MagicOS 8.0 安全技术白皮书

发布日期 ： 2024-01-10

HONOR

商标声明

HONOR和其他荣耀商标均为荣耀终端有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受荣耀公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，荣耀公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

荣耀终端有限公司

地址：深圳市福田区香蜜湖街道东海社区红荔西路8089号深业中城6号楼A单元3401

网址：https://www.hihonor.com

客户服务电话：4006966666

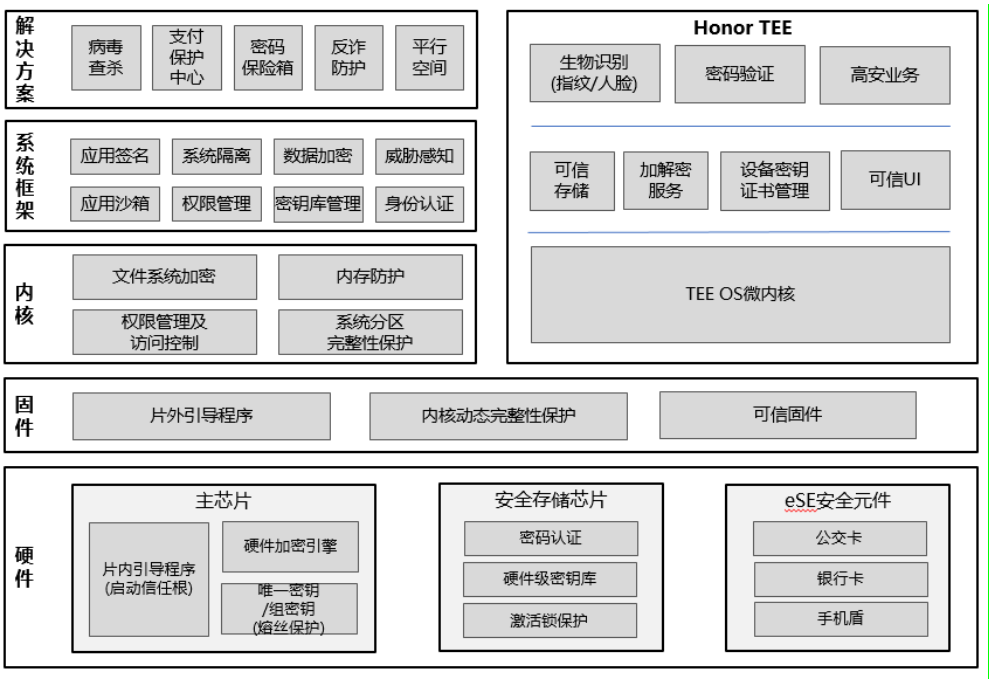
目录

注：*表示不是所有设备都支持该特性。由于不同型号或不同国家市场特性的差异，具体以产品说明为主。本文其他地方不再单独说明。

概述

简介

MagicOS 以数据为中心、基于芯片和安全性硬件为基础软硬件结合的安全平台，为用户的数据安全及隐私保护提供完整的解决方案（整体架构如下图所示），提供从硬件、系统、应用到云的端到端安全保护包括：硬件芯片、可信执行环境、系统内核、数据、应用、网络、互联、服务的安全以及隐私保护。



MagicOS 安全架构

MagicOS 从底层硬件芯片开始提供安全启动机制来保证 ROM 镜像不会被篡改，ROM 镜像必须经过签名校验才能在设备上正常运行，保证了设备 Bootloader、Recovery 以及 Kernel 镜像的启动安全，防止启动过程中攻击者对系统的篡改和恶意代码植入，从而确保从硬件芯片到软件系统启动过程的安全。

为保证数据安全，用户数据基于硬件提供的设备唯一密钥（Hardware Unique Key，简称 HUK）和用户的锁屏密码进行加密，不同的应用之间的数据文件存储在应用自己的文件沙箱内，其它应用无法访问。在设备回收或恢复出厂设置时，提供安全擦除功能来永久清除数据，避免数据被非法恢复。同时 MagicOS 与云服务的结合，帮助用户进行数据的备份和同步以保证数据的安全。

为保证应用安全，除了安全沙箱和权限管理等安全机制外，MagicOS 通过预置系统管家提供病毒查杀、骚扰拦截、流量管理等功能，安装应用时会自动检测应用是否存在威胁（如病毒、木马、恶意软件等），并对应用提供细粒度的权限管理、流量管理。

本文主要从以下几个章节进行阐述：

- 硬件安全：安全启动、硬件加解密引擎及随机数发生器、设备唯一密钥、设备组密钥、安全元件
- 可信执行环境：安全 OS、可信存储服务、加解密、设备证明等
- 系统安全：完整性保护（HKIP 内核完整性保护、完整性度量机制、系统软件更新）、内核安全（系统访问控制能力、内核地址空间布局随机化）、身份认证

- 数据安全：通用密钥库、锁屏密码保护、数据加密保护、安全擦除、密码保险箱
- 应用安全：应用签名验证、应用沙箱、应用运行时保护、安全输入、应用威胁检测、恶意网址检测、短信验证码保护
- 网络与通信安全：VPN、TLS、无线局域网安全、防伪基站
- 设备互联安全：同一荣耀账号 MagicOS 设备互联安全、IOT 设备互联安全
- 服务安全性：荣耀账号、查找设备&激活锁、支付保护中心、移动设备管理 API
- 隐私保护：权限管理、隐私访问记录、录音/录像提醒、定位服务、设备标识符体系、差分隐私、隐私政策声明
- 由于 MagicOS 最终用于不同硬件芯片平台的产品，因此在不同硬件及芯片上提供的安全实现方式并不完全相同，不同设备的实际规格以产品手册为准。

硬件安全

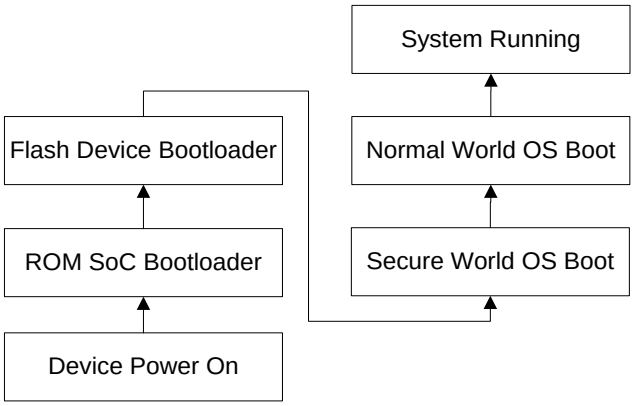
MagicOS 采用了基于硬件芯片的安全能力，并辅以安全的软件解决方案提供整体安全性，其中硬件芯片安全是 MagicOS 安全体系的核心。本章节主要阐述荣耀设备的硬件芯片安全，包括如下关键安全特性：

安全启动

安全启动是防止设备在启动过程中加载并运行未经授权应用的安全机制。启动程序通过签名公钥验证软件的数字签名，确保软件的完整性和可信性。只有通过签名校验的镜像文件才可以加载运行，这些文件包括启动引导程序、内核镜像、基带固件等镜像文件。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。

设备启动时最初执行的是固化在芯片当中的一段引导程序，称作片内引导程序（ROM SoC Bootloader）。这段代码在芯片制造时被写入芯片内部只读 ROM 中，出厂后无法修改，是设备启动的信任根。

片内引导程序执行基本的系统初始化，从 Flash 存储芯片中加载二级引导程序（Flash Device Bootloader）。使用保存在主芯片内部 Fuse 空间（熔丝工艺，一旦熔断不可更改）的公钥哈希对公钥进行验证后，片内引导程序再利用公钥对二级引导程序镜像的数字签名进行校验，成功后运行二级引导程序。二级引导程序加载、验证和执行下一个镜像文件。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，防止未经授权的程序被恶意加载运行。



MagicOS 产品支持 Verified Boot 功能。在对开启 Verified Boot 保护的只读系统分区进行访问时，系统会使用构建只读分区镜像时生成的完整性保护信息校验所访问区域的完整性。此特性有助于防止恶意软件永久驻留系统分区，确保用户在启动设备时处于与上次使用时相同的状态。

硬件加解密引擎及随机数发生器

为了满足高性能加解密及密钥保护的需求，MagicOS 会使用硬件安全引擎进行数据加解密及密钥派生等操作。芯片提供了高性能的硬件加解密加速引擎，支持的主要算法及功能如下（包括但不限于）：

- 3DES、AES128、AES256
- SHA1、SHA256
- HMAC-SHA1、HMAC-SHA256
- RSA1024、RSA2048、RSA3072、RSA4096
- ECDSA-P256、ECDH-P256
- ED25519、X25519
- 国密 SM2、SM4
- 符合 NIST SP800-90A 标准的 CTR_DRBG 随机数发生器及满足 NIST SP800-90B 标准要求的硬件熵源

设备唯一密钥

设备唯一密钥是在芯片内部固化的一个唯一标识。由于具备只能被硬件加解密引擎用于密钥派生且每个芯片都不相同的特性，设备唯一密钥为 MagicOS 的密钥设备唯一性提供了保证。锁屏密码保护和文件系统加密等功能均使用到了此特性。

设备组密钥

设备组密钥是在芯片内部固化的一个标识，具有只能被硬件加解密引擎用于密钥派生且同一类设备的设备组密钥相同的特性。使用设备组密钥使得 MagicOS 在同一类设备能派生出相同的密钥。

StrongBox*

StrongBox 是一种基于硬件的密钥管理功能，对侧信道攻击、半侵入式攻击有着更好的防御能力。应用可以通过 StrongBox 提供的接口，使用更加安全的方式来保护自己的密钥。荣耀产品通过使用安全元件或独立安全存储芯片，已支持 StrongBox 功能，提供了更加安全的密钥管理措施，为 Passkey 等数字身份认证业务提供更强的保护措施。

安全元件*

安全元件（Secure Element）是一个提供安全执行、数据存储保护并经过业内安全认证的芯片，满足移动金融支付的安全要求。安全元件拥有独立的内存、持久化存储介质、加密/解密逻辑电路、处理器以及软件系统等，可保障在内部运行的应用及数据安全，抵御外部攻击。荣耀产品支付功能也使用了安全元件来保证支付交易的安全性，安全元件通过了 CC EAL6+（硬件）、EAL5+（软件）安全认证，以及 EMVCo 等国际标准认证。

*注：此功能仅在部分芯片型号的产品上提供。

手机盾*

荣耀产品支持的手机盾功能采用安全元件，支持银行的手机证书业务，将传统的 USB 插拔式 U 盾与手机结合，变为随身携带的手机盾，为电子支付提供金融级的硬件保护。

在用户开通手机盾时，MagicOS 的可信服务管理平台（TSM）会作为安全元件的管理者，手机上的功能模块通过与安全元件建立安全协议通道（SCP）进行通信，在安全元件内开辟可信、独立的安全运行空间。随后银行应用将在该安全空间生成用于交易使用的密钥对和证书，并要求用户设置 PIN 码保护。

用户在使用手机盾时，首先通过可信 UI 界面输入 PIN 码进行认证通过后安全元件会使用开通过程中生成的私钥对用户的交易请求进行数字签名。银行交易系统在处理该交易请求时进行验签，确保交易的安全。

用户在注销（关闭）手机盾时，系统会直接销毁安全元件中存储的钥密钥对，且不可恢复。

从证书公私钥产生到证书销毁，整个生命周期内，证书私钥将始终位于安全元件内，保障证书密钥安全不泄露。

独立安全存储芯片*

荣耀部分产品使用了与主芯片独立的安全存储芯片，该芯片符合硬件级 CC EAL5+安全认证标准，拥有独立的内存、持久化存储介质、处理器、硬件加解密引擎以及软件系统，进一步增强锁屏密码验证、生物特征数据、激活锁数据的保护，保障用户的数据安全。

可信执行环境中的管理程序与安全存储芯片采用安全通道协议（SCP）以及共享的配对密钥进行安全通信。配对密钥在设备生产过程中预置，使用主芯片的硬件唯一密钥（HUK）进行派生并通过可信执行环境注入到安全存储芯片当中，达到安全存储芯片与主芯片一对一绑定，避免换拆芯片带来的安全风险。

