MIUI 11

安全与隐私白皮书

SECURITY AND PRIVACY WHITE PAPER

2019.11

目录

声明

由于小米产品或服务升级、调整或其他原因，本文档内容有可能变更。小米有权再对本文档内容进行增加、修改、删节、废止，请及时在官方网站下载最新版本。

本文档仅作为用户了解 MIUI 及小米云服务的信息安全与隐私保护的参考性指引。小米基于当前的 MIUI 版本和主要使用的硬件架构，尽力提供相应的介绍。但由于技术升级、产品迭代、适用法律法规变化、措辞一致性等潜在的问题，小米在此明确声明对本文档内容的完整性、准确性和适用性等不作任何明示或暗示的保证。

如若发现本文档存在任何错误或对本文档内容存在任何疑问，请通过 security@xiaomi.com 邮箱直接联系小米。

01

概述

Summary

1 概述

小米公司作为全球领先的智能手机制造商，以始终坚持做“感动人心、价格厚道”的好产品，让全球每个人都能享受科技带来的美好生活作为企业的使命。在智能化互联时代，安全与隐私是用户对产品的基本需求，因此，小米将用户的安全与隐私问题放在首位。

小米设计的 MIUI 以安全性和易用性为核心，软件、硬件和服务在每台小米手机上紧密集成、协同工作，为用户提供端到端的安全保护。其中既包括硬件芯片、系统内核、数据安全等基础安全能力，也包括帐号、支付、云服务、语音 AI、图像 AI 等一系列关键服务的信息安全与隐私保护。

本文秉承客观透明的原则，详细介绍了 MIUI 的安全架构、技术原理、功能设计和隐私保护措施。希望小米用户、开发者、合作伙伴和相关监管部门能够更加清晰地了解小米在手机及云服务的信息安全与隐私保护方面的体系架构和实现方式。

MIUI 的安全性技术源于构建自硬件的安全根，通过安全启动将可信链传递到操作系统；通过使用并加强 Android 安全内核，监控应用运行时的状态，保证操作系统及应用安全；通过加密和数据保护功能来保护文件系统和用户数据的安全；通过服务功能划分和纵深防御对云服务进行综合防护。下图展示了小米 MIUI 安全与隐私白皮书的逻辑结构，本文将依据该结构展开。

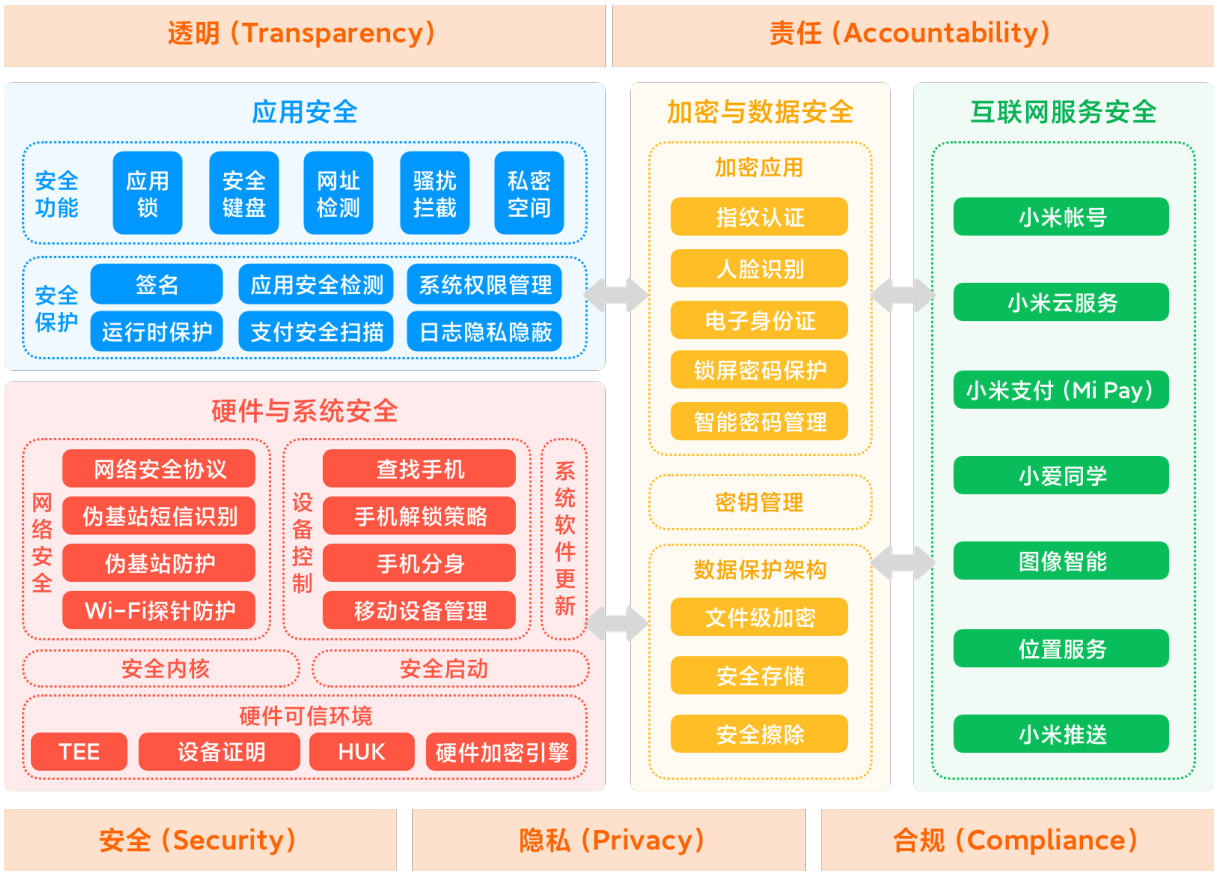


图 1-1 白皮书逻辑结构

硬件与系统安全：小米手机是安全的一体化软硬件平台，包括由硬件构建的可信环境、安全启动、安全内核、网络与通信安全、设备控制及系统软件更新。

加密与数据安全：基于 MIUI 设计的数据保护架构提供的加密应用，在保障用户数据安全的同时，也提升了 MIUI 的易用性和便捷性。

应用安全：MIUI 针对 APP 的基础保护机制和一系列应用安全功能，确保了手机应用的安全运行及用户数据的安全性。

互联网服务安全：针对运行在 MIUI 上的小米主要的互联网服务，小米采取了最大程度的保护措施，保护用户的隐私与数据安全。

安全认证与隐私政策：小米在信息安全与隐私保护方面的总体原则、组织架构、安全与隐私认证、隐私政策以及持续改进机制。

02

硬件与系统安全

Hardware and system security

2 硬件与系统安全

硬件与系统安全是应用和数据安全的基础，为 MIUI 的整体安全提供底层框架，包括硬件可信环境、安全启动、安全内核、网络与通信安全、设备控制、系统软件更新等内容。

MIUI 通过硬件、系统和服务的紧密集成，确保从初始启动到系统软件更新，再到应用程序的每个组件均有安全验证机制，最大程度保障用户的数据安全。

2.1 硬件可信环境

2.1.1 可信执行环境（TEE）

MIUI 支持 TEE（Trusted Execution Environment，可信执行环境）安全操作系统。TEE 可以构建一个隔离于主操作系统的小型操作系统，让具有安全、隐私诉求的应用隔离于 Android 系统运行于此。

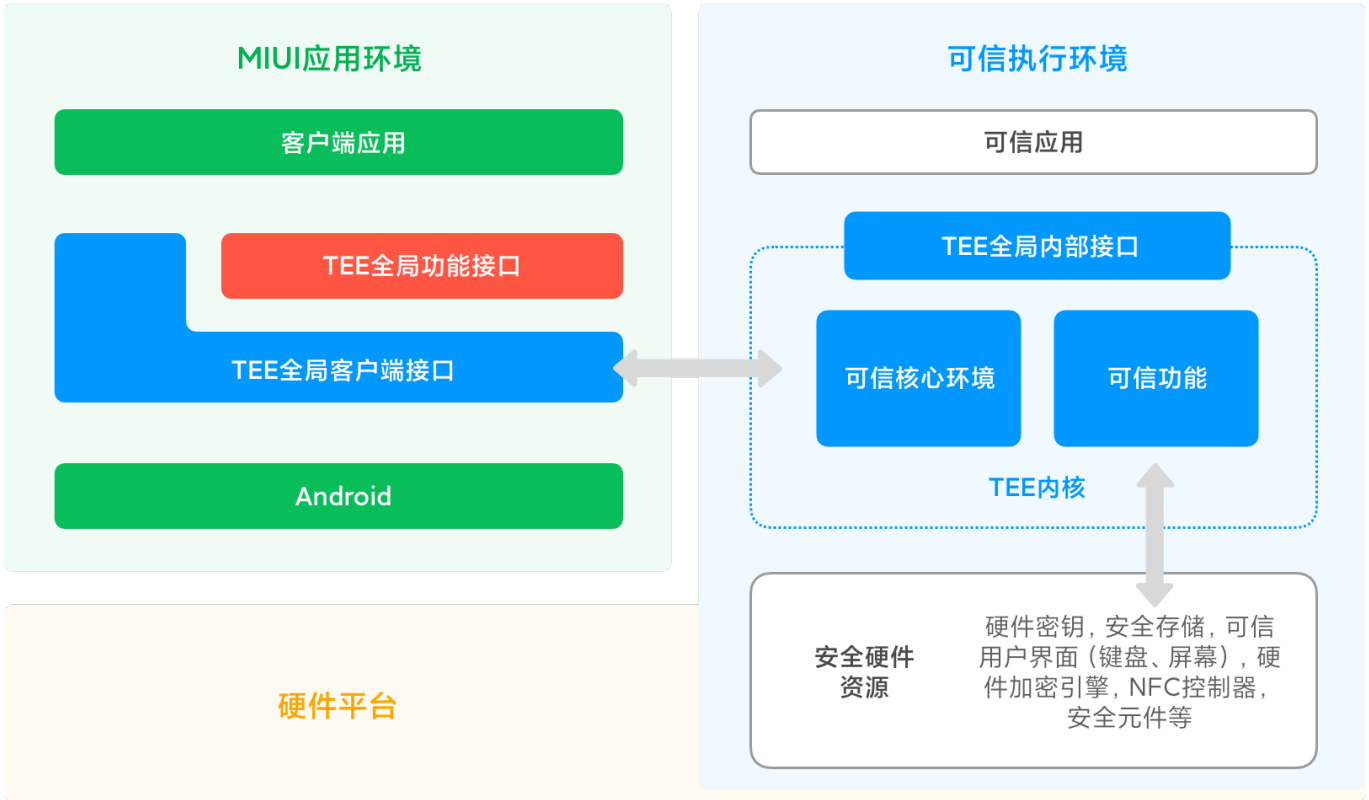


图 2-1 可信执行环境逻辑架构

TEE 所能访问的软硬件资源是与主操作系统分离的，TEE 提供了可信应用的安全执行环境，同时也保护可信应用的资源和数据的保密性、完整性及访问权限。为保证 TEE 本身的可信根，TEE 在安

全启动过程中需要通过验证并且与主操作系统隔离。在 TEE 中，每个可信应用是相互独立的，而且在未授权的情况下不能互相访问。TEE 内部 API 主要包含了密钥管理、密码算法、安全存储、安全时钟等资源服务，以及扩展的可信 UI 等。

> 可信 UI 是指在关键信息的显示和用户关键数据（如口令）输入时，屏幕显示和键盘等硬件资源完全由 TEE 控制和访问，Android 系统中的软件不能访问。

2.1.2 设备证明

为确保手机自身是可信的，小米手机出厂时在 TEE 中预置了设备证书，用于标识该设备的身份，TEE 的公钥统一存储在小米服务器中。在某些安全性要求较高的应用场景中，应用可以向小米服务器发起验证，以确定该设备的真实性。

2.1.3 设备唯一密钥（HUK）

HUK（Hardware Unique Key，设备唯一密钥）出厂时固化在手机主板上，每台手机的 HUK 都不相同且无法被篡改，仅有硬件加密引擎可以访问。HUK 为锁屏密码保护和文件系统加密功能所使用的密钥提供了设备唯一性保证。

2.1.4 硬件加密引擎

加解密操作是一个非常复杂的过程，需要强大的计算能力。但对于移动设备而言，速度、节能和安全都至关重要。小米手机在设计时充分考虑了这些因素，为设备搭载了高性能的硬件加密引擎 *，确保设备在运行速度、电池续航和数据安全等多个方面达到平衡。加密引擎支持的主要算法有：

