●	●	
	6.9 报警事件管理	●	●	●	
	6.10 设备传感器说明	●	●	●	
	6.11 设备日志安全监控	●	●	●	
	6.12 安全设置指南			●	
	6.13 演示模式			○ *	* 智能门锁

● 表示该等级的全部产品均需满足的要求

○ * 表示该等级的部分特殊品类需满足的要求，适用的品类在最后一列特殊说明中给出。例如，“1.1.1 调试接口默认关闭”适用于中、高等级的所有产品，也适用于低安全等级的 CarIoT 设备。

附录 C 敏感信息定义与举例

1. 敏感信息定义

敏感信息 = 敏感安全参数 + 个人信息

2. 敏感安全参数定义与举例

敏感安全参数 = 公共安全参数 + 关键安全参数

- 公共安全参数

与安全有关的公共信息，其修改会损害安全模块的安全。

例 1：用于验证软件更新的真实性 / 完整性的公钥。

例 2：证书的公共部分。

- 关键安全参数

与安全有关的秘密信息，其披露或修改会损害安全模块的安全。

例：私钥、认证值（如密码）、PIN、证书的私人部分。

3. 个人信息定义与举例

- 个人信息

个人信息是指以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映自然人活动情况的各种信息。

表 A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等

个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

[来源：GB/T35273-2020《个人信息安全规范》附录 A]

● 个人敏感信息

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

表 B.1 个人敏感信息举例

个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

[来源：GB/T35273-2020《个人信息安全规范》附录 B]

● 特殊类型的个人信息

揭示种族或民族血统、政治观点、宗教或哲学信仰或工会会员资格的个人数据，以及处理基因数据、用于唯一识别自然人的生物识别数据、有关健康的数据或有关自然人的性生活或性取向的数据。

[来源：General Data Protection Regulation - Article 9]

附录 D 硬件选型重点关注

设备的很多安全能力都需要硬件的支持，在项目早期预研阶段根据产品安全等级和硬件选型关注表，选择满足设备安全要求的芯片等硬件，能保障设备安全能力的实现。

附录 E 修订记录

版本号	修订时间	修订内容
1.0	2020.12	初版
2.0	2021.12	1. 优化描述，移除不适用内容； 2. 增加产品安全等级定义方法及关注点； 3. 增加基线要求分级适用表，明确各安全等级产品需满足的不同要求； 4. 增加米家已实现的通用安全解决方案； 5. 增加产品硬件选型注意事项； 6. 增加产品用户体验关注项； 7. 增加不符合基线要求对应的历史漏洞等级参考表。
3.0	2022.12	1. 优化安全要求描述； 2. 补充完善通用方案及参考方案（新增多个通信认证鉴权方案）； 3. 增加产品安全等级划分表、更新高 & 中安全产品定级参考依据； 4. 更新敏感信息定义； 5. 补充与国际标准核心差异项（覆盖 ESTI/EN 303645 中全部的强制要求内容）； 6. 优化 PDF 易读性（通用方案合并到正文、正文增加要求适用等级、目录跳转等）。
4.0	2023.11	1. 优化修改了 33 项安全要求描述； 2. 新增 2 项针对 Android 系统的通用要求； 3. 新增 2 项技术通用解决方案和要求； 4. 补充新增 5 项针对门锁品类特殊安全要求； 5. 优化 PDF 易读性（更改统一专业术语描述、细化缩写解释、补充基线阅读指南）。
5.0	2024.11	1. 优化修改了 22 项安全要求描述； 2. 新增 1 项针对 Android 系统的安全要求； 3. 新增和优化了 6 项针对门锁品类安全要求； 4. 新增 11 项 CarIoT 适用的安全要求； 5. 新增 4 项 通用产品品类安全要求； 6. 优化 PDF 易读性。