安全通道协议所使用的会话密钥，在会话建立时通过随机生成的因子以及配对密钥进行派生，防止通信内容泄露。

*注：此功能仅在部分芯片型号的产品上提供。

可信执行环境

本章节主要阐述设备的可信执行环境。荣耀可信执行环境，遵循 Global Platform TEE 标准，是荣耀自主研发的基于形式化微内核的安全操作系统，具有高安全、高性能、高扩展和高稳定的特性。

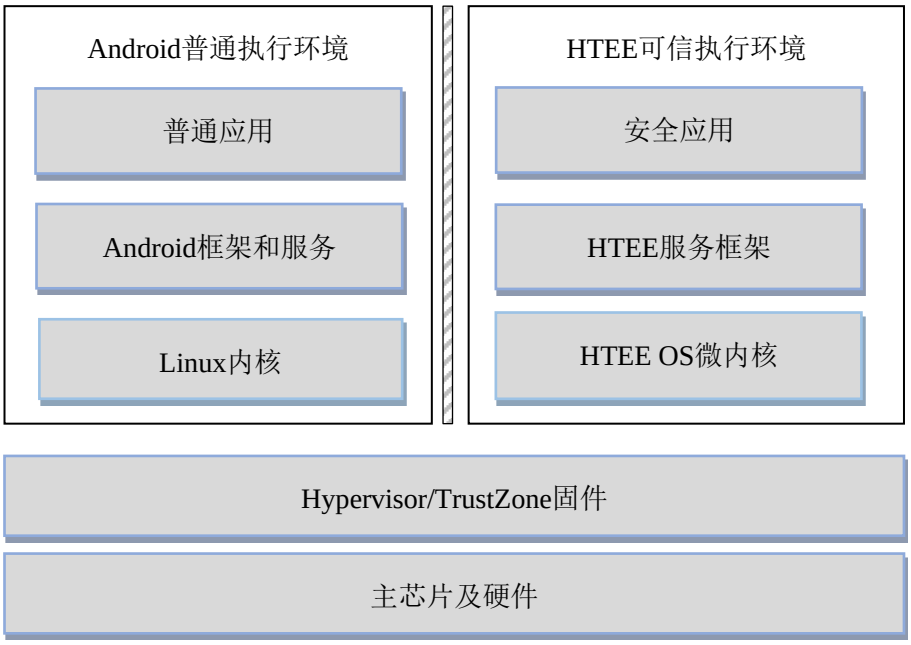
HTEE 安全 OS 介绍

HTEE（Honor Trusted Execution Environment，荣耀可信执行环境，简称 HTEE）是荣耀采用微内核技术实现的可信执行环境，包括了安全 OS 内核、框架层以及系统核心可信应用等构成，基于 TrustZone 和虚拟化技术构建。

TrustZone 是硬件级别的安全，兼顾了性能、安全和成本的平衡。TrustZone 技术将处理器的工作状态分为安全世界（Trusted Execution Environment ，TEE，也叫可信执行环境）和非安全世界（Rich Execution Environment，REE，也叫普通执行环境）。通过特殊指令在 CPU 的安全世界

和普通世界之间切换来提供硬件隔离。在安全世界下，提供了对硬件资源的保护和隔离，包括内存、外设等，通过执行过程保护、密钥保密性、数据完整性和访问权限实现了端到端的安全，可防止来自非安全世界中的恶意软件攻击。

Hypervisor 虚拟化是一种广泛使用的技术。用虚拟化可以对同一个物理核上运行的虚拟机进行隔离。这使得多个执行环境可以共享同一套硬件环境，对于 ARM 架构的芯片, Hypervisor 运行在 EL2 异常级别。只有运行在 EL2 或更高异常级别的软件才可以访问并配置各项虚拟化功能。HTEE 运行在 VM 中，与其他 VM 隔离，通过 Hypervisor 与其他 VM 通信。



*注：部分芯片型号的产品上采用主芯片厂商提供的 TEE，与荣耀 HTEE 功能规格有部分差异，具体以产品实际情况为准。

微内核

HTEE 使用微内核架构，通过简化内核功能，模块化设计，将系统服务更多地在内核之外实现，微内核只提供最基础的服务，系统服务更多的在用户

态，通过按需扩展，提升性能并降低攻击面，通过加强细颗粒度权限设计，使得 HTEE 具备如下优势：

良好的扩展性，通过构筑分布式设备统一的安全内核，能承载更多异构设备各种业务的能力诉求，如多核支持，按需并发，大小核调度等。

易于实现与调试，通过提供稳定的底层库接口，降低应用开发移植难度，支撑安全业务生态发展。

形式化验证

HTEE 采用形式化验证方法显著提升系统 TEE 内核安全等级，构建可信安全。形式化验证方法是使用数学定理证明的方式从源头验证系统正确，无漏洞的有效手段。传统验证方法如功能验证，模拟攻击等只能在选择的有限场景进行验证，而形式化验证方法可通过数据模型验证所有软件运行路径，通过验证核心模块，验证核心 API 及进程隔离，权限管理等高层机制的正确性，保证无数据竞争、无内存访问错误等。

HTEE 安全 OS 的目标是持续构建没有漏洞的可信执行环境，为产品提供更高的安全保证，

另外， HTEE 还采用多种技术手段对 REE 侧系统安全、通道安全、鉴权安全、TEE 侧系统安全等进行全方位地安全加固，通过镜像反逆向、系统反入侵、数据反侵害等基于杀伤链的安全防御技术提高系统安全性。比如反逆向主要是在入侵准备阶段的提前防御，通过对镜像进行加密保护，芯片出厂阶段使能镜像加密，防止逆向攻击。反入侵主要是对鉴权信息加密、REE 与 TEE 的通

信会话严格鉴权，保证 TEE 侧从 REE 侧来源的数据完整可信，反侵害主要是采用控制流保护、栈金丝雀等技术完成对常见内核漏洞攻击手段的防护。

最后，HTEE 通过构筑主动防御能力，识别程序的异常行为，识别 REE 侧系统异常，做到安全响应提前一步，保护敏感信息。

HTEE 安全 OS 可保证安全应用的运行安全，为安全应用提供一个可信的执行环境，保证安全业务在运行时的安全。HTEE 安全 OS 支撑 MagicOS 多种安全业务，主要支持如下应用场景：

内容保护	用于 DRM（Digital Rights Management）数字版权保护领域，保护视频在播放过程中的安全性，防拷贝。
移动支付	用于移动支付领域，保证输入信息的安全性，同时可配合 NFC 进行使用。HTEE 可保护用户输入信息的安全，防止被恶意程序窃取。
应用逻辑保护	可保护关键应用逻辑不被窃取或篡改。

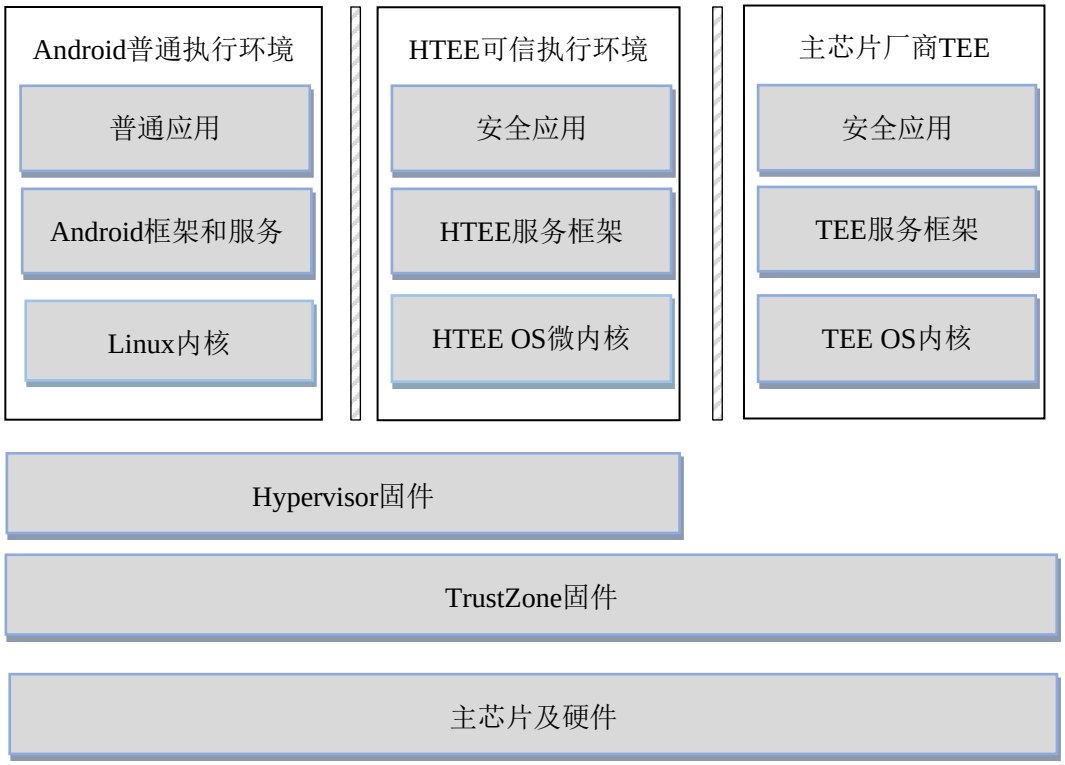
举例来说，荣耀手机指纹/人脸解锁及支付、密钥管理等功能，均由 TEE 安全 OS 提供可信执行环境进行安全保护。

双 TEE 系统*

基于 Trustzone 和 Hypervisor 虚拟化机制，在部分产品实现“主芯片厂商 TEE”+“荣耀 HTEE”的双 TEE 系统，持续打造可信的系统安全能力和友好的安全生态。

SoC 芯片厂商 TEE 基于芯片自身的安全启动、安全硬件（RPMB、硬件加密引擎）、密钥管理等核心能力持续构建硬件安全框架，提供可信存储、加解密、文件加密等硬件级安全能力。

HTEE 基于形式化验证、多核多线程、国密算法等基础能力和安全应用开发、部署、维护的应用完整生命周期管理能力，可以快速集成已有安全业务并持续拓展。



*注：双 TEE 功能仅在部分芯片型号的产品上提供。

HTEE 可信运行环境支持的基础安全能力如下：

可信存储服务

HTEE 安全 OS 的可信存储分为两种：安全文件系统存储与 RPMB（Replay Protected Memory Block）存储，前者将密文存储到特定的安全存

储分区，后者存储到 NAND Flash 特定的存储区域，RPMB 支持防删除、防回滚特性。可信存储支持设备绑定，支持不同安全应用之间的隔离，每个安全应用仅能访问自己的存储内容，无法打开、删除或篡改其它应用的存储内容。

基于 HTEE 安全 OS 实现的安全文件系统（SFS），提供对关键信息的存储保护能力，可用于存储密钥、证书、个人隐私数据和指纹模板等数据，具有机密性、完整性、原子性、隔离性等特点

HTEE 中运行的 TA（Trusted Application，可信应用）可通过安全存储的 API 来将数据加密并存放于安全文件系统中，加密后的数据只有 TA 本身能够访问，外部应用无法访问。

安全存储采用 AES256 算法加解密，兼容 GP TEE 标准规范。安全存储的密钥通过设备唯一密钥进行派生，密钥不出设备 TEE 安全区，经密钥加密过的数据安全区外部无法解密。

MagicOS 进一步提供了基于 Flash 的 RPMB 存储功能，保护系统关键数据不会被非法删除和访问。RPMB 由 HTEE 直接进行安全管理，RPMB 的访问鉴权密钥与设备唯一密钥进行绑定，只有 HTEE 才能访问 RPMB 分区保护的内容，REE 侧不提供访问的接口，RPMB 对于数据的存储通过内置的计数器和密钥、HMAC 校验机制防止重放攻击，确保数据不被恶意覆写或篡改。