- 3DES
- AES-128、AES-256
- SHA-1、SHA-256
- HMAC-SHA1、HMAC-SHA256
- RSA-1024、RSA-2048
- ECDSA-256

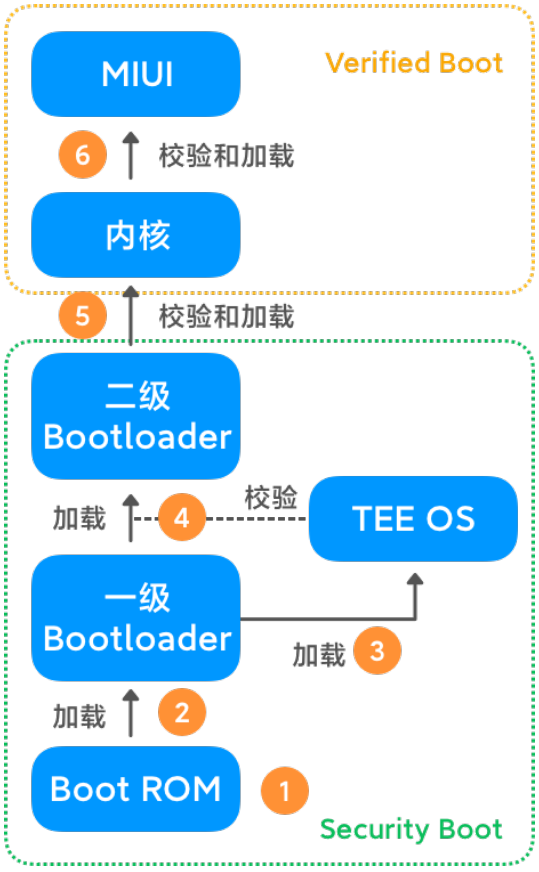
* 注：部分机型未搭载硬件加密引擎。

2.2 安全启动

安全启动是在系统启动过程中，通过签名公钥验证文件或程序的数据签名，确保启动文件或程序

的完整和可信，以防止在启动过程中加载并运行了未经授权的程序。在安全启动机制下，所有启动文件（如：启动引导程序、内核镜像、基带固件）均需先通过签名校验才被允许加载运行，在启动过程的任何阶段，如果签名验证失败，则启动过程会被终止。

片内引导程序（ROM SoC Bootloader）是在芯片制造时被写入芯片内部只读 ROM 中的一段引导程序，出厂后无法修改，设备上电后最先执行此代码。



1. 设备上电，PC 指针指向芯片内部 Boot ROM 地址并执行。
2. Boot ROM 从外部存储设备加载、验证一级 Bootloader 并跳转执行。
3. 一级 Bootloader 加载 TEE OS 镜像文件。
4. 一级 Bootloader 加载二级 Bootloader，并由 TEE OS 校验。
5. 二级 Bootloader 校验并加载内核文件。
6. 内核程序校验并加载 MIUI 系统。

图 2-2 MIUI 安全启动过程

设备上电后，片内引导程序执行基本的系统初始化，从 Flash 存储芯片中加载一级引导程序，并利用保存在主芯片内部 Fuse 空间的公钥对一级引导程序镜像的数字签名进行校验，验证成功后运行一级引导程序。随后，一级引导程序加载、校验和执行 TEE OS 镜像，TEE OS 运行起来后，由 TEE OS 和一级引导程序共同校验、加载和执行二级引导程序。以此类推，直到整个系统启动完成，从而保证启动过程的信任链传递，防止未授权程序被恶意加载运行。

MIUI 系统的启动过程支持 Android 的 Verified Boot 2.0（AVB2.0）功能。在设备启动过程中，从受硬件保护的信任根到引导加载程序，再到启动分区和其他已验证分区（包括 system、vendor 和可选的 OEM 分区），无论是在哪个阶段，都会在进入下一个阶段之前通过加密认证方式验证代码可靠且没有任何已知的安全缺陷之后才会执行。AVB 有助于防止永久驻留的 Rootkit 恶意软件持有 ROOT 权限危害设备，可确保设备在启动过程中的安全性。

2.3 安全内核

MIUI 支持 Android 原生的 SELinux 特性，对系统中的进程、文件、目录等所有资源的操作均实施强制访问控制，任何进程想在 SELinux 系统中执行操作，都必须先在安全策略配置文件中赋予权限，而访问控制的策略在设备启动过程中会被保护起来，无法被第三方更改。通过 SELinux，MIUI 可以阻止系统进程读写受保护的数据，还可以阻止系统进程绕过内核的安全机制或攻击其他进程。

MIUI 支持 KASLR（Kernel Address Space Layout Randomization，内核地址空间布局随机化），在每次系统启动时，MIUI 都对内核的地址空间布局进行随机安排，内核的地址空间布局难以预测，使代码重用攻击的难度被提升，降低了遭到许多复杂攻击的可能性，进一步提升了系统内核的安全性。

2.4 网络与通信安全

2.4.1 安全网络协议

使用安全的网络协议，可降低用户设备连接网络时数据遭受泄露、篡改的风险。MIUI 用户可借用公网链路建立自己的 VPN 专用私有网络。MIUI 支持的 VPN 模式包括：PPTP、L2TP/IPSec PSK、L2TP/IPSec RSK、IPSec Xauth PSK、IPSec Xauth RSA、IPSec Hybrid RSA。用户可按需选择 VPN 模式，用于访问和传输敏感数据。

MIUI 的 WLAN 连接支持 WEP、WPA/WPA2 PSK、802.1x EAP、WAPI 等多种认证方式，供不同安全级别需求的用户选用。

MIUI 的 WLAN 热点功能默认关闭，当用户开启时，默认使用 WPA2 PSK 认证方式，保证连接安全。同时，WLAN 热点功能支持设置终端 MAC 地址黑名单。

2.4.2 伪基站防护

伪基站是一种利用了通信系统缺陷的非法无线电通信设备，常被犯罪分子用于冒用他人手机号码向伪基站周边的用户手机发送诈骗短信或垃圾短信。当伪基站运行时，会干扰和屏蔽一定范围内的运营商信号，用户手机信号被强制连接到该设备，影响用户正常使用。

MIUI 为用户提供了伪基站防护功能 *，防止手机接入伪基站，用户可以通过“设置”–“更多设置”–“系统安全”–“伪基站防护”开启该项功能（默认关闭）。

* 注：仅限于使用了高通芯片的小米手机支持此功能。

2.4.3 伪基站短信识别

如果用户未开启伪基站防护功能，MIUI 仍为用户提供了伪基站短信识别功能，且该功能不依赖于芯片，适用于所有型号及版本的 MIUI 用户。

通过手机端的 AI 机器学习模型，根据伪基站接入手机的特征和伪基站短信的文本特征，判断伪

基站疑似程度，识别伪基站短信。MIUI 针对伪基站短信的识别均在用户手机端离线进行。识别为伪基站短信时，MIUI 会向用户进行提示。

2.4.4 Wi-Fi 探针防护

Wi-Fi 探针盒子是通过监听空中其他电子设备发出的 Wi-Fi 信号，从数据包中获取其 MAC 地址来识别用户身份。MIUI 支持利用随机 MAC 地址发送数据包，防范 Wi-Fi 探针获取手机真实的 MAC 地址 *。

* 注：MIUI 11 已经在多数设备中支持在未连接状态下的 Wi-Fi 探针防护。此外，升级到 Android Q 的手机支持连接状态下的 Wi-Fi 探针防护。

2.5 设备控制

2.5.1 查找手机

MIUI 为用户提供了查找手机功能，为用户找回丢失手机提供帮助，同时保护手机的数据安全。此功能需用户手动开启后才能使用。启用后，在手机丢失的情况下，用户可登录小米云服务网页（https://i.mi.com）远程对丢失的设备进行以下操作：查找定位、设备发声、丢失锁定和清除数据。

查找定位	通过网络或短信指令获取手机当前的位置并通过地图直观展示。
设备发声	通过网络或短信指令使手机响铃，用于查找可能就在附近的手机。
丢失锁定	通过网络或短信指令锁定手机，锁定后周期性自动上报定位位置，同时自动解绑 Mi Pay 绑定的银行卡。
清除数据	通过网络或短信指令重置手机，同时关闭数据同步及解绑 Mi Pay 银行卡。

2.5.2 手机锁定 / 解锁策略

在用户丢失手机或忘记小米帐号密码的情况下，手机均有可能被锁定，针对手机锁定的情况，MIUI 设计了多种安全策略来保障用户权利。

激活锁定	开启查找手机后，如果手机被恢复出厂设置，再次激活使用时必须验证开启查找功能时所绑定的帐号密码。
密码重置防护	为避免用户手机丢失后，帐号密码被使用手机验证进行重置，小米帐号重置密码后 3 天内无法关闭“查找手机”功能，为丢失手机的用户提供时间补办 SIM 卡，重新夺取帐号和手机的控制权。

客服解锁	在用户忘记了小米帐号密码且无法找回的情况下，MIUI 在手机锁定界面提供了解锁编号用于客服解锁。用户通过解锁编号申请解锁必须要提交申诉申请，由客服进行详细的人工审核后方可解锁。

此外，当手机丢失后，由于锁屏密码的存在，很大可能性会被强制刷机。MIUI 将帐号与设备关联关系保存到云端服务器(部分设备是将关联状态写入不被刷机覆盖的特殊分区中)，关联关系无法篡改。开机引导时，如果设备未联网，会要求强制联网，并从服务器获取真实的关联关系。如果当前设备登录帐号的状态和服务器上的关联帐号不同，MIUI 会要求用户切换回关联帐号后才能继续使用。

> 在解除 BL 锁的设备上，可以通过强制刷入一个非 MIUI 或篡改非官方 MIUI 规避手机锁定。不过此类 ROM 无法 OTA（Over the Air，空中下载），无法正常登陆小米帐号。当刷回官方 MIUI 包时，会再次受到“查找手机”功能的保护。

2.5.3 手机分身

MIUI 用户可通过手机分身创建一个完全独立于原系统的独立空间，实现用户的帐户、应用和数据等与主空间的完全隔离以及分别的加密保护，并支持通过不同的解锁密码进入主空间和分身空间，实现如同拥有第二部手机一般的虚拟手机体验。用户可以通过对这个独立空间设置访问密码，保存各类私密文件、图片等信息，安装私密应用等。这个独立空间又类似于一个“沙箱”，在这个“沙箱”内进行任何的操作，都不会对手机主空间造成影响。

2.5.4 移动设备管理（MDM）

MDM（Mobile Device Management，移动设备管理）是 MIUI 提供给设备管理类应用的设备保护功能，对手机设备进行管理和操作的接口。通过 MDM 应用和 MIUI 提供的 API 接口，企业 IT 系统可以轻松实现对 MIUI 设备的控制和管理。API 接口调用需要授权，保证接口调用的权限管控和安全性。

对于引导或提供非正常使用设备管理器权限的应用，按标准执行系统管控策略，包括但不限于：在系统内强提醒用户进行关闭处理、禁止应用获取服务或权限接口。

对于引导或提供通过设备管理器权限，对用户的数据、设备使用安全可能产生危害的应用，将严格执行如下操作：将该应用在小米应用商店进行下架处理、禁止应用获取相关服务接口、禁止相关应用在设备管理器应用列表中显示。

2.6 系统软件更新

MIUI 支持 Android 原生的 OTA（Over the Air，空中下载）机制，并在 Android 基础上提供了

更安全、高效的系统升级管理。

系统软件更新前，手机系统更新程序对通过 OTA 下载或线下拷贝到手机存储中的 ROM 进行完整性校验。校验内容包括但不限于文件大小、文件哈希值等。校验通过后，手机重启调用底层的恢复模式，并再一次校验签名密钥的正确性，校验通过后恢复模式才会将 ROM 中更新内容写入系统存储。

03

加密与数据安全

Encryption and data security

3 加密与数据安全

本章节主要阐述 MIUI 的数据安全防护机制，在 MIUI 中，文件系统分为系统分区和用户分区，系统分区只读且与用户分区隔离，普通应用仅可访问部分系统分区目录；对于用户分区，系统提供基于文件的数据加密和目录权限管理机制，限制不同应用间的数据访问。同时，基于加密技术，MIUI 提供了更多的安全功能和应用，在保证用户数据安全的同时提升了 MIUI 的便捷性和易用性。