加解密服务

HTEE 安全 OS 支持多种对称、非对称加解密算法以及密钥派生算法，支持同一芯片平台相同密钥的派生，支持设备唯一密钥，支持基于 SE 派生硬件级

别的密钥，支持国际标准加密算法和国密算法，为第三方开发存储和使用密钥的业务 TA 提供支持，加解密 API 遵从 Global platform TEE 标准。

为提高安全性，HTEE 安全 OS 内部的密钥生成和计算，均由独立的硬件芯片完成。密钥将被存储在独立的安全存储芯片中，或严格加密的安全存储空间中。用户可根据业务的需要，开发 TA 来使用可信密钥服务。

后量子密码学

为满足针对量子威胁来增强数据安全的迫切需求，美国国家标准与技术研究所（NIST）于 2023 年发布了第一批后量子密码学算法的 FIPS 草案(FIPS 203/204/205)，其中包含一个公钥封装机制算法和三个数字签名方案。

为了保护现有数据抵御 “立即存储，未来破解”的风险，从 MagicOS 8.0 开始后量子密码算法迁移。MagicOS 引入了后量子公钥封装机制算法 CRYSTALS-Kyber 和数字签名算法 CRYSTALS-Dilithium 对部分关键数据进行安全加强，以保证在量子计算机出现后，这些关键数据不会因为 RSA/ECC 密码算法的脆弱性而导致数据安全问题。

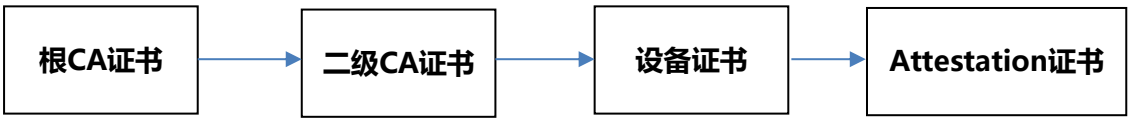
设备证明

为了确保 MagicOS 设备是可信的，荣耀在产线就预置了设备证书与公私钥对，设备证书和公私钥对每台设备不同，用于标识设备的唯一合法身份。证书和密钥写入到 MagicOS 的可信执行环境 TEE 内部后加密保存，业务无法直接访问证书和密钥，只能通过荣耀统一密钥管理服务提供的唯一接口访问。

设备证书由荣耀 PKI 系统签发，包含三级证书链如下：

对于支付类、账号类等高安全要求的业务，如果需要验证设备、用户或者账号的合法性，可通过设备证书及私钥签发对应的业务证书（又称为 Attestation 证书），形成证书链提供给对应的业务方进行验证。业务方验证通过后才允许执行对应的业务，确保只有可信的设备才允许开展相应的业务。

业务 Attestation 证书在手机的 TEE 中通过设备证书签发，包含四级证书链如下，业务校验四级证书链通过后，同时进行最后一级证书的签名校验成功后可认为此设备的合法性，允许执行相应的业务：



可信 UI（TUI）*

在 REE 侧负责的应用环境中，应用显示的支付金额或输入的密码可能被恶意应用劫持，HTEE 安全 OS 提供了无法截屏的 TUI（Trusted UI，可信 UI）显示技术（符合 GP 规范）来保护的 TA 显示的内容，采用与外部隔离的显示。当显示时完全阻止 REE 侧对该显示区域的访问，可防止恶意应用对于显示和输入的劫持和篡改。确保恶意程序既看不到显示屏上的信息，也无法访问触摸屏。

TUI 特性可以保证显示给用户的信息不会被任何 REE 侧的软件或者 TEE 侧未授权的应用截取，修改，遮盖,显示的信息不会传递到 REE 侧，同时使用权限

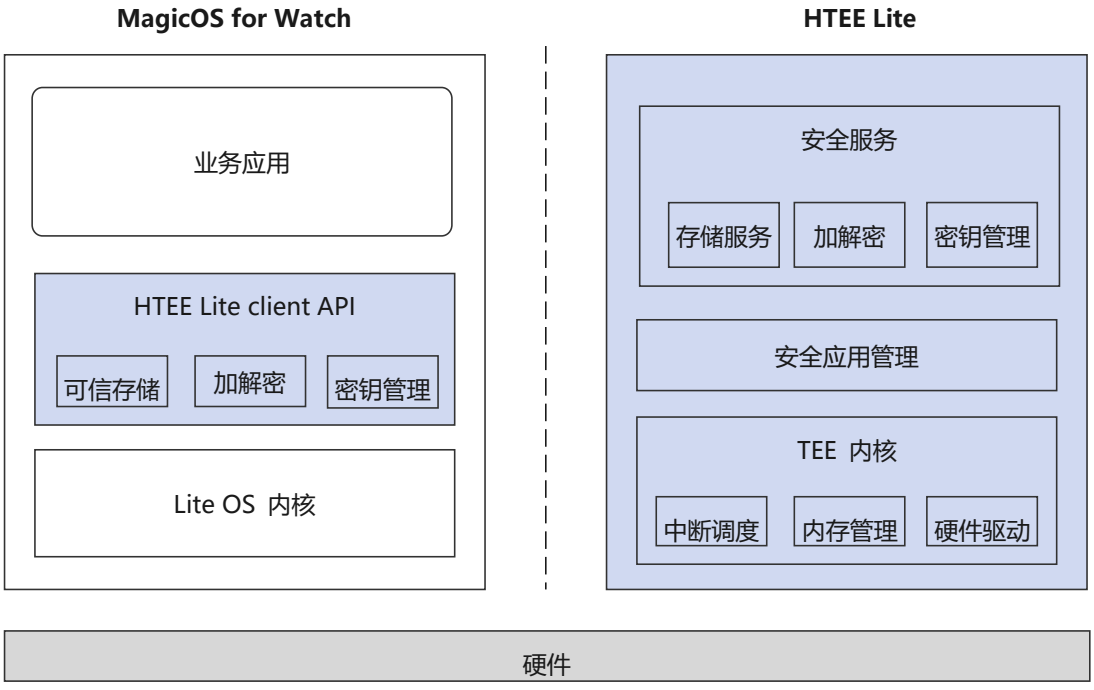
控制保证只有授权的 TEE 侧应用才能访问。TUI 界面显示成功后会显示预置的图片或文字，提示用户当前的环境处于安全的显示输入状态。

TUI 支持 PNG 图片、文本、按钮和输入框等基本控件，支持显示统一大小的汉字、英文字母、符号和数字，支持定制界面，输入键盘按键随机化支持丰富的控件支持、窗口管理，界面使用终端 MagicOS 的 UI 风格。

*注：TUI 功能仅在部分芯片型号的产品上提供。

HTEE Lite*

HTEE Lite 是荣耀在手表产品提供的可信执行环境，基于 ARM cortex-M 芯片的 Trustzone 功能，提供硬件隔离的独立安全世界，用于执行支付、关键信息存储等相关高安操作，提供可信计算、可信存储、加解密等安全功能。



系统安全

系统安全旨在确保 MagicOS 设备基于硬件芯片的安全能力，为运行在系统上的应用程序提供软硬件结合的基础安全能力，主要从如下六个方面进行构筑：

- 完整性保护技术：该技术是系统安全的基础，确保设备初始运行的是由厂家提供的可信系统软件，并且通过运行时的完整性保护技术 HKIP 与完整性度量检测技术，确保运行时内核不被恶意破坏，或者既使系统被破坏，也能及时被检测出来；
- 系统软件更新：当系统出现问题或者被恶意破坏时，能通过最小系统进行系统软件的安全更新，确保只有合法的系统软件才能更新设备；
- 内核漏洞防利用技术：系统在运行时将面临内核漏洞被恶意利用的风险，一旦内核被突破，系统将无法为上层应用提供基础保护，应用的机密数据将面临泄露的风险，因此需要采取多种内核漏洞防利用技术，来确保内核在运行时漏洞不会被找到，如：内核地址空间布局随机化技术 KASLR 等；或者既使漏洞被找到，也能通过访问控制权限来禁止漏洞被利用，如：特权模式访问禁止 PAN/特权模式执行禁止 PXN、控制流完整性 CFI 等；
- 强制访问控制技术：基于上述四类技术打造了安全可信的系统内核基础之后，通过在内核中构建强制访问控制技术，基于策略规则来定义系统中各种应用对不同资源的合理使用，从而确保整个系统为上层应用提供基础的安全能力。
- 身份认证：MagicOS 提供指纹识别和人脸识别两种生物特征识别能力，即利用人体所固有的生理特征（指纹特征和人脸特征）来进行个人身份鉴定，可应用于设备解锁、支付、应用登录等身份认证场景。

完整性保护技术

HKIP 内核完整性保护*

虽然 Secure Boot 和 Verified Boot 确保了启动时软件的合法性及完整性，但合法代码中仍然可能存在漏洞会被攻击者利用。HKIP 通过 ARMv8 处理器提供的 Hypervisor 模式（EL2）对内核保护，防止系统关键寄存器、页表、代码等被篡改。从而达到系统运行时的完整性保护和防提权的目的。HKIP 不但实现了对于代码及只读数据段等静态数据的保护，而且实现了稀有写（Write-Rare）保护机制对于部分动态数据提供保护。HKIP 利用稀有写机制保护了内核里部分大部分时间是被读取而极少被更改的数据。攻击者即使通过漏洞获取了内核级别的内存写能力，也无法修改这部分数据。

目前 HKIP 支持如下安全保护机制：

- 内核及驱动模块的代码段不可被篡改
- 内核及驱动模块的只读数据段不可被篡改
- 内核非代码段保证不可执行
- 内核关键动态数据不可被篡改
- 关键系统寄存器设置不可被篡改

*注：此功能仅在 MTK 芯片部分型号的产品上提供。

完整性度量检测*

MagicOS 实现了对系统关键代码和资源文件的完整性度量检测，实现了一个系统完整性度量框架，提供对系统关键组件或进程完整性度量的统一服务，解决了运行时的度量以及对用户态进程的动态度量问题，能够探测受保护进程是否被恶意篡改，从而能及时提供相应应对策略。完整性度量框架包括以下三部分：

1）基线提取

基线提取的目标是为要保护的软件程序生成静态的度量基线值。通过对目标文件进行哈希计算来获取基线度量值。有两种可选方式：

- 离线生成，在构建过程中计算完整性基线值，通过私钥签名保护，构建到软件的镜像版本当中；
- 运行时生成，基于系统安全启动能够保证文件合法的假设，基线参考值在第一次加载目标程序时生成。

2）静态度量

对于一个文件，所谓的完整性通常就是指其内容或属性均没有被修改过。从密码学的角度来讲，文件对应的哈希值可以被用来检测一个文件是否有被篡改。因此通过收集被度量目标的哈希值来判断程序或数据实例在内存加载过程中的完整性。

3）运行时度量

在度量评估阶段，将基线数据和运行时采集的度量数据进行比较，用来确定运行时的程序是否与基线一致，最终提供完整性检查的结果，由决策者（对应的业务）来决定后续的处理策略。

*注: 此功能仅在 MTK 芯片平台对应的产品上提供。

系统软件更新

MagicOS 支持设备的 OTA 升级，以便能及时修复可能存在的漏洞。系统软件更新中的安全防护流程如下：

系统软件更新时，会对升级包的签名进行校验，只有通过校验的升级包才被认为合法并安装。

此外，MagicOS 提供了系统软件更新的管控，当下载完成软件包开始 OTA 升级时，需向服务器申请升级的授权，将由设备标识、升级包版本号、升级包哈希及设备升级 Token 组成的摘要信息发给 OTA 服务器，OTA 服务器验证摘要信息确认版本是否可以提供授权，若可以进行授权则对摘要进行签名再返回给设备，设备鉴权通过后才允许升级，否则提示升级失败，防止对系统软件的非法更新，尤其是防止可能带有漏洞的版本升级，给设备造成风险。

MagicOS 定期发布系统安全补丁，在系统更新后会自动更新上对应的安全补丁，以确保 MagicOS 系统的安全性。有关软件更新安全性的详细信息，请访问 https://www.hihonor.com/cn/support/bulletin/

内核漏洞防利用技术

内核地址空间布局随机化（KASLR）

在代码重用攻击中，，必须确定一个明确的重用代码跳转地址。KASLR（Kernel Address Space Layout Randomization）内核地址空间布局随机化技术可以让内核镜像映射的地址相对于链接地址有个偏移，此偏移地址在每次开机启动时随机生成，从而做到每次重启后内核镜像映射的虚拟地址都不一样，使得内核地址空间布局难以预测，代码重用攻击难度被提升，提升了系统内核的安全性。

特权模式访问禁止（PAN）/特权模式执行禁止（PXN）

MagicOS 支持使用 ARMv8 的 PAN（Privileged Access Never）和 PXN (Privileged execute never) 安全防护技术保护内核，禁止内核访问用户空间的数据和执行用户空间的代码。

在某些针对内核的攻击方法中，攻击者通过篡改内核使用的部分数据结构内的数据指针，使其指向攻击者在用户态准备好的数据结构，影响内核的行为达到攻击目的。PAN 技术阻止了内核访问用户态数据，这种攻击行为会被阻止。

在某些针对内核的攻击方法中，攻击者通过篡改某些内核使用的数据结构内的代码指针，使其指向用户态的提权代码，并通过系统调用触发提权代码的执行。PXN 技术阻止了内核直接执行用户态代码，这种攻击行为会被阻止。

控制流完整性 CFI

ROP(Return Oriented Programming)和 JOP(Jump Oriented Programming)是通过程序漏洞将程序控制流重定位到现有程序的代码片段的一种攻击手段。攻击者通过组合这些代码片段实现完整的攻击行为。

由于实现 ROP/JOP 攻击的常用方法是利用程序漏洞来覆盖内存中的函数指针，因此可针对性进行检查。CFI 技术通过添加额外的检查来确认控制流停留在预先设定的范围中，以缓解 ROP/JOP 攻击，如果检测到程序发生未定义的行为，则丢弃程序执行。尽管 CFI 无法阻止攻击者利用已知漏洞，甚至改写函数指针，但它可严格限制可被有效调用的目标范围，这使得攻击者在实践中利用漏洞变得更加困难。

MagicOS 采用 CLANG CFI 及栈保护、PA/BTI 等技术以缓解 ROP/JOP 攻击威胁内核：

- 在每个间接分支之前添加检查，以确认目标地址的合法性，防止间接分支跳转到任意代码位置；
- 编译器支持链接时优化技术 LTO(Link time optimization)，以获得完整的程序可见性，从而可确定每个间接跳转分支的所有合法调用目标；
- 支持运行时加载内核模块。通过在编译时使能(cross-DSO)，使得每个内核模块包含有效本地分支目标的信息，内核可根据目标地址和模块的内存布局，从正确的模块中查找信息；
- 在函数末尾退出时对栈布局进行检查，防止通过溢出漏洞修改返回地址；
- PA（Pointer Authentication）/ BTI（Branch Target Identification）是基于硬件的 ROP/JOP 攻击缓解措施，PA 针对指针进行签名与验签，保证了指针的完整性，BTI 针对函数跳转的目标进行了限制，保证了跳转目标的完整性。

  *注：PA/BTI 功能依赖芯片硬件，仅在部分产品上提供。

强制访问控制技术

MagicOS 支持 SELinux 特性，强制访问控制策略在设备启动时加载到系统内核中，无法被动态更改。该特性对所有进程访问目录、文件、设备节点等操作资源实施强制访问控制，对具有 root 权限的本地进程实施基于权能（root capabilities）的强制访问控制，阻止恶意进程读、写受保护数据或者攻击其他进程，把被恶意篡改的进程对系统的影响限制在一个局部范围内，有力的支撑上层应用实现各种安全防护。

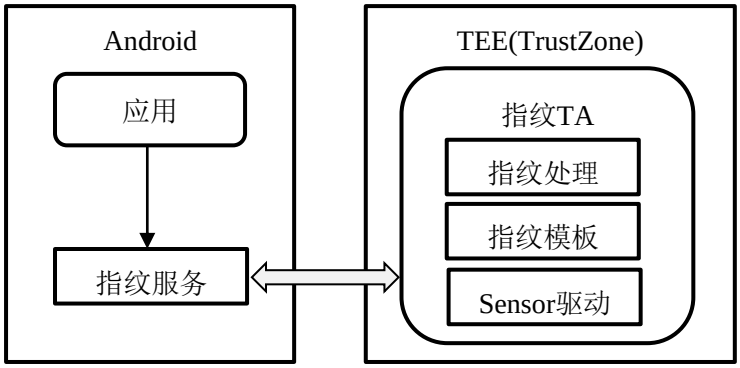
MagicOS 同时也支持 seccomp 特性，基于只读文件系统中的规则文件，对上层应用进程能够调用的系统调用进行限制，避免恶意应用通过使用敏感的系统调用对系统造成危害。

身份认证

指纹识别

MagicOS 提供电容指纹、光学指纹两种指纹识别能力，两种方式的识别能力（识别率、防伪率）基本一致。不同的设备根据需要选配使用不同的技术，具有外置指纹器件的使用电容指纹技术，具有屏下指纹器件的使用光学指纹技术。

MagicOS 的指纹识别安全框架图如下：



MagicOS 在指纹传感器和 TEE 之间建立安全通道，指纹信息通过安全通道传递到 TEE 中，REE 侧无法获取。MagicOS 对指纹图像信息采集、特征提取、活体检测、特征比对等处理完全在 TEE 中，基于 TrustZone 进行安全隔离，REE 的指纹框架只负责指纹的认证发起和认证结果等数据，不涉及指纹数据本身。

指纹特征数据通过 TEE 的安全存储进行存储，采用高强度的密码算法进行数据加密和完整性保护。外部无法获取到加密指纹数据的密钥，保证用户的指纹数据不会泄露。外部第三方应用无法获取到指纹数据，也不能将指纹数据传出 TEE。MagicOS 不会将任何指纹数据发送或备份到包括云端在内的任何外部存储介质。

MagicOS 的指纹识别支持防暴力破解机制，在亮屏场景下用户使用指纹识别连续错误 5 次，则在 30 秒内不能进行指纹识别。在熄屏场景下用户指纹识别可以连续错误 10 次，然后锁定 30 秒不能进行指纹识别。如果指纹识别连续失败 20 次，则必须使用密码来解锁设备。

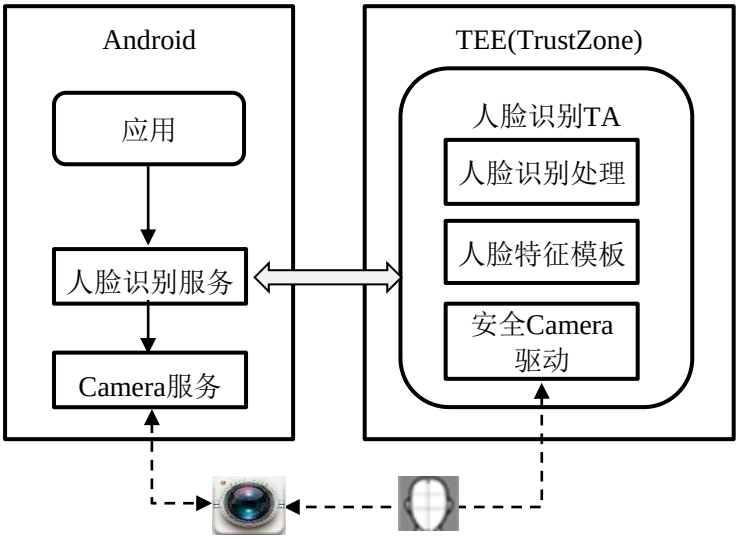
指纹采集器件被污损、手指不洁净以及手指过湿等外部因素都会影响识别成功率，使用时需要注意避免这些情况。

另外需要注意到，在使用指纹识别提供便利的身份识别的同时，用户可能更容易忘记锁屏密码，当前采用 72 小时内未使用密码解锁则强制要求用户输入密码解锁，以便加强用户记忆，减少忘记密码的异常情况发生。

人脸识别*

MagicOS 提供 2D 人脸识别、3D 人脸识别两种人脸识别能力，不同的设备根据需要选配使用不同的技术，具有 3D 人脸能力的设备才可以使用 3D 人脸识别技术。3D 人脸识别技术识别率、防伪能力都优于 2D 人脸识别技术。3D 人脸识别技术可支持支付场景。

MagicOS 的 3D 人脸识别安全框架图如下：



MagicOS 在摄像头和 TEE 之间建立安全通道，人脸图像信息通过安全通道传递到 TEE 中，REE 侧无法获取。MagicOS 对人脸图像采集、特征提取、活体检测、特征比对等处理完全在 TEE 中，基于 TrustZone 进行安全隔离，外部的人脸框架只负责人脸的认证发起和认证结果等数据，不涉及人脸数据本身。

人脸特征数据通过 TEE 的安全存储进行存储，采用高强度的密码算法对人脸特征数据进行加解密和完整性保护。外部无法获取到加密人脸特征数据的密钥，保证用户的人脸特征数据不会泄露。外部第三方应用无法获取到人脸特征数据，也不能将人脸特征数据传出 TEE。MagicOS 不会将加密的人脸数据或者未经加密的人脸数据发送或备份到包括云端在内的任何外部存储介质。

MagicOS 的人脸识别支持防暴力破解机制，用户使用人脸识别连续错误 5 次，则不能进行人脸识别，必须输入密码解锁设备。

对于长相相似的双胞胎和兄弟姐妹、未满 13 岁的儿童，人脸识别率有所不同，也可考虑使用指纹识别或密码认证。

在使用人脸识别提供便利的身份识别的同时，用户可能更容易忘记锁屏密码，当前采用 72 小时内未使用密码解锁则强制要求用户输入密码解锁，以便加强用户记忆，减少忘记密码的异常情况发生。

*注：3D 人脸识别功能仅在部分产品上支持。

在支持独立安全存储芯片的产品上，用户在设备中录入的人脸、指纹模板数据采用双重加密机制，基于主芯片的硬件唯一密钥以及安全存储芯片中保存的密钥在可信执行环境中进行加密。

持续身份识别*

MagicOS 提供持续身份识别能力，基于 AO 低功耗 Camera 和低功耗 NPU 能力使用用户的生物信息（人脸/呼吸音/触屏行为等）来持续的识别使用者是否是机主。本功能默认不开启，需要用户主动打开，并同意隐私保护协议。

持续身份识别能力使用的生物信息仅在端侧安全环境中采集和处理，生物信息被安全存储，采用高强度的密码算法对生物信息数据进行加解密和完整性保护。外部无法获取到加密生物信息数据的密钥，保证用户的生物信息数据不会泄露。外部第三方应用无法获取到生物信息数据，也不能将生物信息数据传出设备。MagicOS 不会将加密的生物信息数据或者未经加密的生物信息数据发送或备份到包括云端在内的任何外部存储介质。

*注：持续身份识别功能仅在部分产品上支持。

数据安全

本章节主要阐述 MagicOS 的数据安全防护，MagicOS 的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，普通应用无权访问，同时对于存储在用户分区的数据，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。对于用户分区的关键数据，MagicOS 提供了：锁屏密码保护、关键资产安全存储服务、密码保险箱、安全擦除等机制确保用户的高敏感数据的安全存储、安全使用和安全销毁。同时，MagicOS 对应用开发者提供了荣耀通用密钥库系统（HUKS）的框架能力，方便应用开发者安全的存储应用的密钥与数字证书，并安全的使用密钥加密保护应用中的机密数据。

通用密钥库

荣耀通用密钥库（HUKS，Honor Universal Keystore）是 MagicOS 系统中基于 JCA/JCE 架构实现的密钥与证书管理系统，向应用提供 KeyStore 及 Crypto 接口 API，包括密钥管理，对称/非对称加密解密，证书管理等功能。HUKS 提供了基于设备证书的设备合法性认证能力，云端服务器可以通过证书认证的方式，对设备进行合法性认证；与生物认证结合，HUKS 可以为支付应用提供 TEE 安全级别的登陆和支付等服务。

HUKS 管理的密钥及证书存储在 TEE 环境中，所有密钥都基于硬件唯一密钥进行 AES_256_GCM 加密保护。密钥在使用时，在 TEE 内先解密出密钥明文再进行数据加解密计算，密钥明文不会离开 TEE 环境，加解密过程受 TEE 保护。

HUKS 对密钥的使用实施严格的访问控制。在密钥生成时, HUKS 记录了应用的 UID（User ID，应用安装时由系统分配）、签名、包名等身份信息。应用使用密钥时，HUKS 先对应用的身份信息进行校验，校验通过后才允许应用使用。