3.1 数据保护架构

3.1.1 文件级加密

MIUI 支持 Android 的 FBE（File-based Encryption，文件级加密）功能特性，FBE 是针对每一个文件单独加密的，可以使用不同的密钥对不同的文件进行加密，并且可以对这些文件进行单独解密，这使得系统不需要把所有文件都进行加密，以及可以针对不同用户使用不同的密钥进行区分。文件级的数据加密，可以防止未经授权用户对设备实施物理攻击（如：直接读取 Flash）获取用户数据，为用户数据提供更好的安全性保障。

在 MIUI 中，文件加密使用的密钥由 Class Key 封装而来，而 Class Key 受到由设备唯一密钥(HUK)派生的 Keymaster Key 进行加密保护，而且在使用 Class Key 解密数据之前，需要用户通过锁屏密码或指纹进行认证授权。

图 3-1 文件级加密过程 *

* 注：本示意图适用于采用高通芯片并支持 FBE 的小米手机

在每一台支持 FBE 的小米手机上，每位用户均有两个可供应用使用的存储位置：

- 凭据加密（CE）存储空间：这是默认存储位置，只有在用户解锁设备后才可用。
- 设备加密（DE）存储空间：在开机未解锁期间以及用户解锁设备后均可用。

MIUI 中应用程序默认保存数据的位置是凭据加密（CE）存储空间，以保证应用及应用数据的安全。仅有像无线认证、闹钟、铃声、蓝牙等应用将部分数据保存在设备加密（DE）存储空间，保障一些必要的服务可以在用户提供凭据之前运行，同时系统仍能保护用户的私密信息。

3.1.2 安全存储

MIUI 的安全存储功能是基于 TEE 提供的安全文件系统（Secure File System，SFS）实现，用于安全存储密钥、证书、指纹模板等敏感信息。TEE 中运行的 TA（Trusted Application，可信应用）通过安全存储的 API 来加密并存储数据，加密后的数据只有 TA 能够访问，外部应用无法访问。MIUI 中的安全存储采用 AES-256 进行加解密，安全存储的密钥通过设备唯一密钥（HUK）进行派生，密钥始终存储在设备 TEE 内，经密钥加密过的数据 TEE 外部无法解密。

MIUI 进一步提供了基于 Flash 的 RPMB（Replay Protected Memory Block，重放保护内存块）分区功能来保护某些系统数据不会被非法删除和访问。RPMB 由 TEE 直接进行安全管理，采用设备唯一密钥（HUK）派生的密钥进行绑定，只有 TEE 才能访问 RPMB 分区保护的内容，外部 Android 侧不提供访问的接口。RPMB 通过内置的计数器和密钥、HMAC 校验机制来防止重放攻击，确保数据不被恶意覆写或篡改。

3.1.3 安全擦除

普通的“恢复出厂设置”操作，并不保证彻底删除保存在物理存储上的数据。为了提高效率，通常是通过删除逻辑地址的方式实现，但是实际存储的物理地址空间并没有清除，导致数据可以被恢复回来。MIUI 为用户提供了在设备恢复出厂设置时可选择“格式化模拟 SD 卡”选项，当用户选择“格式化模拟 SD 卡”时，系统会对存储空间执行格式化操作，彻底删除数据，以保护用户设备转售、废弃后的数据安全。

3.2 密钥管理

MIUI 的密钥管理功能主要用于管理应用开发者所使用的密钥和证书的全生命周期，同时为 TEE 环境中的设备证书提供远程证明。密钥管理具有如下功能：

1) 生成与存储

MIUI 的密钥管理提供由硬件保护的密钥存储机制，应用生成的密钥是经过加密的，只有对应的设备才可以使用。

2) 加密与解密

当应用需要使用密钥时，将之前生成的经过加密的密钥和待加密数据一起发送回对应设备的 TEE，只有在对应设备的 TEE 中才能使用密钥进行加密与解密操作。

3) 密钥认证

每台小米手机在生产时都在设备中注入了由 Google 公司颁发的证书，任何生成的密钥都可以使用 Google 的证书进行校验。使用密钥认证功能，网络服务可以对 MIUI 设备进行认证。

MIUI 的密钥管理的技术基础是 Android Keystore，它通过密钥提取防范和密钥使用授权等措施，避免了密钥材料在设备之外和设备上以未经授权的方式使用：

1）提取防范

为避免在 MIUI 设备之外以未经授权的方式使用密钥材料，通过 Android Keystore 密钥执行加密操作时，应用会将待签署或验证的明文、密文和消息发送到执行加密操作的系统进程，而不是应用进程。因此，即使应用进程遭受攻击，攻击者也无法提取密钥材料。

同时，MIUI 还将密钥材料绑定到小米设备可信执行环境的安全硬件，使其不会暴露于安全硬件之外。即使 MIUI 操作系统遭受攻击或者攻击者读取到设备的存储空间，也无法从设备上提取这些绑定安全硬件的密钥材料。

2）密钥使用授权

为了避免在 MIUI 设备上以未经授权的方式使用密钥，在生成或导入密钥时，Android Keystore 会让应用指定密钥的授权使用方式。一旦生成或导入密钥，其授权将无法更改。以后每次使用密钥时，都会由 Android Keystore 强制执行授权。MIUI 支持的密钥使用授权分为以下几类：

- 加密：授权密钥算法、运算或目的（加密、解密、签署、验证）、填充方案、分块模式以及可与密钥搭配使用的摘要；
- 时间有效性间隔：密钥获得使用授权的时间间隔；
- 用户身份验证：密钥只能在用户最近进行身份验证时使用。

3.3 加密应用

3.3.1 指纹认证

指纹认证是借助人体固有的指纹生理特征进行身份认证，可用于手机屏幕解锁、应用解锁、电子支付、隐私内容保护等需要强认证机制的场景。

MIUI 对指纹图像预处理、指纹特征提取、指纹模板生成、录入以及认证等处理均在 TEE 中进行，指纹数据无法传出 TEE。TEE 外部的 Android 第三方应用只能通过外部指纹框架发起指纹认证和接受认证结果，无法收集指纹数据本身。

MIUI 的指纹数据采用 AES-256 加密，加密过程通过调用 Keystore 来实现，外部无法获取到加

密指纹的密钥，保证用户的指纹数据不会泄露。MIUI 不会将指纹模板数据发送或备份到包括云端服务器在内的任何外部存储介质。

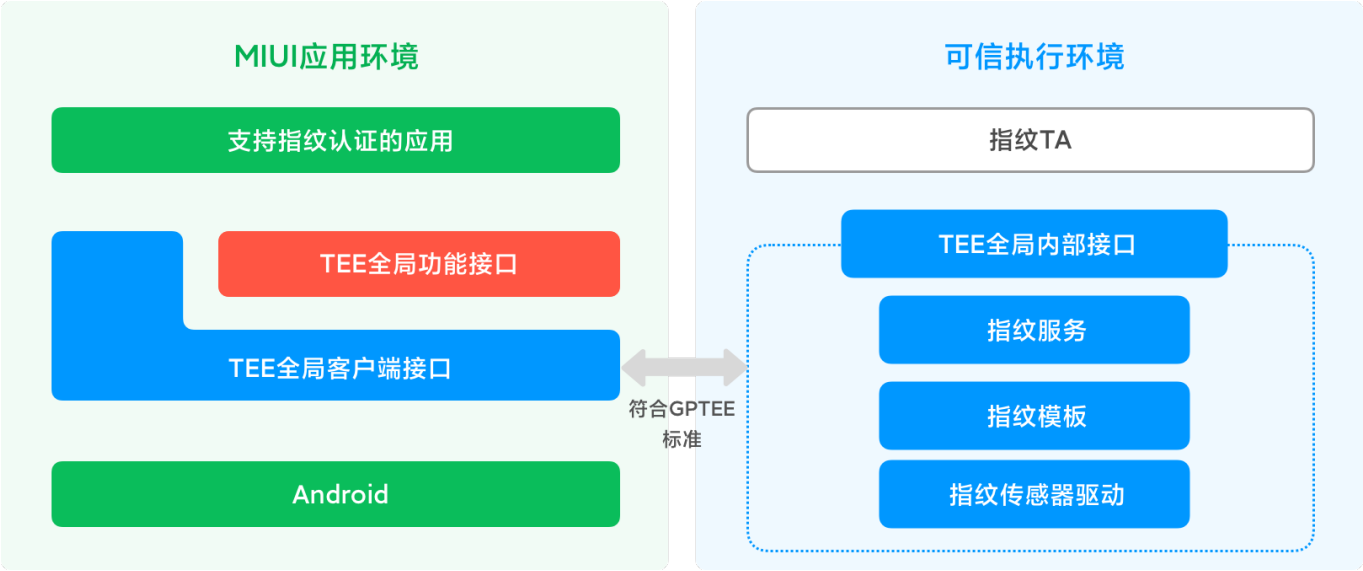


图 3-2 指纹安全框架

3.3.2 人脸识别

人脸识别，是基于人的脸部特征信息进行身份识别的一种生物识别技术。MIUI 基于 AI 人脸识别算法，智能检测面部特征进行高精度匹配，实现通过人脸解锁手机。

用户的脸部特征信息属于个人敏感信息中的个人生物识别信息，为保证安全，MIUI 对人脸图像的采集、特征提取、特征比对等处理完全在 TEE 环境中进行，人脸特征数据无法传出 TEE。TEE 外部的 Android 第三方应用只能通过外部人脸识别框架发起人脸认证和接受认证结果，无法收集人脸特征数据本身。

人脸特征数据通过内置安全芯片进行加密和解密，外部无法获取到加密密钥，确保人脸特征数据不会泄露。MIUI 也不会将人脸特征数据发送或备份到包括云端服务器在内的任何外部存储介质。

3.3.3 电子身份证

网络电子身份标识 eID（以下简称“eID”）是小米和公安部第三研究所联合开发的电子身份证应用，在公安部门认可的场合可以承担与物理身份证相同的功能。

小米手机遵循 eID 相关标准规范，具体包含如下：以安全芯片为载体；该芯片内部拥有独立的处理器、安全存储单元和密码运算协处理器；只能运行专用安全芯片操作系统。eID 信息经过加密存储在安全芯片 eSE 中，只有特定程序才能访问。开通 eID 时，安全芯片内部采用非对称密钥算法生成一组公私钥对用于签名认证，确保 eID 无法被非法读取、复制、篡改和使用，用户可以更安全地使用网络数字身份服务。

MIUI 的手机钱包客户端支持 eID 的全生命周期管理，用户可以随时在手机上开通、下载、使用和注销个人 eID。

* 注：仅部分机型支持此功能。

3.3.4 锁屏密码保护

MIUI 锁屏密码支持绘制图案、数字密码和混合密码三种方式，每一种方式均有最低密码长度要求来保证密码的强壮性。

- 绘制图案：至少需要连接 4 个点；
- 数字密码：支持 4~16 位长度的数字密码；
- 混合密码：支持 4~16 位的任意大小写字母、数字以及符号的组合。

MIUI 的锁屏密码通过设备唯一密钥（HUK）进行保护，在 TEE 中进行加密。在用户创建、修改锁屏密码，或验证锁屏密码进行解锁时，这些密码的处理都在 TEE 环境中进行。

MIUI 对锁屏密码输入错误的次数进行限制，连续多次输入错误的密码后，手机将被锁定，防止锁屏密码被暴力破解。

3.3.5 智能密码管理

随着内置帐号体系应用的增加，用户为手机各个应用设置不同的高强度的密码越来越困难，易于发生忘记用户名和密码的情况。智能密码管理 * 是 MIUI 为用户打造的一个安全的帐号密码管理工具，它可以将手机应用的登录信息（用户名和密码）集中保存，同时也可以与触摸指纹、锁屏密码关联，在用户登录应用时自动填充登录信息，让使用强密码变得容易。

小米智能密码管理也是基于 Keystore 技术实现，提供了硬件级加密能力，对用户托管的应用登录信息进行了高强度加密且仅允许在 TEE 中使用。因此，除了用户自己可以通过指纹和密码访问外，包括小米在内的任何其他方均无法获取到这些登录信息。

当前智能密码管理不提供云同步及云备份，只能在设备上由用户授权后才能使用，因此无需担心托管的密码库会被窃取或破解。

* 注：仅国内机型支持此功能。

04

应用安全

Application security

4 应用安全

在 MIUI 的底层硬件安全与系统安全框架以及 MIUI 提供的数据安全防护机制基础之上，通过应用层的安全技术实现对应用运行环境的保护，如：应用保护签名、运行时保护、应用安全检测等。

与此同时，MIUI 进一步提供了一系列的安全功能供用户选择使用，从而实现更进一步的数据安全与隐私保护，如：应用锁、安全输入键盘、骚扰拦截、私密空间等。

4.1 应用安全保护

4.1.1 签名

MIUI 会对应用包的完整性和来源官方性进行验证，以：

- **保证应用包没有被篡改**

开发者生成公钥和私钥，用私钥对应用包签名，并将公钥打包到应用包里面，应用安装时，用公钥验证应用包未被更改。

对已安装应用进行升级时也需要进行应用签名验证，只有与被升级应用程序具有相同签名的应用才被允许升级，以防止恶意应用程序取代现有应用程序。

- **保证应用包无法被伪造**

将应用包的 APP ID 和用于验证签名的证书使用官方的私钥签名。如果 A 开发者用自己的证书对 B 开发者的应用包签名，并将自己的证书文件打入应用包，则如果 A 开发者将其上传到应用商店后会导致官方签名验证失败。

- **保证应用包权限无法随意更改**

对授权列表、APP ID、证书同时用官方私钥签名，在安装运行时，检查授权列表和其实际调用的系统服务是否一致，如果不一致，会导致其调用 MIUI 服务失败。

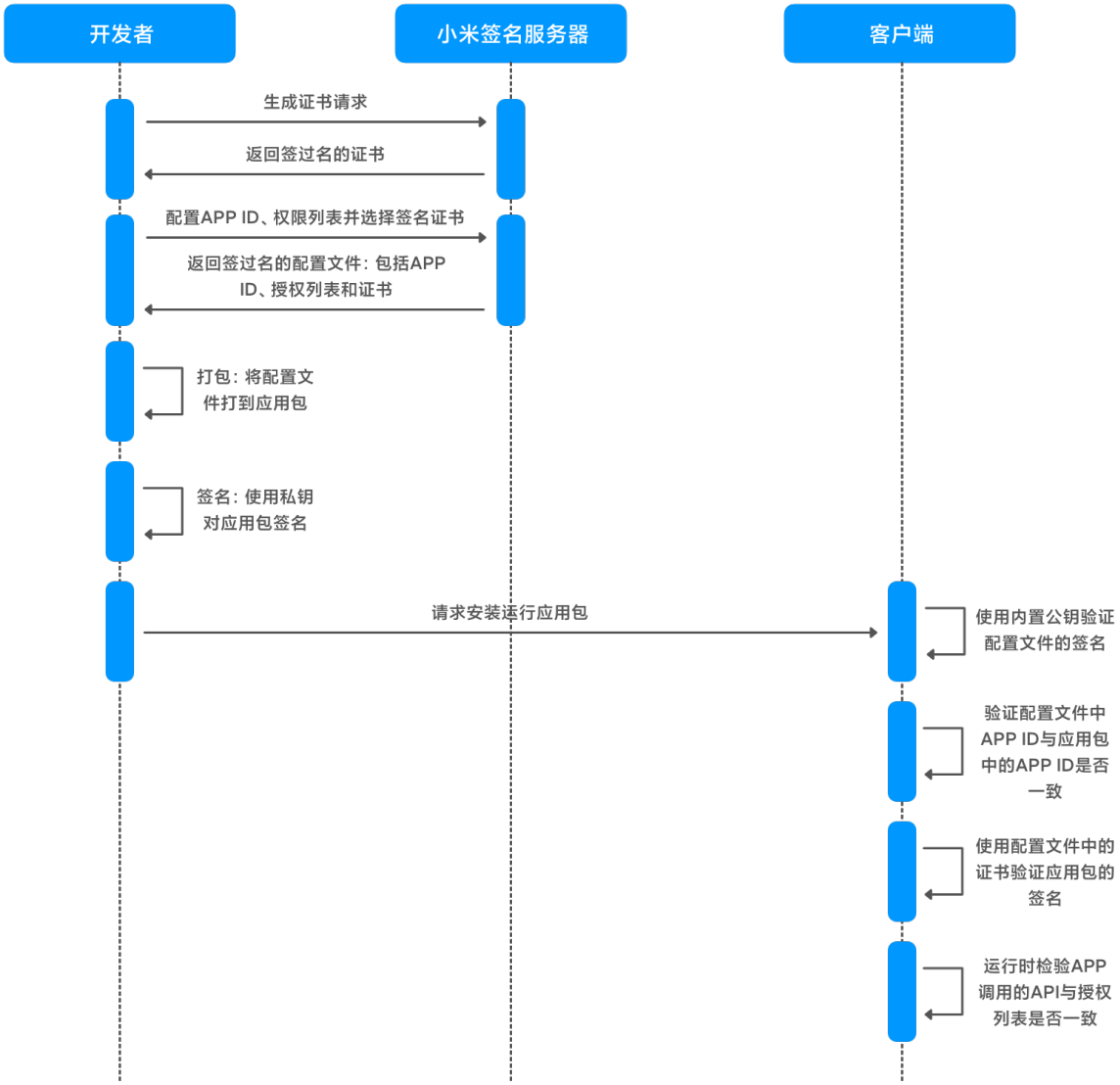


图 4-1 新应用签名流程

4.1.2 运行时保护

MIUI 支持 Android 原生的地址空间布局随机化（Address Space Layout Randomization，ASLR）及数据执行保护技术（Data Execution Prevention，DEP）。ASLR 提供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，增加攻击者预测目的地址的难度，防止攻击者定位攻击代码位置，达到阻止溢出攻击的目的。ASLR 技术提高了攻击者在利用内存漏洞上的难度。DEP 机制会把内存中的特定区域标注为不可执行区，以防止内存漏洞攻击。

此外，MIUI 也使用原生 Android 的应用沙箱机制，确保每个应用运行在沙箱中且相互隔离，保证应用运行时安全。

4.1.3 应用安全检测

小米应用商店对每一款应用均进行自动测试、安全扫描和人工审核，保证应用来源的安全。

在设备端，MIUI 为用户提供了嵌入多种杀毒引擎的病毒查杀和应用安装监控等系统防护检测机制。

此外，“手机管理”–“异常检测”功能还提供了 ROOT 安全检测以及手机性能、操作、耗电等异常检测，以保护应用安全，包括以下功能：

手机性能异常检测	检测 APP 是否开启了辅助功能、设备管理器，手机剩余内存是否不足。
操作异常检测	检测是否开启了飞行模式、拦截联系人来电、拦截陌生人来电、勿扰模式、护眼模式。
耗电异常检测	检测自启动应用是否过多（超过 5 个），是否开启了热点。
其他异常检测	检测系统是否被 ROOT，存储空间不足 5% 时提示用户无法安装应用。

4.1.4 支付安全扫描

支付安全扫描旨在保护用户支付时的安全。当用户使用支付类应用时，后台检测系统环境是否安全，检测到风险项时会通过弹框等交互方式提示用户，以降低用户的支付风险。

MIUI 内置一份支付类应用或页面的白名单列表，仅在用户打开名单内应用或页面时开始生效。该列表中涵盖了市面常见的主流应用。相关的检测项包括：

Wi-Fi 安全扫描	检测 Wi-Fi 是否有安全风险。
输入法安全检测	检测用户的输入法是否为白名单中的正版安全输入法。
病毒运行检测	检测后台进程是否有木马、病毒运行。
验证码窃取风险检测	检测第三方应用是否获取了读取通知类短信的权限，以避免验证码泄漏。

* 注：仅中国大陆地区提供此功能。

4.1.5 系统权限管理

Android 原生系统为应用提供了动态权限管理机制，旨在限制敏感操作，保护用户个人数据。应用在获取权限前以弹窗形式进行请求，由用户决定是否授予。

在此基础上，MIUI 新增了自启动管理、链式启动管理（相互唤醒）、后台弹出界面、锁屏显示界面等多个自定义权限，针对应用在后台长期运行、无故相互唤醒、恶意推广等多种行为进行限制。

MIUI 针对 APP 后台调用摄像头和录音权限的行为进行监测 *，如发现此类行为，会在状态栏提示通知，同时发出呼吸灯颜色提示，以警示用户。

* 注：仅部分机型支持。

4.1.6 日志隐私隐蔽

MIUI 针对 Android 原生日志中涉及到的隐私信息（如：基站位置、IP 地址、设备标识符等）使用星号“*”进行局部屏蔽，增强隐私信息的保护。

4.2 应用安全功能

4.2.1 应用锁

应用锁既可保护应用数据安全，同时又防止应用中的隐私信息被他人窥见。

MIUI 用户可通过“应用管理”进入“应用锁”模块，为应用设置多种样式的解锁密码（图案、数字、混合），通过该模块，用户可设置在退出应用后或是退出应用 1 分钟后锁定，以及在锁屏后再次打开应用时验证应用锁。为了增加解锁的便捷性和安全性，MIUI 增加了指纹生物识别解锁机制。

4.2.2 安全键盘 *

用户在“设置”–“语言与输入法”–“安全键盘”中设置启用安全键盘，在输入密码时，MIUI 自动启用安全键盘。安全键盘不具备联想和记忆功能，没有联网权限，禁止后台录屏或第三方应用截屏，禁止第三方应用悬浮窗覆盖在安全键盘之上，确保用户的密码输入安全。

* 注：仅中国大陆地区提供此功能。

部分银行 APP 使用自行开发的输入法，MIUI 安全键盘不会生效。

4.2.3 网址检测 *

针对日益严峻的网络安全形势，小米提供恶意网址检测服务，基于海量网址类别知识库识别恶意网址，当用户在手机自带浏览器、短信等入口访问恶意网址时弹窗提示风险，该项服务具备以下特点：

- **检测类型多样**：能够检测出涵盖社工欺诈、信息诈骗、虚假销售、恶意文件、博彩网站、色情网站等恶意网址类别；
- **高吞吐率**：可以支撑每天 2500 万次的网址检测请求；
- **低延迟**：服务平均响应时间在 100ms 以内；
- **检测精度高**：百万量级标注样本的检测准确率在 97% 以上；
- **保护用户隐私**：除网址外不会收集其他信息。

* 注：仅中国大陆地区提供此功能。

4.2.4 骚扰拦截

MIUI 骚扰拦截能够为用户提供全面的防骚扰电话和垃圾短信拦截功能，有效拦截广告推销、房产中介等骚扰电话及垃圾短信。用户可以快速地从“通话记录”、“联系人”添加号码至黑白名单，也可以将地区加入黑白名单，实现对已知号码的拦截和放行。实时更新的黄页数据库能够为用户提供准确的号码黄页信息，避免用户受到陌生号码的骚扰。

MIUI 提供多种拦截规则，用户可以根据需要手动配置，这些配置可以备份到云端，以实现跨终端同步等功能：

- **黑白名单**：放行白名单号码、拦截黑名单号码；
- **黑白关键词**：放行包含白关键词的短信、拦截包含黑关键词的短信；
- **黑白名单地区**：放行白名单地区、拦截黑名单地区的电话及短信；
- **未知号码**：拦截未知号码的来电；
- **呼叫转移**：拦截呼叫转移的来电；
- **海外号码**：拦截海外号码的来电；
- **智能拦截**：通过黄页数据库及拦截引擎进行骚扰电话和短信的过滤。

* 注：仅中国大陆地区提供黑名单地区、呼叫转移、海外号码功能；仅中国大陆地区及印度地区提供智能拦截功能。

4.2.5 私密空间

MIUI 为用户提供了私密短信、私密相册、私密文件夹与私密便签等一系列私密空间功能。

用户可以通过“设置”–“密码、隐私与安全”–“隐私密码”菜单进行设置，通过输入隐私密码或指纹密码解锁，打开私密短信、私密相册、私密文件夹和私密便签专有空间，用户在此空间中管理私密的联系人、相册图片、文件和便签。与私密联系人之间发送的短信、存储在私密相册中的图片、私