HUKS 支持使用生物识别功能(指纹/人脸识别等)增强密钥的访问控制，HUKS 确认生物识别结果后才允许应用对相应密钥访问与操作。

HUKS 提供了密钥认证（Key Attestation）功能。设备生产时，产线为每台设备写入唯一的设备证书。TEE 环境下，HUKS 利用设备密钥及证书对应用的密钥签发密钥认证证书（详见设备证明章节）

TPM 密钥管理

PC 设备上，HUKS 的能力基于 Windows 系统和 TPM 可信固件，内部实现了包括密钥管理、数据保护、对称/非对称加密解密、证书管理和设备认证等功能。通过 HUKS，MagicOS 应用开发者可以进行完整的密钥、证书的生命周期管理和加解密算法的调用。

HUKS 提供了基于硬件根密钥的分级分类管理能力。对密钥使用做了严格的访问控制，不同 windows 用户、不同业务的密钥相互隔离，且都由硬件唯一密钥（HUK）采用 AES_256_GCM 算法加密保护。密钥管理过程受 TPM 保护，其中 HUK 加解密完全在 TPM 内部完成，对 windows 环境不可见，以抵御来自系统的安全攻击。

HUKS 的数据保护功能提供了一机一密（基于 HUK）和一型一密（基于 GID）两种形式的业务数据加密能力。加密过程绑定调用者的身份，被加密保护的数据只有调用者本身能够解密使用。

HUKS 的对称/非对称加密解密功能提供了基于硬件安全随机数的常用密码算法，包括对称的 AES 加解密、HMAC 验证，非对称的 RSA/ECC 签名验签、密钥协商等能力。

锁屏密码保护

MagicOS 提供固定 6 位数字（默认）、固定 4 位数字、不固定位数（大于等于 4）数字或混合密码和图案锁屏密码。用户设置锁屏密码后，除了能被用于解锁设备，还能为文件系统加密密钥提供熵。这意味着攻击者即使拿到设备，在没有锁屏密码的情况下，也没法访问某些被锁屏密码熵保护的数据。

MagicOS 对用户的密码输入错误后，通过逐渐递增的延缓尝试时间间隔，防止锁屏密码被暴力破解。当用户的密码长度越长、字符类型越多，意味着尝试所有组合的耗费的时间会更长。

锁屏密码通过设备唯一密钥 HUK 保护，在用户创建、修改锁屏密码，或者日常验证锁屏密码进行解锁操作时，这些锁屏密码的处理都在 TEE 环境中进行。这意味着暴力尝试只能在受到攻击的设备上进行。在不考虑延缓尝试间隔的情况下，如果攻击者能够直接通过暴力尝试 6 位数字和字母混合密码，尝试所有组合需要消耗 8 年时间。即使 TEE 以外的系统遭到了破坏，也可以保证锁屏密码不会遭受到暴力破解。

对于带有独立安全存储芯片的产品，支持通过该芯片对锁屏密码验证过程进行保护增强， 锁屏密码校验及防暴力破解机制（连续错误计数及尝试间隔计时）在独立安全存储芯片中进行。只有密码验证通过后，可信执行环境中的管理程序才能从安全存储芯片中获取到密钥材料进行密钥派生，对加密的文件数据进行解密，从而保证用户数据安全。

数据加密保护

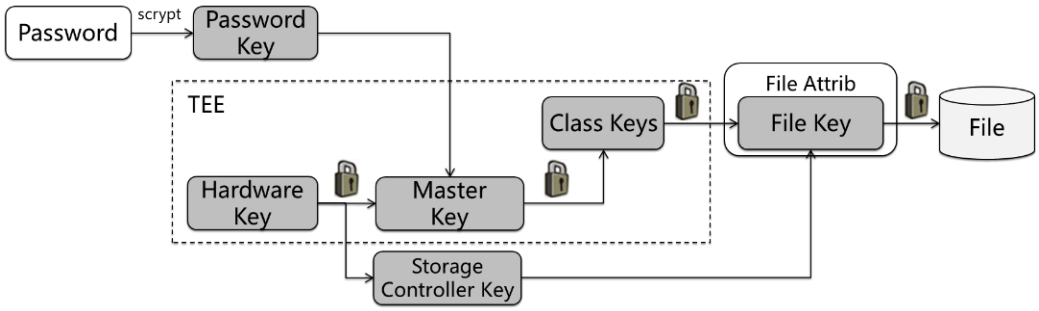
文件加密

MagicOS 提供基于文件级加密功能，利用内核的加密文件系统模块和硬件加解密引擎，采用 AES256 算法的 XTS 模式实现数据存储加密保护。

为兼顾用户数据安全和应用体验，MagicOS 提供了以下几种不同的方案：

1）用户凭据加密方案：应用默认采用该类数据保护方案。此类方案中加密数据的类密钥（Class Keys）与锁屏密码相关联，被用户锁屏密码和设备唯一密钥共同保护。该类数据只能在 MagicOS 设备首次解锁以后才可访问。由于数据加密与用户锁屏密码相关联，如果忘记密码会造成设备内的数据无法解密，建议用户能够保护好密码，同时做好数据备份。

2）设备加密方案：该类保护方案中数据是否可访问与设备锁定状态无关，受 DE 方案保护的数据在设备一上电后即可访问，如壁纸、闹钟、铃声等。该类密钥被设备唯一密钥保护，与锁屏密码无关。



文件加密密钥保护

关键资产数据安全存储服务

一些应用会处理比较短小但是敏感的数据，比如用户密码和认证凭据，这类数据使用文件系统会显得繁琐。关键资产安全存储服务为这些数据提供安全保护，并对数据作精细化的访问控制。

被保护的数据密文由设备唯一密钥及应用身份共同保护，解密和加密过程完全在安全环境中进行，加密数据的密钥不出安全环境。应用的单条密文由 AES_256_CCM 模式加密保护，批量密文由 AES_256_CBC 模式加密保护。

关键资产安全存储服务提供以下两类数据的保护：

- 敏感数据：关键资产敏感数据，如用户可保存其应用账号、密码用于下次登录认证时快速填充输入等
- 认证凭据：认证凭据或令牌，通常是应用使用某个服务的凭证。例如 APP 连接服务器，使用 TOKEN 做会话的合法性认证。

关键资产安全存储服务会对查询数据的应用的签名、包名，以及系统为该应用分配的 ID 等信息进行校验，以验证应用对该数据的访问权限，确保访问安全。

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，往往通过删除逻辑地址的方式实现，导致实际存储的物理地址空间没有清除，可以被恢复回来。

MagicOS 的恢复出厂设置，支持对存储数据的安全擦除。通过给物理存储器发送命令，进行覆写操作，完成底层数据擦除。擦除后数据是全 0 或者全 1，确保用户的敏感数据不能通过软硬件手段恢复，能够保护用户设备转售、废弃后的数据安全，满足 NIST SP800-88 要求。

密码保险箱

随着应用越来越多，各种应用登录都需要用户名和密码，因此忘记用户名和密码的情况随时可遇；密码保险箱可以将应用登录账户信息（用户名\密码）保存，同时可以与人脸、触摸指纹和锁屏密码关联，在用户登录应用时密码保险箱可以自动填充账户密码数据；

密码保险箱把应用账户密码信息加密保存到终端设备之中，以储存在文件系统中的 SQLite 数据库的形式实现，密码保险箱提供硬件级加密存储能力；密码保险箱保存的“密码”数据通过认证加密方式进行加密保护，加密算法为 AES_256_CCM；对应的加密密钥受 TEE 保护，加密/解密处理始终在 TEE 内执行；

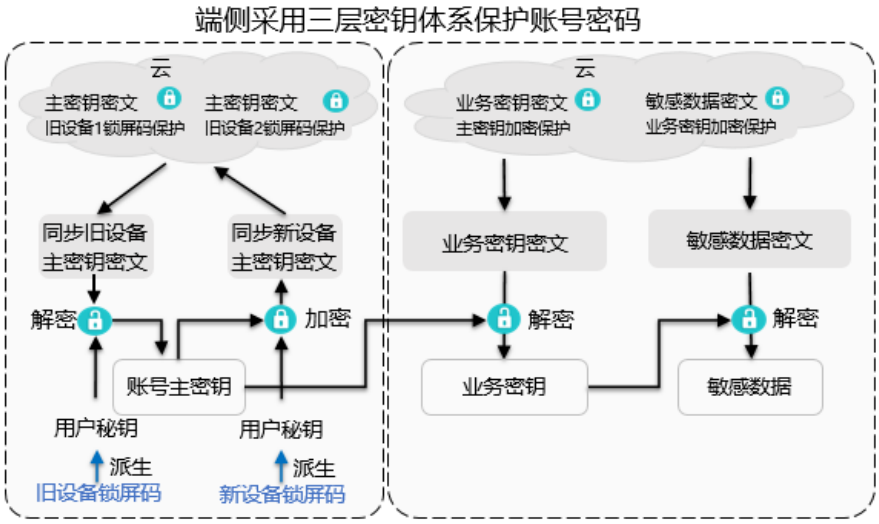
当前密码保险箱保存的账户密码数据可以通过手机克隆的方式在支持密码保险箱的荣耀终端设备之间加密传递（仅在支持 PKI 证书的荣耀设备之间提供

密码保险箱的克隆能力）；同时也可以通过 PC 备份的方式在同一部终端上恢复 PC 侧保存的加密数据。

手机克隆过程中传输的密码保险箱数据通过 AES_256_CBC 的方式进行加密，加密密钥通过两部手机在 TEE 侧生成的非对称密钥进行密钥协商获取，密钥协商过程在 TEE 侧完成，协商出的克隆加密密钥受 TEE 保护，加密/解密操作在 REE 侧执行以便密码保险箱数据克隆操作的快速执行；

PC 备份过程的传输的密码保险箱数据通过 AES_256_CBC 的方式进行加密，加密密钥通过终端设备唯一密钥（HUK）派生，非本设备无法恢复 PC 备份的数据。

从 MagicOS 6.0 版本开始，您可以通过荣耀云将账号和密码信息自动同步到其他登录荣耀账号的设备，您的信息会被加密，其他人以及荣耀都无法读取。荣耀通过端到端加密来保护您的信息，从而提供最高级别的数据安全性。您的数据受密钥保护，该密钥通过您设备独有的信息以及只有您知道的设备密码生成。其他人以及荣耀都无法访问或读取这些数据，无论是传输中的数据还是储存的数据都将做加密处理。



应用安全

本章节主要阐述 MagicOS 上应用程序相关的安全机制。由于应用程序来源于各种渠道，用户随时可能下载到带有恶意威胁的应用，如果处理不当，应用程序可能给系统的安全性、稳定性以及用户的个人数据甚至个人财产带来安全风险。

为此，MagicOS 提供了整套应用安全解决方案，从如下几方面确保应用运行环境的安全：

- 应用安装阶段，通过应用签名校验机制，确保开发者的 APP 不被恶意篡改。应用安装时， 系统对应用进行威胁检测（如病毒、恶意软件扫描），如果识别出风险则对用户进行提醒。
- 应用运行阶段，通过应用沙箱、运行时内存保护、安全输入等机制确保应用内产生的数据不会被非法应用恶意读取，造成用户的数据泄露。

应用签名验证

MagicOS 只允许安装具有开发者完整签名的应用程序。应用签名能保证应用程序的完整性和来源的合法性，系统在安装应用程序时，会对应用签名进行验证，以检查应用程序是否被篡改，对于验证不通过的应用拒绝安装。

对于系统预装的应用程序和用户已安装的应用程序进行升级时，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，以保证恶意应用程序无法通过升级的方式替换用户现有应用程序。