密文件夹中的文件以及私密便签的内容只在私密空间中展示，增强对用户隐私信息的保护。

用户也可以自行设置是否让私密短信在常规界面上显示通知。

如果用户设置了手机分身空间，上述功能会联动变化为：在分身空间中展示私密内容，在主空间展示常规内容。

05

互联网服务安全

Internet service security

5 互联网服务安全

针对运行在 MIUI 及其他小米应用上的互联网服务，小米严格遵循 Security by Design 和 Privacy by Design 原则进行设计，充分保障用户数据安全，并严格遵守隐私合规法律要求。在为用户提供便捷功能的同时，也给予用户相应的隐私选项，尊重用户的隐私权。

5.1 小米帐号

小米帐号是用来识别小米用户身份的标识。用户可通过小米帐号使用小米提供的一系列产品和服务，包括但不限于小米云服务、小米支付（Mi Pay）、小米商城、米家 APP、小米社区、小米音乐等。用户也可通过小米帐号购买米币以使用小米的各种虚拟产品和增值服务（如：游戏、电子书等）。

为防止未经授权的使用，小米采取如下技术手段和管理措施保障用户帐号安全。

5.1.1 帐号安全设置

用户注册或更换密码时，需设置字符长度为 8~16 位的强密码，至少包含数字、字母、特殊符号中的两种。成功登录后，在帐号安全设置里，用户可以绑定安全手机、安全邮箱，设置密保问题 * 及开启跨设备验证。在用户更改帐号信息或重置密码时，这些安全验证方式将被用来验证用户身份。

* 注：仅中国大陆地区注册的小米帐号支持此功能。

5.1.2 登录保护

小米帐号通过账号智能风控服务实现登录保护，有效降低用户帐号被非授权登录及帐号被盗刷的风险。

用户登录时，为保证登录安全，小米帐号会检测登录环境及用户操作方法，多次登录失败后，转为采用图片验证码、滑动或点选图片的交互验证方式进行环境安全检测。当识别为其他的异常登录行为时，如判定存在登录风险，则要求用户进行安全验证，如未通过，将根据风险等级，限制此帐号允许访问的服务。当识别为严重风险时，此帐号将被冻结，并被强制退出当前所有登录，当前密码也不可再使用或复用。

帐号智能风控服务定义的异常登录行为包括：

- 在非可信环境中登录小米帐号；
- 查看隐私数据（如：使用网页查看储存在小米云端的相册、短信、通讯录等）；
- 修改“帐号安全”中的设置（如：更换绑定手机或邮箱等）。

验证方式包括但不限于跨设备验证、短信验证和邮箱验证。

当用户帐号使用行为发生变更时(如: 修改密码、在新设备上登录小米帐号等),如判定有异常风险,小米将向用户发送电子邮件和短信通知,提示用户立即修改密码。

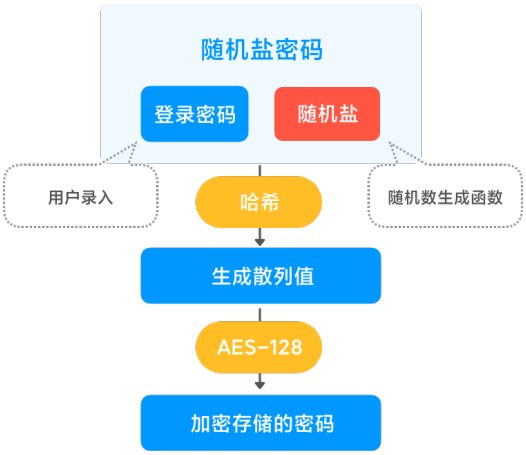
此外,小米帐号具备以下安全特性进一步保障帐号登录安全:

- 通过多种方式识别二次回收手机号。在引导新用户注册小米帐号的同时,禁止原用户使用此手机号登录小米帐号。
- 第三方应用调用小米帐号登录时采用 APP 白名单技术,只有被授权的应用才能调用小米帐号。
- 系统下发域名和 IP 时使用小米自主研发的接口,防止小米帐号在登录过程中受到 DNS 劫持攻击。

5.1.3 数据安全

小米将用户注册时录入的个人信息进行了数据加密,包括:

个人信息	加密方式
手机号码、电子邮箱、帐号 ID	AES-128 加密
登录密码	加盐哈希、AES-128 加密



利用随机数生成函数生成字符串(随机盐)附加到登录密码中,再通过密码散列函数(哈希)产生散列值后,采用 AES-128 算法进行加密。每个用户的随机盐是不同的,即使两个用户使用了同一个密码,最终生成的散列值也是不同的。

图 5-1 登录密码加密过程

在用户注册或登录小米帐号时,帐号相关信息均采用 HTTPS 加密通道向服务端传输。小米将用户个人信息加密后存储在专用数据库中,并进行多副本备份,备份数据的安全保护程度等同于在线数据。小米对用户数据进行基于角色的分级化访问控制,并接受相应的安全审计。

用户数据的加解密密钥统一由小米自主研发的 Key Center 密钥管理平台进行管理,该平台由独立团队负责运维,实现业务、数据和密钥的管理职责分离。基于角色的访问控制,保证任何个人无法

获得解密用户数据所需的所有权限。此外，存储用户数据的服务器和数据库还部署了实时监测机制，可以对异常访问行为进行告警。

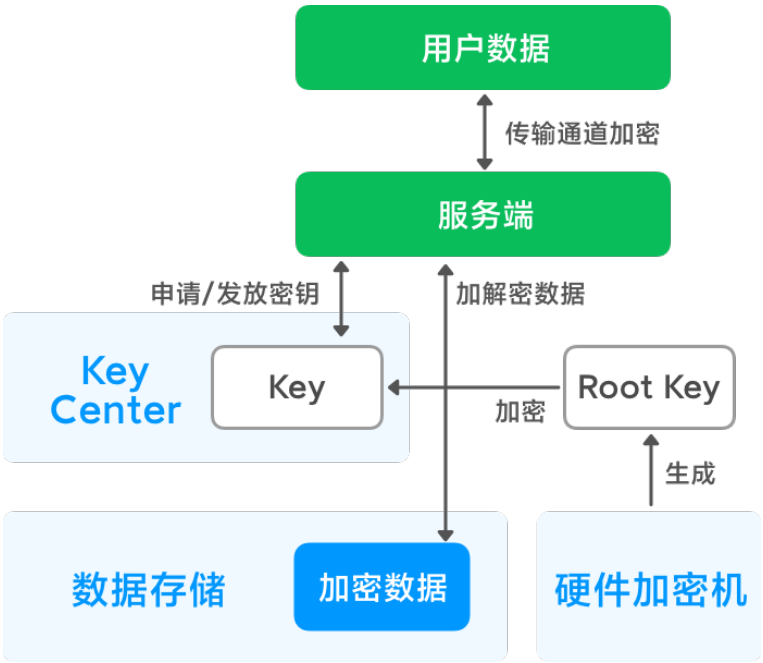


图 5-2 Key Center 密钥管理逻辑架构

为保证 Key Center 中存储密钥的安全，采用 4096 位的 Root Key 对其进行加密处理，而 Root Key 密钥则是由硬件加密机产生。

5.1.4 帐号登录的其他方式

- **扫码登录**

小米帐号提供扫码登录功能，用户可扫描网页上的二维码登录小米帐号。二维码超过一定时间会自动失效，用户需重新刷新二维码。

- **第三方授权登录**

小米帐号支持第三方帐号的绑定授权，用户可以使用第三方帐号登录小米帐号，目前国内支持微博帐号、微信帐号、支付宝帐号、QQ 帐号，海外支持 Facebook 帐号、Google 帐号。小米帐号采用 OAuth2.0（开放授权标准），并遵循标准的 OAuth2.0 协议和流程，以实现授权第三方帐号登录。OAuth2.0 的安全机制保障了小米帐号相关信息不会传递给第三方。

5.2 小米云服务

小米云服务可以储存用户的通讯录、短信、相册、通话记录、便签等信息，并让这些信息在用户的

设备间自动同步。同时，用户可以在手机损坏或丢失时尽可能挽回数据。用户可以随时随地在其他设备上或通过 web 端（https://i.xiaomi.com）浏览和管理自己的数据。

5.2.1 用户数据同步

用户主动开启小米云服务后，可选择同步以下数据内容，也可以随时设置关闭。

云服务同步模块	同步数据内容
短信同步	用户当前的电话号码
	用户的本地短信数据
	用户置顶的短信会话列表和私密短信的号码列表
通话记录同步	用户当前的电话号码
	用户的本地通话记录
联系人同步	用户的联系人信息、头像
便签同步	用户的本地便签
浏览器同步	用户的本地浏览器书签、历史记录、标签等
Wi-Fi 设置同步	用户连接的 Wi-Fi 设置数据

云服务同步模块	同步数据内容
录音同步	用户的本地录音及录音文件信息
桌面云备份	用户的桌面布局、壁纸
	用户设置的闹钟和世界时钟
	用户的通知管理
日历同步	用户的小米日历数据
相册同步	本地相册内的数据和用户指定同步的文件夹内的数据
小米云盘	用户上传的数据
音乐同步	用户 ID、播放歌单、播放音乐等
安全中心 / 手机管家	用户设置的通讯录黑白名单、VIP 名单、勿扰模式等
智能助理	用户在智能助理中的设置

5.2.2 智能照片分类

开启云服务时，手机将自动开启相册同步和智能照片分类功能。启用智能照片分类功能后，手机相册会对用户照片按照人物、地点、风景、植物、美食等多个维度进行自动分类和展示，用户也可以在“云服务”—“相册”中关闭此功能。

智能照片分类功能依靠图片智能算法和训练模型来实现，小米不会使用用户同步的照片数据来训练算法。算法在独立环境训练完成后内嵌在小米云服务端，照片自动同步到用户云空间后，调用图片智能算法模型对照片进行分类，将分类标签下发到手机相册中，打开相册即可浏览分类照片。

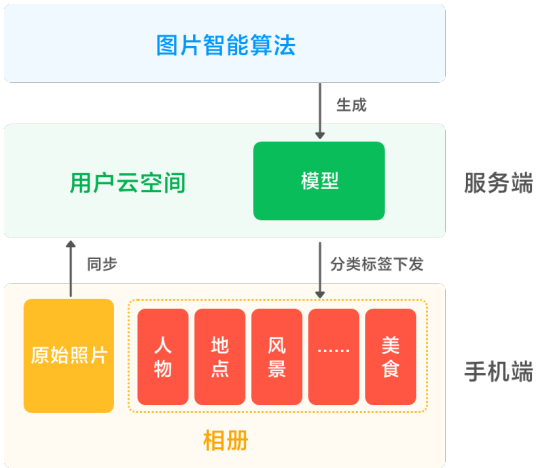


图 5-3 智能照片分类实现逻辑

5.2.3 数据安全

为防止用户数据被窃取或篡改，在数据同步过程中 web 端、手机端与服务端之间采用 HTTPS 加密通道进行传输。此外，云服务 web 端设置了 15 分钟超时自动退出机制。

在数据存储过程中，小米云服务将每个文件分为区块，每个文件区块均经过至少 128 位 AES 密钥单独加密后存储在服务器上，即没有密钥，即使直接拿到磁盘也无法解密数据。

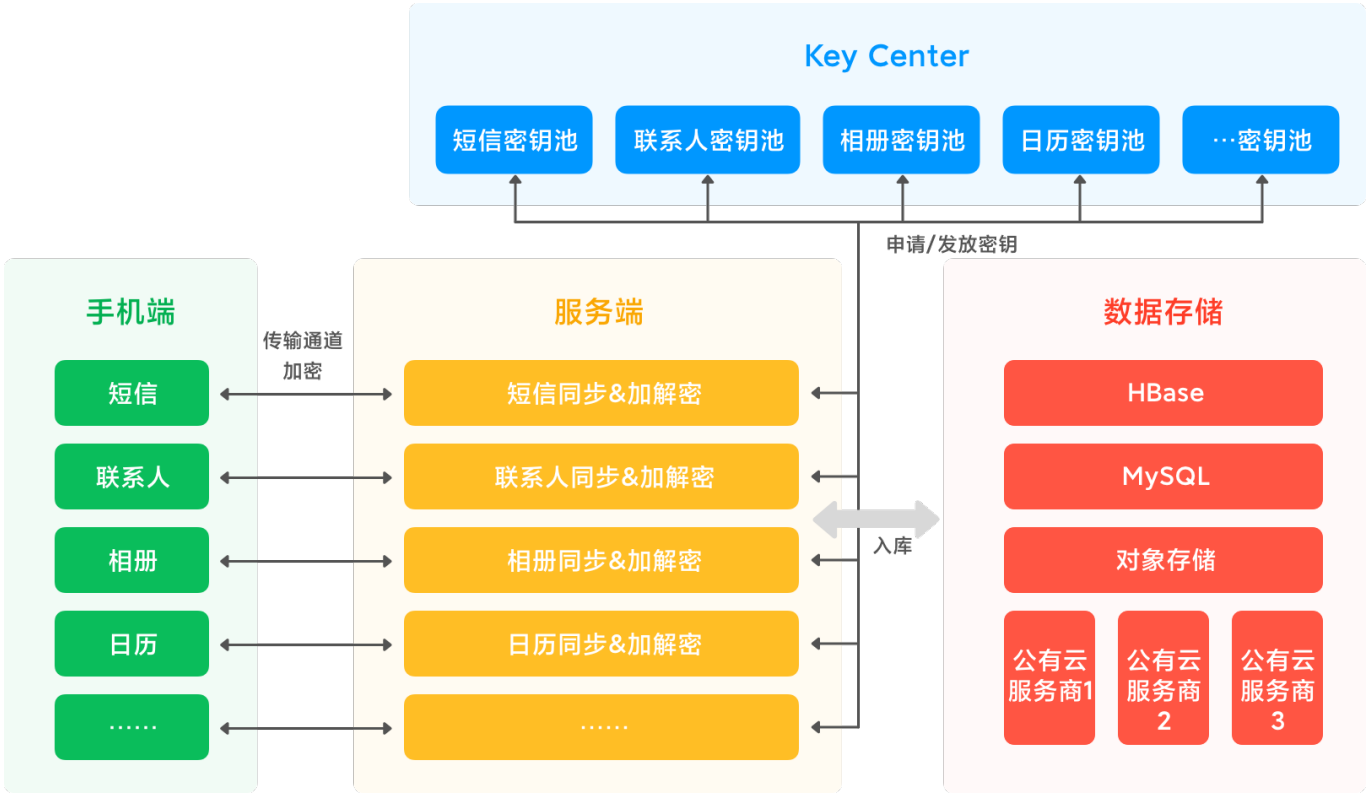


图 5-4 云服务数据安全架构

为防止用户云空间数据因不可抗力因素丢失，小米选择多家公有云服务商提供数据存储和备份服务。针对存储用户数据的公有云服务商，小米制定了严格的安全要求和评审规范，严苛地选择符合要求的服务商。小米仅将加密后的数据块存储在第三方公有云上，不会分享加密密钥。

5.2.4 用户数据删除

对于用户上传到云空间的数据，用户有权利对其进行更正或删除。当用户主动删除数据后，云空间的相应数据会被标记为已删除状态并暂存在回收站，在 30 天内，用户仍然可以通过回收站找回数据，以减少因误删除而导致的损失。

回收站中手动清空或超过 30 天自动清空的数据，将从服务端彻底删除，无法恢复。如果用户注销小米帐号，则云空间上的用户数据也将被彻底删除。

5.3 小米支付（Mi Pay）

Mi Pay 是小米钱包提供的手机支付服务。使用 Mi Pay 无需使用实体银行卡和银行密码，只需通过用户的指纹验证即可完成支付。为保证支付安全，在硬件层面，小米手机提供支付指纹信息的硬件加密与银行卡信息的安全存储，实现支付信息的物理隔离；在系统软件层面，发起支付时 MIUI 会自动检测支付环境是否安全可靠。同时，付款交易过程只在用户、商户和发卡机构之间发生，Mi Pay 服务在支付过程中并不会收集用户的任何交易信息。

5.3.1 Mi Pay 组件

- **安全元件**：安全元件（Secure Element，SE）是业内公认的、运行 Java Card 平台的认证芯片，它符合金融行业对电子支付的强制要求。
- **NFC 控制器**：NFC 控制器负责处理近距离无线通信(Near Field Communication,NFC)协议，在应用程序处理器和安全元件之间以及安全元件和销售点终端之间传输信息。
- **小米钱包**：用户可以在小米钱包中添加和管理银行卡，查看其添加的卡片和发卡机构提供的其他信息（如：发卡机构的隐私政策、最近的交易等），还可以在小米钱包中添加和管理交通卡、模拟门禁卡等 *。
- **TEE**：在小米手机上，TEE 负责管理用户指纹认证过程以保障支付交易的安全。
- **Mi Pay 服务器**：Mi Pay 服务器负责管理小米钱包中的银行卡、交通卡和模拟门禁卡的设置，以及储存在安全元件中的设备卡号。Mi Pay 服务器会和手机以及发卡机构服务器进行通信。

* 注：交通卡、模拟门禁卡功能仅部分机型支持此功能。

5.3.2 Mi Pay 安全元件

安全元件中包含用来管理 Mi Pay 的专用小程序，还包含由支付网络或发卡机构认证的小程序。支付网络或发卡机构发送的加密银行卡信息被储存在这些小程序内，并通过安全元件的安全性功能进行保护。交易期间，销售点终端使用专门的硬件总线，通过 NFC 控制器直接与安全元件进行通信。

5.3.3 Mi Pay NFC 控制器

作为安全元件的入口，NFC 控制器确保所有非接触式支付交易都通过处于设备近距离范围内的销售点终端进行，NFC 控制器只会将来自射频场内销售点终端的非接触式支付请求标记为可通信请求。

当用户使用指纹进行 Mi Pay 支付时，NFC 控制器会将安全元件内支付小程序准备的非接触式响应发送给射频场。交易的支付授权详细信息通过安全元件加密后直接发送给支付网络，不会透露给应用程序处理器。

5.3.4 添加银行卡

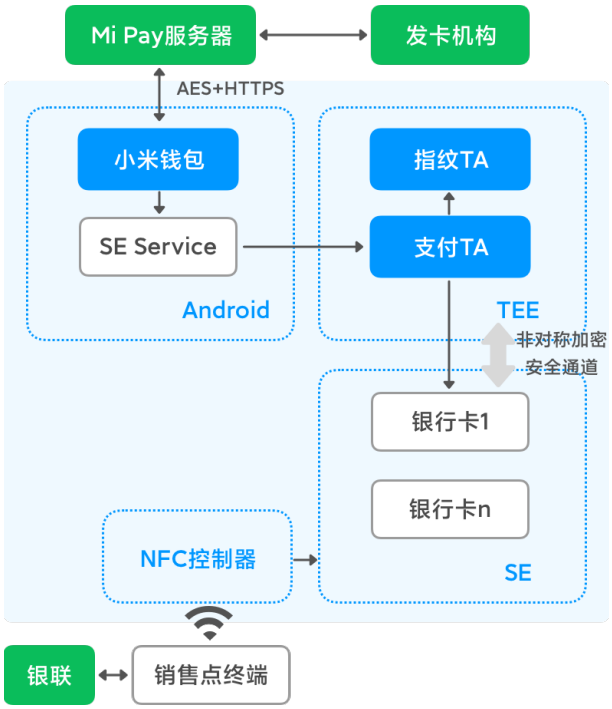
用户在 Mi Pay 中添加银行卡时，需要使用卡号、卡片有效期和 CVV 码等信息。用户可以在小米钱包中手动录入这些信息，也可以使用设备上的摄像头和 NFC 读写程序来自动录入，拍摄的银行卡识别信息成功录入后将立刻从内存中释放，不会保存在设备端或上传至服务器。

银行卡号信息输入完成后，小米钱包会将卡号发送到 Mi Pay 服务器再透传到发卡机构进行验证。验证通过后，小米钱包将向用户返回银行协议，仅当用户同意后才能继续添加流程。用户后续填写的银行卡其他信息，将通过“银联安全服务控件”加密后发送到 Mi Pay 服务器，并再次由 Mi Pay 服务器透传给发卡机构。同时，小米还会与发卡机构共享设备型号、SE 号，以及添加银行卡时用户大致位置（如果用户当前启用了“定位服务”）。发卡机构将会依据这些信息来决定是否批准将银行卡添加到用户 Mi Pay。

5.3.5 支付授权

在配备 TEE 的设备上，SE 仅在收到来自 TEE 的授权后才会允许进行支付操作。在小米手机上，用户使用指纹认证进行支付授权。

TEE 和 SE 之间通过串行接口连接，使用 ECC 加密算法进行签名认证确保通信安全。MIUI 为进一步增强支付的安全性保障，针对 Mi Pay 实施激活控制，默认要求必须验证指纹后才能使用 Mi Pay 中绑定的银行卡。



- TA 和 SE 均采用硬件级别的加密；
- TEE 和 SE 之间使用 ECC 加密算法进行签名认证，确保 SE 只接受来自本机 TEE 的授权信息，即使物理入侵 SE 卡也无法激活其中的银行卡；
- 银行卡在被调出使用前必须校验用户是否通过了指纹验证；
- 小米钱包客户端与 Mi Pay 服务器的数据通信采取 AES 加密后 HTTPS 传输的双重加密方式，防止被截获和篡改；
- 用户的指纹生物信息只会保存在手机的 TEE 中，无法被任何应用读取，也不会上传到服务器。

图 5-5 支付授权逻辑架构

5.3.6 暂停使用或移除银行卡

用户可以登录小米钱包，手动移除已添加的银行卡。针对已添加的“Mi Pay 银行卡”，当开启“查找手机”的“丢失模式”或“清除数据”功能时，Mi Pay 会通知发卡机构进行自动注销。即使设备未接入网络，支付网络或发卡机构也可停用其支付功能。此外，用户还可以通过致电发卡机构来暂停使用或移除该银行卡。

5.4 小爱同学

用户可通过说出“小爱同学”来唤醒支持的智能设备，以实现语音对话、天气查询、拨打电话、控制智能家庭设备等。开发者基于 AI 技术的小米语音引擎，可以使用户在手机、电视、音箱等硬件设备上实现语音交互。

5.4.1 基础架构

小米语音引擎主要由以下模块构成：

1）语音识别（Automatic Speech Recognition，ASR）模块负责将采集到的人类语音转化为文本；

2）语义处理（Natural Language Processing，NLP）模块负责对文本进行处理和理解，结合语境和对话，转为结构化的查询表达式；

3）智能搜索和执行（Intelligence Search Engine & Execution，ISEE）模块负责通过文本转换而来的指令，对智能家庭设备进行控制，或搜索各垂直领域的优质内容和服务（如：音乐播放、天气查询等），返回最符合用户需求和当前语境的查询结果；