MagicOS 系统支持以下 Android V1/V2/V3 三种应用签名的方案：

- Android V1 签名格式，是一种基于 JAR 包的签名方案。由于 V1 签名方案不保护 APK 的 ZIP 元数据，在最新的 Android 系统上不建议单独使用 V1 签名。
- Android V2 签名格式，是 Android 7.0 之后引入的一种全文件签名方案，能够发现对 APK 的受保护部分进行的所有更改（包括 ZIP 核心目录、目录结束标识和文件数据内容），从而有助于加快验证速度并增强完整性保证。使用应用签名方案 V2 进行签名时，会在 APK 文件中插入一个 APK 签名分块，V2 签名和签名者身份信息会存储在应用签名方案 V2 分块中，并且能够防止攻击者将 V2 签名伪造成 V1 签名的应用进行验证。
- Android V3 签名格式，是 Android 9 版本之后引入的签名方案，支持应用密钥轮转，使应用能够在应用更新升级过程中更改其签名密钥。

Android V1/V2/V3 三种签名方案中，新的签名格式支持向后兼容。MagicOS 系统在对应用进行签名验证的过程中，会根据应用中的 API 级别信

息，以及签名分块中的标识，兼容处理签名验证。如果应用以 Android 11（API 级别 30）为目标平台，应用必须使用签名方案 v2 或更高版本进行签名。

应用沙箱

MagicOS 使用应用沙箱机制，确保每个应用运行在沙箱中，且每个应用之间相互隔离，保证应用运行时的安全；同时应用在安装时，系统给应用分配了私有存储目录，应用私有目录不能被其他应用访问，保证静态数据安全。通过沙箱隔离技术，保护应用和系统不受恶意应用的攻击。

系统为每个应用程序分配了唯一的身份标识用户 ID（UID），并基于 UID 构建应用沙箱，沙箱构建包括自主访问控制（DAC）、强制访问控制（MAC）等多种内核访问控制机制，限制应用访问沙箱外文件、资源等。所有应用默认情况下均是沙箱化，如果应用要访问沙箱以外的信息，需要通过系统提供的服务或者其他应用对外开放的接口，并获取相应权限才能完成。在没有权限的情况下，系统会阻止应用越权行为。

相同签名的应用程序，可以共享用户 ID，在同一个沙箱内可以共享代码和数据。

强制执行分区存储

为了让用户更好地管理自己的文件并减少混乱，以 MagicOS 4.0（Android API 级别 29）及更高版本为目标平台的应用在默认情况下被赋予了对外部存储空间的分区访问权限（即分区存储）。每个应用只能访问外部存

储空间上由系统分配的应用专属目录，以及本应用所创建的特定类型的媒体文件。应用私有目录不能被其他应用访问，保证数据安全。

应用运行时保护

应用运行时，若每次运行分配使用的内存地址是相对固定的，容易被恶意应用通过查看内存的方式获取到，MagicOS 支持地址空间布局随机化(ASLR)、系统调用控制(Seccomp)。

ASLR 是提供防止缓冲区溢出漏洞利用的安全保护技术，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。提高攻击者在利用内存漏洞上的难度。

Seccomp 机制可以控制应用进程可执行的系统调用的范围，对于非进程范围内的系统调用执行会被拒绝，可有效阻止针对部分系统调用存在漏洞而对进程执行的攻击。

应用锁

应用锁对应用入口进行保护，防止应用中的隐私信息被他人窥视。MagicOS 用户可通过“设置>安全>应用锁”开启应用锁能力，设置应用锁密码并选择需要加锁的应用。应用锁能力开启后，启动加锁应用前会对用户进行身份认证（认证方式包括密码、指纹、人脸等），认证通过后才允许使用，保护机主的隐私。受应用锁保护的应用，未解锁前，在系统最近任务列表中的缩略图也被加锁保护，防止隐私泄漏。

安全输入*

在用户输入密码的场景下，MagicOS 提供安全输入功能。打开安全输入功能，在用户输入密码时，会自动切换到安全输入法。安全输入法和普通输入法的管理是分离的。安全输入法没有联想和记忆功能，没有联网权限，不会收集用户的密码。安全输入法启动后禁止后台录屏或第三方应用截屏，确保用户的密码输入安全。

*注：部分应用会使用自己开发的输入法进行密码输入，该情况下安全输入法不会生效。

病毒查杀

第三方未知来源应用可能存在安全隐患，从第三方渠道下载应用可能引入恶意威胁。MagicOS 系统安装应用时支持检查应用来源是否合法，默认情况下，系统不允许安装第三方未知来源的应用。建议用户保持默认的安全设置，以免带来不必要的风险。

MagicOS 系统内置业界领先的杀毒引擎，用于检测用户安装的应用是否存在病毒。支持本地病毒查杀和联网病毒查杀两种方式，确保用户设备无论是否联网，都能够发现应用是否存在风险。病毒查杀引擎支持应用安装时检测和后台闲时扫描，一旦发现了病毒应用，会立即向用户提出风险警告，并提示用户对病毒应用进行处理。

流氓广告拦截*

流氓广告频繁在桌面、锁屏等界面弹出广告，严重影响用户使用体验。MagicOS 提供了流氓广告识别功能，通过对应用的行为特征进行评估，识别流氓广告应用，并对其后台弹窗行为进行拦截，禁止应用在桌面、锁屏上弹出广告界面。

防诈骗*

电信网络诈骗给用户带来巨额的财产损失。MagicOS一方面通过识别和拦截风险电话、应用、网址，另一方面在设备本地进行风险行为识别，对受诈风险行为进行识别和提醒，降低用户受诈风险。

恶意网址检测*

MagicOS 提供了短信和智慧视觉扫码等使用场景中的恶意网址的威胁检测功能，检测是否为钓鱼网站或者带有恶意威胁的网址。在接收短信时能够自动识别出短信中的恶意网址，在用户使用智慧视觉扫码时，会检测二维码中的恶意网址，并提醒用户存在风险。

验证码短信保护*

当前验证码短信已成为重要的移动应用的身份认证因子之一，验证码短信一旦被第三方劫持将给用户带来信息泄露或经济损失等安全风险，为了降低可能带来的风险，MagicOS 提供了验证码短信保护功能，防止恶意应用拦截用户短信，盗取验证码。

MagicOS 在系统层增加短信验证码智能识别引擎，若识别为验证码短信，则将短信只分发给 MagicOS 系统中设置的默认短信客户端，若默认短信客户端为 MagicOS 自带的系统短信客户端，则系统短信客户端会对验证码短信进行加密保存，并对访问进行过滤，防止第三方短信客户端或应用读取到验证码短信。即使对短信数据库直接读取，验证码的短信内容依然是加密的，其它应用无法解密。

*注：带星号(*)的功能仅在中国区部分型号的产品上提供。

网络与通信安全

设备连接网络时，需使用安全的连接机制，否则有可能连接到恶意的站点，导致传输数据泄露。本章节主要阐述 MagicOS 的网络连接与传输的安全机制，以及对于设备通信、设备互联传输数据时所提供的安全防护。

VPN

通过 VPN，用户可以借用公网链路建立自己的安全专用私有网络，进行安全的数据传输。MagicOS 支持以下 VPN 协议和认证方式：

1. PPTP，支持 MS-CHAPV2 密码和 RSA SecurID 进行用户认证、支持 MPPE 加密
2. L2TP/IPSec，支持 MS-CHAPV2 密码、PSK 共享密钥、证书认证
3. 支持 IKEv2/IPSec，支持共享密钥、RSA 证书、ECDSA 证书、EAP-MSCHAPv2 或 EAP-TLS 进行认证

4. 支持 IPSec Xauth PSK 共享密钥，IPSec Xauth RSA 证书认证，IPSec **Hybrid RSA 证书认证**

MagicOS 支持以下 VPN 功能：

针对使用基于证书认证的网络， IT 策略通过使用 VPN 配置描述文件 来指定哪些域需要 VPN 连接。

支持为应用单独设置 VPN，更精确地建立 VPN 连接。

支持始终打开 VPN，用户在连接到网络后不需要手动打开 VPN 以启用保护。

支持对通过移动设备管理（MDM）解决方案管理的设备禁用与启用 VPN 功能，保护组织内的数据安全。

TLS

设备支持 TLS v1.0,1.1,1.2,1.3。TLS 是一种安全协议，它能为通信提供数据安全和完整性保障，应用层协议能透明地运行在 TLS 协议之上，TLS 协议负责创建加密通道需要的身份认证和密钥协商。应用层协议传送的数据在通过 TLS 协议时都会被加密，从而保证通信的私密性。

设备默认为所有 TLS 连接启用 TLS 1.3，相比 TLS1.2，TLS1.3 提升了性能和安全性（如移除了脆弱和较少使用的算法、）；TLS1.3 加密套件不可自定义，并且在启用 TLS1.3 后，受支持的加密套件会始终保持启用状态，且会忽略试图将其停用的行为。

无线局域网安全*

MagicOS 支持 WPA/WPA2 PSK，WPA3(部分产品支持)，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。

为了避免设备被跟踪，加强对用户隐私的保护，在未连接到 WLAN 网络之前，MagicOS 设备扫描网络时使用随机的 MAC 地址。。

连接到 WLAN 网络时，设备默认使用随机 MAC 地址连接(部分产品支持，依赖于芯片能力)。用户如果信任目标网络，也可以手动修改为使用设备 MAC 地址进行连接。

同时设备也支持 WLAN 热点功能，默认情况下是关闭的，当用户开启时默认 WLAN 热点支持 WPA2 PSK 认证方式，保证连接的安全。

公共场所等外部 WLAN 提供便利的同时也可能被非法利用，窃取用户的隐私以及钓鱼，可能给用户带来隐私泄露和经济损失等安全问题。MagicOS 提供了对 WLAN 接入点的威胁检测引擎。对需连接的 WLAN 进行检测，一旦发现风险将会提示用户 WLAN 热点的安全风险，用户可以进行对应的操作，确保用户的 WLAN 连接的安全。

*注：本功能仅在中国地区的版本支持。

防伪基站*

不法分子通过部署伪基站可获取用户的位置和身份信息，或给用户发送广告推销、诈骗信息等，不仅严重干扰用户正常通信，甚至会造成用户的财产损失。MagicOS 提供芯片级防伪基站功能，通过对 GSM/LTE 伪基站的接入和重

选的网络参数特征以及正常基站网络参数特征的对比学习和分析，拒绝驻留和接入识别出的伪基站（LTE 伪基站的识别仅部分芯片平台支持）。设备除了利用解码系统消息识别伪基站，还可结合伪基站攻击无鉴权重定向等流程特征增强识别，避免驻留和接入具备伪基站特征的小区。

*注：防伪基站特性仅在设备接入中国区网络时生效。

设备互联安全

为了实现用户数据在用户各个设备之间的安全流转，需要保证设备之间相互正确可信，即设备和设备之间建立过信任关系，并能够在验证信任关系后，搭建安全的连接通道，实现用户数据的安全传输。

设备之间的信任关系包括同一荣耀账号 MagicOS 设备之间的可信关系以及 MagicOS 设备和 IoT 设备之间建立的可信关系等。

同一荣耀账号 MagicOS 设备互联安全

MagicOS 为登录同一荣耀账号的设备互联提供设备认证服务。各 MagicOS 设备在登录账号后将会生成椭圆曲线公私钥对作为各自的身份标识，并向荣耀云服务器申请对其公钥进行认证。认证通过的同一荣耀账号下的设备，可在设备互联业务中互相认证并交换各自的身份公钥，确认对端是可信设备。进一步地，基于双方的身份公私钥对，同一荣耀账号的设备间可以进行密钥协商并建立安全通信通道。仿冒设备和非本账号下的其他设备将无法通过认证鉴权。

同一荣耀账号 MagicOS 设备组网服务

登录同一荣耀账号的设备认证服务同时支持登录同一荣耀账号 MagicOS 设备间的可信组网，涉及手机、平板、PC 等设备。MagicOS 设备上可信组网服务启用时，将对附近登录同一荣耀账号的其他设备分别进行身份认证，并协商设备间的会话密钥。

当用户启用业务连接同账号下的其他设备，会基于上述可信设备组网服务，完成同一荣耀账号下的设备认证与会话密钥协商，设备间传输的数据将被协商的会话密钥加密保护。

智慧空间与设备云连接安全

智慧空间为家庭IoT设备数据本地存储提供服务，设备云为上传至云端的IoT设备数据提供安全加密和认证服务。智慧空间基于可信环境生成设备唯一密钥，使用AES-GCM-256算法加密缓存用户设备信息，支持用户将分享的家庭成员账号标识上传至设备云。智慧空间和设备云之间的通信基于TLS1.2及以上安全协议，此外还会使用认证协商获取的会话密钥对传输的业务数据进行二次加密。设备云会为每一个IoT设备分配唯一工作密钥，并使用AES-GCM-256算法加密保存上传的设备身份信息和家庭成员账号标识。