4）语音合成（Text To Speech，TTS）模块通过文本转语音，将智能搜索返回结果转换为语音回答，再结合以上模块，实现流畅、自然的人机交互。

小爱同学基于小米语音引擎，集成第三方的内容、服务以及 AI 技术，可通过统一的 API 和 SDK 对外提供服务，系统架构如图所示：

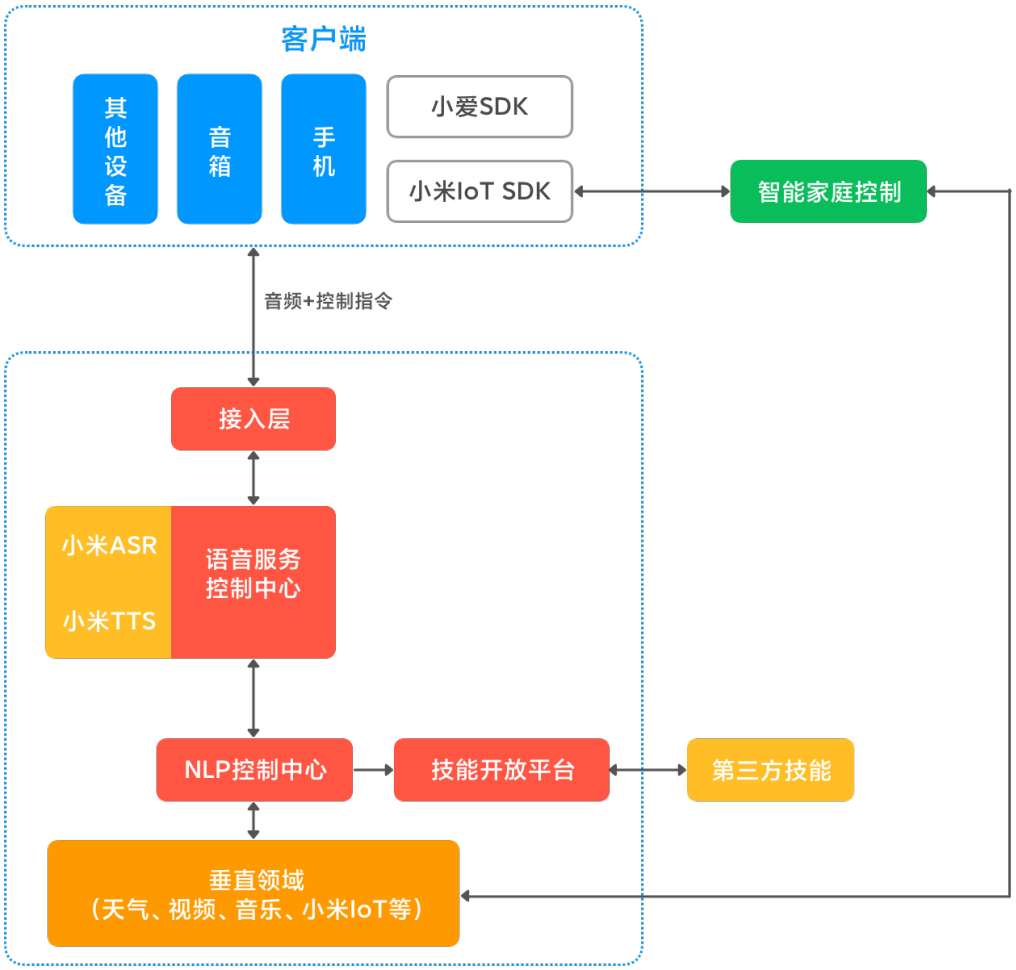


图 5-6 小爱同学基础架构

5.4.2 语音唤醒与识别

当用户说出“小爱同学”时，设备端开始记录用户语音，录音（包括后续的语音指令）会被上传至服务端。在小爱同学未被唤醒的状态下，传入麦克风的声音不会被记录和上传。

当用户使用小爱时，登录的小米帐号 ID、终端设备标识符的哈希值等可标识用户身份的信息将通过传输层加密上传。在服务端，这些信息不会与用户的录音内容直接关联，小米帐号 ID 会被映射为假名化的随机 ID，此 ID 映射关系表加密后单独保存在与用户其他数据隔离的数据库中，密钥则保存在 Key Center。在小米内部，任何人均不会被同时授予 ID 映射关系表和密钥的访问权限。

上传到服务端的录音片段会通过语音识别模块进行语音模型训练，用于优化语音唤醒和语音识别的准确度。这些录音片段仅关联到上述经过随机化和加密处理的 ID，无法识别用户身份。

小爱语音助手的用户可以为自己录制声纹 *，用以实现仅预设声纹匹配的用户可以唤醒设备。声纹的特征信息也是仅关联到上述经过随机化和加密处理的 ID，无法识别用户身份。

升级到小爱同学 v4.8 版的用户可通过 MIUI 或语音设备 APP 中的隐私开关 * 进行以下设置：

- 是否上传唤醒音频和声纹信息并用于语音唤醒优化；

- 是否将语音数据用于语音识别优化。

* 注 1：仅部分机型和音箱支持此功能。

* 注 2：部分设备隐私开关的设置路径和内容不同。

5.4.3 拨打电话

当用户使用小爱同学给通讯录中的联系人拨打电话时，小爱同学会根据用户说出的联系人姓名，从通讯录中筛选出最接近的一个或一组。筛选出的数据采用 AES-128 加密后经过传输层加密上传至服务端，经语义理解模块处理后下达到设备端进行号码匹配和电话拨打。拨打电话过程中，通讯录中的联系人号码不会被上传，且联系人姓名数据不会被存储到服务端。

此外，为提升语音识别准确度，用户可通过 MIUI 或语音设备 APP 中的隐私开关，设置是否通过语音识别模块对通讯录中的姓名数据进行训练，姓名数据不会被上传至服务端。

5.4.4 语音播报

当用户开启语音播报功能时，小爱同学可帮助用户播报短信、未接来电以及微信消息等，语音合成模块仅在设备端运行，消息内容和用户数据均不会被上传至服务端。

5.4.5 智能家庭设备控制

对于支持小爱同学功能的智能家庭设备，在用户使用同一小米帐号登录时，可通过小爱同学对其进行控制。

当用户向终端设备发出语音指令 *，小爱同学会和米家服务端进行关联，并获取小米帐号下智能家庭设备的名称、房间、状态等信息，以执行控制操作。小爱同学服务端存储这些信息，仅用于设备控制，不会用于分析用户生活起居习惯或兴趣爱好。

* 注：使用小爱同学控制小米电视时，需要通过设备端蓝牙或 Wi-Fi 扫描附近的小米电视，获取 MAC 地址，以实现设备匹配。

5.4.6 数据最小化

小爱同学收集和分享用户数据均严格遵循数据最小化原则，仅为实现业务功能而收集或分享最少的数据字段，例如：

- 小爱同学支持基于 OAuth2.0 协议的第三方授权登录，用户可通过小爱同学查询外卖和快递信息(如: 美团外卖和菜鸟裹裹)，小爱同学仅在用户每次查询时调用第三方接口，反馈查询结果，不会获取、存储、使用任何来自第三方的订单信息和快递信息；
- 作为 ASR 与 TTS 能力的备用资源，小米在特定场景下会与外部服务提供商合作以使用其 ASR、TTS 能力（如: 多语言翻译），在调用相关 API 等接口时，除待识别音频与待合成文本外，小爱同学不会向合作方提供任何其他用户个人信息。

5.4.7 数据安全

所有数据在用户设备终端、服务端、第三方之间传输时，均通过 HTTPS 或密钥加密的 WebSocket 进行传输层加密。

用户的小米帐号 ID、设备标识符，以及上文提到的随机 ID，均采用 AES-128 加密后存储至数据库中，加解密的密钥存于 Key Center 中。小米对用户数据进行基于角色的分级化访问控制，并接受相应的安全审计。

5.5 图像智能

图像智能基于智能视觉处理技术为 MIUI 用户提供智能相册、图像识别、智能相机等服务：

- 智能相册可帮助用户便捷地编辑、管理和使用图片。提供的功能包括：美食、风景、人物等多种场景的一键美化；更换背景、智能裁剪、魔法消除等智能编辑；生成分类相册以帮助用户管理存储空间；图像识别与图片搜索以帮助用户快速定位并使用相册中的图片。
- 智能相机预置了多种优化的拍照算法。提供的功能包括：基于场景识别算法的场景优化，实现特殊偏好匹配与精细化画质调教；通过算法识别年龄性别后，匹配不同的美颜参数方案进行

人像优化，实现千人千面的美化效果；短视频特效以帮助用户快速生成类似微电影效果的成品视频。

5.5.1 AI 算法训练和使用

图片智能算法在研发环境中进行训练，训练完成后的算法模型内嵌到 MIUI 的相册、相机中，模型的迭代通过相册、相机的版本升级实现。小米不使用用户个人信息进行算法的开发、测试与优化。

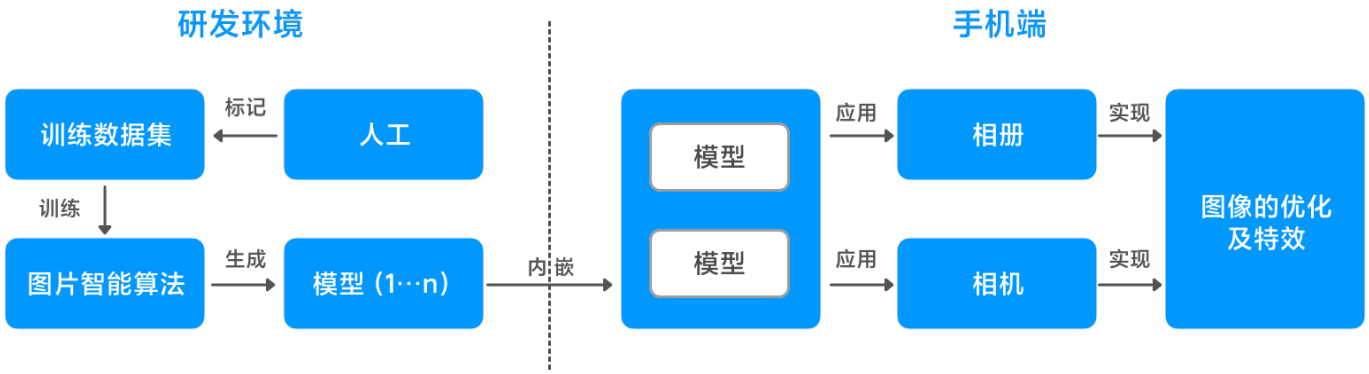


图 5-7 AI 算法逻辑架构

5.5.2 数据安全

当用户使用图像智能提供的服务时，小米仅收集提供服务所必须的用户数据，且所有功能将优先在设备端实现。若用户选择使用云服务的智能照片分类功能时，用户数据将被以加密的方式上传至服务端，具体参见本文 5.2.2 章节。

5.6 位置服务

小米位置服务为运行在 MIUI 上的小米及第三方应用和网站提供基于设备的定位能力，包括 GPS 定位、网络定位和融合定位，各类定位收集的信息如下：

- GPS 定位：通过卫星定位设备，收集的信息包括：设备标识符和经纬度信息；
- 网络定位：网络定位收集的信息包括：Wi-Fi 热点信息和基站信息。

Wi-Fi 热点信息包括：连接的和扫描到的 AP 的名字(SSID)、MAC 地址(BSSID)、信号强度(RSSI)、信道（FREQUENCY）；

基站信息包括：连接的和扫描到的基站的移动国家号（MCC）、移动网络号码（MNC）、位置区码（LAC）、小区代码（CID）、信号强度（RSSI）。

- 融合定位：以 GPS 定位为基础，可进一步叠加网络定位数据和传感器数据进行定位。

当用户开启位置服务且有应用调用定位时，位置服务会将设备附近 Wi-Fi 热点信息及基站信息，

以匿名及加密的方式上传至服务端，此部分数据将用于扩充 Wi-Fi 热点和基站位置的众包数据库，无法用于识别用户身份。

位置服务所收集的数据均通过有鉴权机制的 API，经过 AES-128 加密（其中 AES 会话密钥通过 Pre-shared key 方式与服务端交互）和 Base64 编码后，再通过 HTTPS 传输。

用户可通过 MIUI“系统安全”-“隐私设置”-“位置信息”菜单的“开启位置服务”开关设置是否开启位置服务。

5.7 小米推送

小米推送（MiPush）通过在云端与客户端之间建立一条稳定、可靠的长连接，为开发者提供向客户端应用实时推送消息的服务。

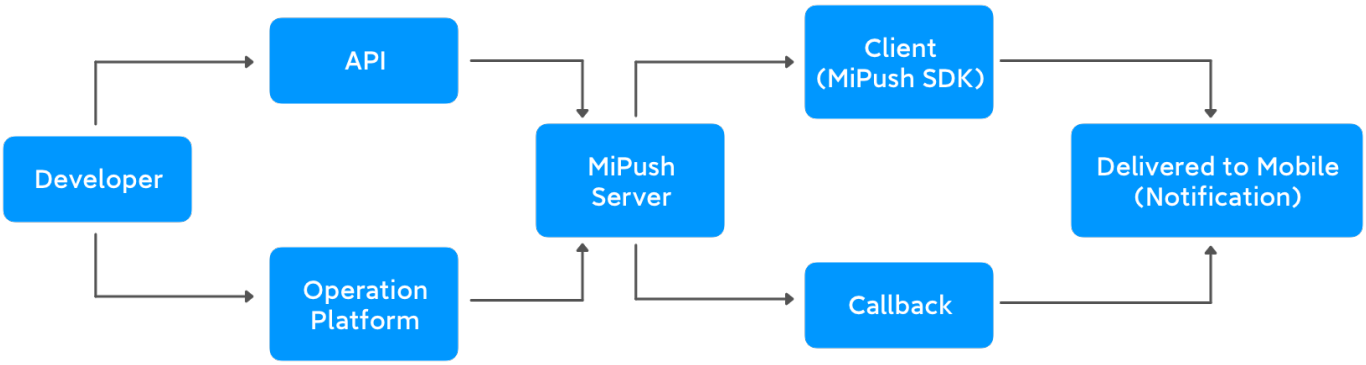


图 5-8 小米推送服务架构

小米推送支持通知栏消息和透传消息两种消息类型，同时提供 API 接口和推送运营平台两种消息下发途径。小米推送 SDK 覆盖 Android、iOS 客户端及服务端主流语言，可以帮助开发者更好的结合自身业务逻辑，满足复杂业务场景需求。