IoT 设备互联安全

MagicOS 同时支持无法自主登录荣耀账号的设备（如智能穿戴等设备）与 MagicOS 设备（手机、平板等）间建立点对点的信任关系，并在具备信任关系的设备间，搭建安全的连接通道，实现用户数据端到端加密传输。

MagicOS 设备的 IoT 业务身份标识

MagicOS 设备为不同的 IoT 设备管理业务生成不同的身份标识，形成不同 IoT 管理业务间的隔离，该标识用于 MagicOS 设备与 IoT 设备之间认证以及通信。与设备登陆荣耀账号申请的账号级设备标识类似，IoT 业务身份标识同样

为椭圆曲线公私钥对（Ed25519 公私钥对）；密钥对在 MagicOS 设备的安全环境生成，私钥明文不出 TEE。

IoT 设备身份标识

IoT 设备会生成各自的设备身份标识，用来与 MagicOS 设备通信。该身份标识同样为椭圆曲线公私钥对（Ed25519 公私钥对）；IoT 设备私钥不出 IoT 设备，设备每次恢复出厂设置，会重置这个公私钥对。

上述身份标识可用于 MagicOS 设备与 IoT 设备间的安全通信：当 MagicOS 设备与 IoT 设备认证对端的交换业务身份标识或设备标识后，可以进行密钥协商并建立安全通信通道。

设备间点对点的信任绑定

MagicOS 设备和 IoT 设备建立点对点信任关系的过程，实际上是相互交换 MagicOS 设备的 IoT 业务身份标识和 IoT 设备的身份标识的过程。

在点对点建立信任关系的过程中，用户需要在 MagicOS 设备上，输入 IoT 设备上提供的 PIN 码：对于有屏幕的设备，该 PIN 码动态生成；对于没有屏幕的设备，该 PIN 码由设备生产厂家预置；PIN 码的展示形式，可以是一个用户可读的 6 位数字，也可以是一个二维码。随后，MagicOS 设备和 IoT 设备间使用 PAKE 协议完成认证和会话密钥协商过程，并在此基础上，保护相互交换的身份标识的完整性。

在 MagicOS 设备上，为了保证与通信对端的可信关系不可篡改，对端的身份公钥信息被存储在 TEE 侧。

MagicOS 设备与 IoT 设备间的通信安全

当建立过信任关系的 MagicOS 设备与 IoT 设备间进行通信时，双方在每次通信时，基于本地存储的对端身份公钥相互进行认证与会话密钥协商，以确认对端设备确实是用户已绑定的设备。

当用户使用 PC 手机“碰一碰”、多屏协同等业务，在手机和荣耀的个人电脑、大屏、PAD 之间共享数据时，可以通过上述安全绑定过程建立点对点的信任关系，并使用认证协商得到的会话密钥对传输的数据进行加密。

远程密码认证

当登录同一荣耀账号的 MagicOS 设备之间建立了可信关系后，业务应用在跨设备数据传输前，业务请求端可以通过远程密码认证机制验证当前的使用者是否是业务接收端设备的拥有者，只有当身份验证通过后才继续进行数据传输。

例如：平板等设备上的应用在请求手机端应用投屏前，需要证明当前平板设备的使用者是手机的机主，而远程密码认证机制就是提供了一种在平板设备上验证手机机主身份的安全方式。用户在平板设备上输入手机设备的锁屏密码，密码不离开客户端，通过远程认证协议与手机进行交互验证密码的正确性，完成对机主的身份识别。

远程认证的安全性

在远程认证的服务端，即业务接收端设备（以下简称服务端），用户在录入锁屏密码或更新锁屏密码后会基于锁屏密码配合盐使用 PBKDF2 派生出密钥并存储在可信执行环境（TEE）中。在远程认证的客户端，即业务请求端设备（以下简称客户端）发起远程认证时，服务端基于上述密钥生成服务端公私钥

对并向客户端发送服务端公钥、签名公钥、挑战值和盐，用户在客户端输入业务接收端设备的锁屏密码后，同样会配合盐值使用 PBKDF2 算法派生密钥，并基于此密钥生成客户端公私钥对，基于客户端私钥和服务端公钥协商出会话密钥，并将其用作 HMAC 密钥，以构成一个基于挑战值的消息验证码，并向服务端发送客户端公钥、消息验证码；服务端基于客户端公钥钥和服务端私钥协商出会话密钥，并使用此会话密钥对消息验证码进行校验。如果校验通过，则说明客户端输入的锁屏密码是正确的服务端设备锁屏密码。服务端此时还需向客户端做双向认证，用协商出会话密钥作为 HMAC 密钥，构造一个派生于挑战值的消息验证码，再使用签名密钥把认证结果信息通过 ESDSA 签名，之后使用会话密钥在 CCM 模式下的 AES 加密认证结果信息和签名，然后向客户端发送消息验证码和认证结果的密文；客户端使用协商出的会话密钥校验消息验证码，再用户会话密钥解密认证结果，使用签名公钥验证认证结果，如果上述操作正确完成，则认证结果是可信的，至此双向验证完成。以上所涉及的处理过程均在可信执行环境（TEE）中完成，服务端具备防暴力破解能力，所依赖的密钥交换协议面向非安全网络环境。

机主识别

在智慧互联业务场景下为您提供了机主识别能力，保护您跨设备信息的隐私安全。机主识别功能打开后，在您设备使用智慧互联服务时系统会识别您的身份保护您的隐私信息。

当您在平板上使用超级通话、超级通知等功能时候会调用机主识别能力识别您的身份。如果您是手机机主，则自动会在平板上显示手机来电联系人或信

息详情等信息。如果您不是手机机主，则会隐藏联系人名称、通知信息详情等信息。

当您智慧互联的设备（手机、平板等）都登录了荣耀账号并且手机上开启机主识别功能时候，会将您手机中录入的人脸图片信息安全传输到与其互联的其他终端设备上加密存储，数据不会上传云端。当您退出荣耀账号、关闭机主识别功能或在手机上删除人脸信息的任一情形中，我们都会同步删除该机主账号下智慧互联设备上加密存储的人脸信息。

用于机主识别功能的人脸图片信息只在同账号的各设备之间进行近场加密传输和存储，荣耀不会收集您的数据，也不会上传到云。

服务安全性

本章节主要阐述荣耀 MagicOS 产品支持的服务的安全防护。对于第三方支付应用，支付过程中除了对恶意应用进行查杀外，MagicOS 提供对支付环境的隔离保护措施来保证支付安全。

荣耀账号

荣耀账号适用于访问所有荣耀服务。对于用户而言，保障荣耀账号的安全，防止未经授权的非法访问十分重要。为了达成这一目标，荣耀要求使用长度至少为 8 个字符的强密码，同时必须包含字母和数字，且不能为常用的密

码。在此规则的基础上，用户可以通过添加更多的字符和标点符号（密码最长为 32 个字符），让密码变得更加安全。

在帐户发生重大更改时，荣耀还会向用户发送短信，电子邮件和推送通知。例如，密码发生更改，或者在新设备上使用荣耀账号登录。如有异常发生，荣耀会提示用户立即更改其荣耀账号密码。另外，荣耀采用了多种策略和程序来保护用户帐户。这包括限制重新尝试登录和尝试重设密码的次数，保持欺诈监控以帮助在发生攻击时进行识别，以及定期回顾策略并针对可能影响客户安全性的任何新信息作出调整。

双重认证

双重认证是账号保护最佳方案，将确保您的荣耀账号使用更安全。

有了账号保护，意味着只能通过您的受信任设备才能访问您的账号。首次登录新设备，需输入密码和安全验证码。安全验证码将只发送到受信任的手机号码或安全邮箱上。验证通过，表示您信任此设备。这就显著增强了荣耀账号以及使用荣耀账号业务（荣耀商城、荣耀俱乐部等）的安全性。

启发式安全认证

如果用户在登录荣耀账号时遗忘了密码，在找回荣耀账号密码时，发现之前通过荣耀账号绑定的手机号码或邮件地址已经不可使用，用户可通过自助申诉来变更手机号码、邮件地址、安全手机号或安全邮件地址。

账号风控

荣耀账号具备端到端的全生命周期风险识别和对抗能力，为账号的注册、登录、密码找回、申诉等场景提供全流程风险防护。通过对账号登录环境和设

备的多重校验，集成多种判断因子，并结合专家规则、机器学习等技术保障账号安全，打击恶意针对荣耀账号的攻击，确保用户资产和数据安全。

协同登录*

新设备 OOBE 阶段，用户可使用已登录荣耀账号的旧设备进行协同登录。新旧设备会建立安全的近场通信通道，新旧设备进行一系列的安全参数及可信参数校验后，账号云基于 HTTPS 协议通道下发账号临时凭据给新设备进行账号登录，实现了新旧设备的账号协同登录。

克隆登录

在新设备上，用户可以通过备份克隆功能建立可信的安全传输通道，将旧设备的账号相关信息同步克隆到新设备。账号云基于 HTTPS 协议通道下发该账号临时凭据给新设备进行账号登录，实现了新旧设备的账号克隆登录。

指纹登录

在新设备上，用户登录荣耀账号后可以开启指纹登录功能，荣耀账号的指纹登录功能基于 FIDO 协议实现。在用户完成指纹录入后，用户每次使用指纹登录时，终端设备上的 FIDO 认证器都会基于用户注册时随机生成的 Key ID 和指纹数据重新混淆计算出用户的指纹标识，后续认证过程都是基于指纹标识完成的，所以荣耀终端设备上不会存储用户的任何指纹数据和指纹标识，仅加密存储用户的 KeyID。

扫码登录

用户可以使用已登录荣耀账号的旧设备通过扫描新设备上的二维码进行扫码登录。用户在使用旧设备扫码完成后，需要在旧设备进行扫码登录确认，完

成确认后，荣耀账号会基于 HTTPS 协议通道和云侧完成扫码请求验证。此时新设备上会收到扫码登录确认，用户确认后整个扫码登录方可完成。

荣耀卡包

手机交通卡

荣耀卡包交通卡是交通卡公司将自己的交通卡应用通过空中下载的方式加载到手机的安全元件（Secure Element，后称 SE）芯片中，并和指定的辅助安全域（SSD）关联后再将卡片的个人化数据下载存储到安全隔离区中的卡应用中，由与之关联的辅助安全域提供安全保障。用户在开通了交通卡后，可以对交通卡进行余额充值、可以查询交通卡中的卡号、余额等卡内信息、可以将交通卡从手机中移除后存储在云端、可以将存储在云端的交通卡再迁移回手机、不再使用交通卡时可以将交通卡退卡，退回卡内余额。

开卡：用户在卡包app 中支付完开通交通卡所需的费用后，发起开卡请求。荣耀可信服务（SEI TSM）在主安全域（ISD）的 SCP（Secure Channel Protocol）的保护下，为待开通的交通卡创建一个单独的SSD，将对应交通卡的卡应用按照 GP Card（GlobalPlatform Card）规范下载安装到SSD中,然后将卡实例让渡给为之创建的SSD。SSD的密钥由交通卡公司的可信服务平台（SP TSM）管理。SP TSM 将一卡一秘的卡片密钥等个人化数据，通过使用 SSD 的密钥建立 SCP 加密保护下载到 SE中的交通卡卡应用内。至此卡片在手机中开通成功。

余额充值：用户在卡包app 中完成充值后发起余额充值请求。SP TSM 在确认收到了款项支付完成的通知后，通过充值初始化指令向 SE 中的卡片发起

随机数挑战值，卡片收到挑战值后，使用卡内密钥计算并返回计算结果。SP TSM 使用该卡片的密钥验算卡片回复的计算结果，验算成功则表明 SP TSM 验证卡片合法性成功。随后SP TSM 再使用卡片密钥做另一次计算，并将计算结果封装在充值指令中下载的SE中的卡片应用内，卡片也需要做一次验算，验算成功则表明卡片对 SP TSM 的合法性认证成功，所以卡片会将本次的充值金额数，累加在卡内的余额存储区域。由于卡片密钥分别存储在 SE 中的卡应用内和 SP TSM 的硬件加密机内，密钥在两个端点的存储均为硬件安全级别，且没有第三者能知晓该密钥，故充值只能依靠交通卡公司的 SP TSM 完成。