5.7.1 开发者隐私合规要求

小米通过开发者协议，规范开发者对终端用户个人信息的保护：

- 开发者在使用小米推送服务时，须同意小米推送按照小米隐私政策收集、存储、使用、披露和保护个人信息。
- 开发者必须制定、发布其隐私政策并获得终端用户同意，且该政策应确保不低于小米推送的隐私保护标准。
- 小米强烈建议开发者，在其面向终端用户的产品隐私政策中加入小米隐私政策的关键条款，以确保终端用户同意小米推送服务收集并使用数据。如果未取得终端用户同意，开发者不应继续使用小米推送服务。

- 小米要求开发者遵守适用于保护终端用户个人信息相关的法律法规、政策和行业标准，并确保其适用于小米推送服务。

5.7.2 设备标识方法

小米推送不直接使用设备标识符（如：IMEI）来标识设备，而是通过去标识化等技术手段对用户个人信息进行处理。小米推送在设备端对三个设备标识字段（设备标识符、序列号、安卓 ID）进行哈希后，将生成的字符串上传至服务端，服务端将此字符串映射至随机生成的 ID 返回给客户端。小米推送将此随机 ID 作为设备的唯一标识推送消息。

5.7.3 数据最小化

小米推送只作为消息通道，不对消息内容、用户行为和偏好等进行挖掘使用；小米推送的原始数据、中间数据和统计结果均不会提供给小米合作方，也不允许合作方以任何形式访问这些数据；小米推送仅为开发者提供包括时间、消息维度的后台统计数据，不提供任何用户个人信息。

5.7.4 数据传输安全

接入小米推送服务的设备端 APP 首次向服务端发起注册请求时，会将设备信息（设备标识字段经过不可逆哈希）上传至服务端，服务端返回随机 ID 和消息内容密钥，此过程采用 HTTPS 加密通道进行数据传输。

小米推送服务要求开发者使用 HTTPS 加密通道将消息内容发送到服务端，服务端各模块之间的通信采用 AES-128 加密，推送到设备端的消息经过对称加密算法加密后，通过服务端和设备端之间建立的 AES-128 加密通道的双重加密，将消息推送到设备端。

5.7.5 数据删除

消息推送成功后，消息内容将在服务端删除。如因异常情形导致消息未送达，服务端会将消息内容保留 14 天；小米推送服务向开发者提供用户数据删除接口，开发者可调用此接口删除此 APP 在小米推送的注册信息；当设备 90 天内没有连接网络，此设备相关的消息内容也会从服务端删除；开发者停止接入小米推送服务或要求停止推送服务时，小米根据开发者指示删除所有相关 APP 的信息。

06

安全认证与隐私政策

Security certification and privacy policy

6 安全认证与隐私政策

小米公司以尊重和保护用户隐私与安全，致力于打造让用户信任的产品，享受科技的乐趣为目标。

为确保信息安全与隐私保护策略的贯彻执行，小米在 2014 年就正式成立信息安全与隐私委员会，通过技术防护、流程制度、评估和审查机制等建立了完善的安全管理体系。同时，小米聘请了欧盟当地的资深律师作为欧盟业务的数据保护官，以确保小米符合各国法律法规的要求。

为向用户提供符合法律法规及业界标准要求的业务运行环境及服务，小米已开展全球化合规治理工作，并接受外部监管机构的定期审查。小米互联网服务遵循网络安全等级保护要求，已通过了网络安全等级保护三级; 支持 MIUI 产品和服务的基础架构、开发、运维及互联网服务遵循国际权威认证体系，已通过了英国标准协会(BSI)的 ISO27001、ISO27018 和 ISO29151 认证; MIUI 操作系统及其内置应用、云服务已经过全球领先的数据隐私管理公司 TrustArc 审核与确认，小米的隐私政策和隐私实践符合 TrustArc 企业隐私与数据治理实践评估标准，并被授予 TrustArc 认证的隐私印章。

ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。

ISO 27018是专注于云中个人数据保护的国际行为准则。通过ISO 27018认证，表明Mi Cloud已拥有完备的个人数据保护管理系统。

ISO/IEC29151:2017认证是国际通行的个人身份信息保护指南。通过ISO/IEC29151:2017认证，小米向用户证明了自己的信息安全保障能力和对个人数据隐私保护的能力。

国际上权威的隐私合规评估机构，整合了各国隐私合规要求，通过其认证表明小米建立了完备的隐私合规体系，具备了国际公认的隐私数据保护能力。

网络安全等级保护是公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵循的通用安全标准。小米互联网服务通过了网络安全等级保护三级，遵循网络安全等级保护要求进行网络安全建设。

小米尊重并保护所有用户的个人隐私权，通过隐私政策详细介绍小米如何收集、使用、披露、处理和保护您在使用小米产品和服务时，提供给我们或我们收集的信息。不同语言版本的隐私政策链接: https://privacy.mi.com/all.

* 注：部分产品有单独的隐私政策链接，可在对应产品页面查看。

小米拥有一支专业的安全与隐私团队，负责为小米产品的安全与隐私提供技术支持，为开发中和已发布的产品提供安全与隐私审核和测试。同时，小米通过自建的小米安全中心 (SRC)、Hackerone 及邮箱等多种途径，向全球的安全研究者征集安全问题和安全情报，并依据问题或情报级别给予不同

金额的奖金。同时小米通过“小米智能生活安全守护计划”主动邀请安全研究者对小米产品进行安全测试，并给予高额奖金。小米会将已确认的安全问题列为高优先级事项并尽快解决。

小米安全中心联系方式：https://sec.xiaomi.com/、https://hackerone.com/xiaomi、security@xiaomi.com。

07

结束语

Peroration

7 结束语

小米公司致力于为全球的个人、家庭和行业用户提供功能完善、安全且易用的数字化软硬件产品，MIUI 作为小米手机的核心组件，肩负着构建可信根基、提供安全保障的责任。MIUI 将增强安全性放在重要位置，本文即是 MIUI 安全设计与实现的一次综合呈现。

小米力图将安全和隐私保护意识根植到每一个业务部门、每一位员工、每一位合作伙伴的心中。如前文提出，小米已建立完善的安全与隐私管理体系，将安全与隐私的要求融入到产品的设计、开发、测试、运营等环节中，并对合作方进行严格的安全和隐私审核，积极地监控和解决新增的安全问题和威胁，以确保用户数据得到全生命周期的保障。为了应对不断演进的安全态势，小米将不断提升安全技术能力、完善产品和服务的安全和隐私保护功能、优化安全与隐私管理体系，并持续通过权威认证、白皮书、隐私政策等方式展示出来，建立用户对小米的产品和服务的信心，使用户更加放心地选择和使用小米的产品和服务。

在这个以大数据和人工智能为主要趋势的时代，企业发展和用户隐私是会存在一些矛盾的，但小米坚信只有做到足够的对用户信息安全与隐私的尊重和保护，才能换取用户对小米产品的长期信赖。因此小米坚持把信息安全与隐私保护放在第一位，不断加大在安全与隐私上的投入，并致力于将小米在信息安全与隐私保护方面的规范做法、最佳实践、技术能力输送给合作伙伴，共同发展、共同守护用户隐私。

08

缩略语定义表

Abbreviation definition table

8 略缩语定义表

英文缩写	中文全称	释义
3DES	三重数据加密算法	DES 加密算法的一种模式，它使用 2 个不同的 56 位密钥对数据进行三次加密。
AES	高级加密标准	一种常用的对称加密算法，采用对称分组密码体制，密钥长度可以为 128、192 或 256 位。
AI	人工智能	研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。
API	应用程序接口	是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码。
ASR	语音识别	把采集到人类语音精准转化为文本。
AVB	安卓验证启动	是 Android 一个重要的安全功能，主要是为了防止启动镜像被篡改，提高系统的抗攻击能力。
BL	引导程序	是嵌入式系统在加电后执行的第一段代码，在操作系统内核运行之前运行，用于初始化硬件设备。
CVV	信用卡验证值	信用卡上的一组 3 位或 4 位数字，相当于信用卡的身份证，用户可以凭此码进行消费交易。
ECC	椭圆曲线密码	一种非对称加密算法，基于椭圆曲线数学，比其他的非对称加密算法使用更小的密钥提供相当的或更高等级的安全。
ECDSA	椭圆曲线数字签名算法	是使用椭圆曲线密码对数字签名算法的模拟。
FBE	文件级加密	Android 7.0 及更高版支持的一项加密技术，可以使用不同的密钥对不同的文件进行加密，并且可以对这些文件进行单独解密。
Flash	闪存	一种电子式可清除程序化只读存储器的形式，允许在操作中被多次擦或写的存储器。

英文缩写	中文全称	释义
Fuse	用户空间文件系统	类 UNIX 系统平台上可加载的内核模块，允许非特权用户创建功能完备的文件系统，而不需要重新编译内核。
HMAC	哈希信息认证码	一种基于哈希函数和密钥进行消息认证的方法。
HTTPS	超文本传输安全协议	是一个安全通信通道，用于在客户计算机和服务器之间交换信息，使用安全套接字层进行信息交换。
HUK	设备唯一密钥	出厂时固化在设备主板上的用于标识和验证该设备唯一性的一个密钥。
KASLR	内核地址空间布局随机化	一种确保内存地址和偏移量不可预测的技术，可以极大降低恶意软件攻击的成功率，提升系统安全性。
MDM	移动设备管理	对移动设备注册、激活、使用、淘汰各个环节进行完整的全生命周期管理。
NFC	近距离无线通信	是一种短距高频的无线电技术，在 13.56MHz 频率运行于 20 厘米距离内，由非接触式射频识别演变而来。
NLP	语义处理	对文本进行处理和理解，并转为结构化的文本。
OAuth	开放授权协议	为用户资源授权提供了一种安全简单的标准，用户在访问第三方 web 或应用的时候，第三方不会知道用户的信息（登录密码等）。
OEM	原始设备制造商	受托厂商按来样厂商之需求与授权，按照厂家特定的条件而生产，所有的设计图等都完全依照来样厂商的设计来进行制造加工。
OS	操作系统	管理计算机硬件与软件资源的程序，同时也是计算机系统的内核与基石。
OTA	空中下载	通过移动通信的空中接口实现对移动终端设备及 SIM 卡数据进行远程管理的技术。
Pre-shared key	预共享密钥	在加密和解密发生之前，保证服务端和客户端均持有相同的密钥。
ROM	只读存储器	一种只能读出事先所存数据的固态半导体存储器。

英文缩写	中文全称	释义
Rootkit	/	是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息。
RPMB	重放保护内存块	是闪存芯片中的一个具有安全特性的分区。
RSA	公开密钥密码体制	一种非对称加密算法，使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。
SE	安全元件	提供私密信息的安全存储、重要程序的安全执行等功能。其内部组件包含有：CPU、RAM、ROM、加密引擎、传感器等。
SELinux	安全增强 Linux	是一个 Linux 内核模块，也是 Linux 的一个安全子系统。
SHA	安全哈希算法	是一个密码散列函数家族，是 FIPS 所认证的安全散列算法。SHA 家族有五个算法，分别是 SHA-1、SHA-224、SHA-256、SHA-384，和 SHA-512。
SoC	片上系统	是在单个芯片上集成一个完整的系统，对所有或部分必要的电子电路进行包分组的技术。
TA	可信应用	在 TEE 环境中运行的，安全性较高的应用程序。
TEE	可信执行环境	移动设备主处理器上一个安全区域，与移动 OS 并行存在，提供一个隔离的执行环境，保证隔离执行、可信应用的完整性、可信数据的机密性、安全存储等。
TTS	语音合成	即“从文本到语音”，是人机对话的一部分，将文本合成转化为自然语音输出。
UI	用户界面	系统和用户之间进行交互和信息交换的媒介，它实现信息的内部形式与人类可以接受形式之间的转换。

英文缩写	中文全称	释义
WebSocket	/	在单个 TCP 连接上进行全双工通信的协议。允许服务端主动向客户端推送数据。客户端和服务器只需要完成一次“握手”，两者之间就直接可以创建持久性的连接，并进行双向数据传输。


MIUI 11
效率革新 声色双全