交通卡空中移除(迁移)：当用户暂时不使用某张已开通的交通卡时，可以将其从本机上移除，移除后的卡片数据会保存在 SP TSM。交通卡卡内数据备份到云端的过程，由 SP TSM 下发迁出指令到 SE 中的卡片内，卡片根据指令要求获取对应数据，并在卡内加密、加 MAC 后返回。SP TSM 在收到结果后，验 MAC，解密数据得到卡内数据并保存。卡数据在卡内加密、加MAC，保证了传输过程中的机密性和完整性。

退卡：用户不再使用交通卡后，可以通过卡包 app 发起卡片的退卡。在退卡流程中，SP TSM 会将卡内余额获取，然后 荣耀可信服务(SEI TSM) 会将卡片从 SE 芯片中彻底删除。SP TSM 将获取到的卡内余额使用用户历史以往的支付订单原路退回给用户的支付银行卡中。

车钥匙

用户通过车企 App 创建车钥匙，车企 App 调用卡包 App 接口告知卡包车机蓝牙设备的 MAC 地址，卡包 App 调用蓝牙服务接口注册车机设备的 MAC 地址。蓝牙服务扫描到车机设备的蓝牙广播后，判断进入有效距离后，蓝牙服务拉起卡包 App，卡包 App 拉起车企 App 服务，由车企 App 服务校验钥匙有效性，完成车辆的解锁；在蓝牙有效距离之外，车辆自动闭锁。蓝牙连接遵循蓝牙协议，车辆解锁遵循车企自身的安全规范。用户在车企 App 或者卡包 App 可以选择删除车钥匙，删除时会同步删除注册到蓝牙服务的车机 MAC 地址和卡包 App 本地数据。

荣耀云

数据同步：支持协同办公，方便用户在多个移动终端设备上同步数据，保障用户数据不丢失。

目前支持日历、笔记、联系人、密码保险箱、WLAN 等应用使用荣耀云 SDK 进行端云数据同步。密码保险箱通过端到端的数据加密方式进行同步，云侧会对数据进行二次加密处理，并以 HMAC-SHA256 做签名，确保数据的存储安全

对于结构化数据，在用户进行同步之前，荣耀云会先和移动终端建立基于 TLS1.2 协议的加密通道，并通过椭圆曲线密钥协商算法协商会话密钥，使用 AES-GCM-256 算法加密待同步的结构化数据。荣耀云会给每个用户分配一个用户密钥，并使用该密钥对数据进行加密入库保存，用户密钥由荣耀云业务密钥进行安全加密，业务密钥会通过 KMS 系统使用硬件加密机保管

非结构化数据（包括图片，文本等）在本地会生成唯一的数据主密钥，大文件处理时，每个分块数据都会由数据主密钥派生响应的分块数据子密钥用于加密分块，数据同步上云时，数据主密钥使用工作密钥加密传输至荣耀云。工作密钥采用基于椭圆曲线算法生成的临时协商会话密钥加密下发，端侧使用HUKS 环境提供的非对称密钥加密工作密钥。

数据备份：备份联系人、日历、录音、信息、通话记录等应用数据，输入法、闹钟、时钟、天气、相机设置、管家设置等系统的设置数据，微信等三方应用数据，备份文件加密方式和同步非结构化数据加密方式一致。

应用商店

开发者实名认证

依据相关法律法规要求，荣耀应用商店会对上架应用所属的开发者进行实名认证，开发者分为个人开发者和企业开发者，只有完成实名认证后才能享受荣耀开放的各类能力和服务，以确保上架应用是合法合规且可追溯的，促进应用生态健康良性发展。

应用安全管控

荣耀应用商店致力于为用户提供安全可靠、隐私合规的应用。在应用申请上架时，会对应用的功能、权限、内容、付费等要点进行全面的安全扫描和人工审核，涵盖病毒检测、权限最小化、广告弹窗、流氓行为、个人信息采集等审核要求。应用上架后，应用商店会定期开展对在架应用的审查，结合用户反馈、投诉和舆情，对于不符合要求的应用，及时推动开发者进行整改或下架处理。通过上架审核、在架巡检和下架处理，对应用进行严格的安全管控，保护

用户的合法权益。

未成年人保护

荣耀应用商店具备完善的未成年人保护机制，所有应用都会进行分类分级，为不同年龄段用户提供适合其身心发展的服务。通过账号完成未成年人身份识别，支持家长对分发内容、使用时长进行管理，限制应用下载、应用内消费、个性化推荐等功能，确保内容安全，保护未成年人身心健康。

开发者套件安全性

开发者服务平台提供了多种套件框架，便于三方开发者在荣耀终端设备上扩展并丰富 APP 的应用能力。

每个使用荣耀开放能力的 APP 需首先在荣耀开发者服务平台注册 APP 信息，填写 APP 的唯一标识符及签名证书指纹信息，完成注册且审批通过后，开发者即可申请开放能力对应权限范畴的 Scope。

端侧开放能力框架后台服务会校验接入 APP 的唯一标识符和签名证书指纹信息，同时会校验三方 APP 请求的开放能力是否在开发者申请的权限范围内，保证了开放能力不被滥用。

查找设备 & 激活锁*

MagicOS 提供了查找设备功能。如您的荣耀手机、平板不慎遗失或被盗，可登录荣耀查找设备官网（https://cloud.hihonor.com/findmydevice/wapFindPhone）或“查找设

备”APP 查找丢失的设备。以下功能可帮助您查找丢失设备、保护设备中数据安全、保护个人隐私安全：

定位设备：可在地图上显示设备所在位置。包括主动定位、低电量位置自动上报位置信息。

播放铃声：无论设备是否处于静音或振动模式，设备均将以最大音量播放提示铃声。

关机验证密码：功能开启后，锁屏状态下需要验证锁屏密码才能关机，避免被拾获者快速关机。

远程连接网络：在您使用查找功能时如设备离线，查找设备会帮助您远程开启丢失设备的移动数据，以便定位查找。

丢失模式：设备屏幕将被锁定并进入超级省电状态，在屏幕上显示留言和联系电话，自动上报位置，上线后短信通知。同时，设备上来电将隐藏联系人信息，新消息将隐藏内容。

SIM 卡加锁：进入丢失模式后可对设备上的 SIM 卡进行加锁操作，加锁后 SIM 卡插入其他设备或重启设备时均需要输入密码才可使用。

擦除数据操作：设备恢复出厂设置，所有数据（含存储卡）将被永久删除。擦除数据后您仍能对设备进行定位，设备使用时仍需验证您的荣耀账号密码。

此外 MagicOS 还提供了设备激活锁功能。在启用了查找我的手机时，会同时开启设备激活锁功能，若设备丢失被非法用户执行强制清除数据，设备重

新启动后需要用户登录荣耀账号才能进行重新激活，确保没有得到授权的用户无法激活和使用设备，保证设备的安全。

设备激活锁也可以通过锁屏码来解除。当进入激活设备界面时，用户可以选择使用设备已经设置的锁屏码来解除激活锁。锁屏码校验通过后，后续处理流程与使用荣耀账号密码解除激活锁相同，都需要通过云端进行远程操作来完成。

*注：海外地区暂不支持此功能。

运动健康

运动健康基于手机和可穿戴设备，提供运动健康数据完整记录、多端同步、安全存储和用户授权开放等服务，保护用户数据的隐私安全是荣耀运动健康的基石。

基于MagicOS提供的数据安全能力，结合硬件安全和可信执行环境提供的安全加密能力，全方位保护用户运动健康数据在移动终端业务处理和数据交换过程中的安全。

在网络中传输的所有运动健康数据，均使用安全传输通道（TLS1.2及以上安全协议），在此基础上，当传输用户个人数据时，还会使用椭圆加密算法对数据进行二次加密和签名校验，确保用户个人数据在传输过程中不会被窃取和篡改。

用户主动上传至运动健康云的所有个人数据，均使用AES_256_GCM算法进行加密存储，密钥会通过KMS系统使用硬件加密机加密后保管，以确保用户个人数据存储、使用和销毁的安全。

此外，借助于荣耀账号和设备互联安全能力，用户还可以通过运动健康云，在同一个荣耀账号下的各种设备上安全快捷地同步更新运动健康数据。

支付保护中心

支付保护中心为支付类应用提供一个独立的安全环境。支付保护中心对加入的支付类应用来源进行严格管控以确保其为官方发布的应用;对支付类应用和外界应用的交互进行严格管控以降低保护中心内的应用遭受外部应用恶意调用和攻击的风险；同时受保护的支付类应用在运行时对系统会对当前运行环境安全状态进行检测以确保，保障用户的财产和支付安全。

移动设备管理 API*

针对企业移动办公或特定行业的移动设备管理（MDM）应用所需要实现对设备的策略配置、访问控制及设备管理等功能，当前 MagicOS 可提供了针对于荣耀移动设备的设备管理 SDK。

对于企业移动办公客户所需的设备管理 API，MagicOS 通过证书的方式来进行授权，企业客户可申请设备管理 API 的使用授权。

对经过荣耀审核的应用开发者，荣耀公司对其签发设备管理证书，开发者在开发的 APK 中集成此设备管理证书后，其 APK 可在荣耀设备上使用授权许可 API 接口。

用户安装带有设备管理证书的 APK 时，MagicOS 系统会解析并校验证书。通过校验后， APK 才能获取到所有权限。证书校验不正确时，APK 将不

具备相应的权限，调用相关的设备管理 API 会失效并抛出安全异常，以此保证荣耀设备的安全。

*注：仅中国区版本支持。

隐私保护

本章节主要阐述 MagicOS 对用户隐私的保护。在荣耀设备中可能存在用户的隐私数据，如：联系人、短信、照片等。为了保护用户的隐私，MagicOS 确保预置的应用完全符合隐私合规要求，同时提供应用的权限管理、通知管理、录音/录像提醒、位置服务管理以及 7 日隐私访问记录等隐私管理功能，此外，MagicOS 还提供设备标识符体系和差分隐私等隐私保护技术手段，进一步保护用户的个人隐私。

权限管理

MagicOS 系统提供了权限的安全机制，旨在允许或限制应用程序访问受限的 API 和资源。默认情况下，应用程序没有被授予权限，通过限制它们访问设备上的受保护 API 或资源，确保了这些 API 和资源的安全。权限在应用程序安装或运行时由应用程序请求，由用户决定授予或不授予。MagicOS 允许用户对已安装的应用程序所申请的权限进行细粒度的控制，可单独允许 / 禁止使用某个权限。权限管理功能管理的权限主要包括：

- 电话
- 短信
- 通讯录

- 通话记录
- 相机
- 位置信息
- 麦克风
- 日历
- 身体传感器
- 健身运动
- 照片和视频
- 音乐和音频
- 文档和文件
- 发送彩信
- 使用呼叫转移
- 悬浮窗
- 创建桌面快捷方式
- 通知
- 设备应用列表
- 附近的设备
- 健康数据

MagicOS 5.0 对应用申请使用相机、麦克风、位置权限时，向应用提供“使用本应用时允许”和“本次使用允许”更细颗粒度的管控能力。当应用申请权限时，如果用户选择“使用本应用时允许”，用户使用应用时，应用拥有

访问相机、麦克风、位置信息的权限；当应用被切换至后台，应用不再拥有访问相机、麦克风、位置信息的权限。如果用户选择“本次使用允许”的授权方式，则应用在本次应用运行周期内，可使用对应的权限；当应用切换到后台或停止运行后，则本次授予的权限会被系统回收，下次使用此权限，需要重新向用户申请授权。

文件访问权限

为了进一步提升用户储在公共存储中文件的安全，MagicOS 7.2 开始把存储权限细分为照片和视频，音乐和音频，文档和文件三种文件类型进行单独授权。MagicOS 8.0 开始支持“选择部分照片和视频”，用户可以向应用授予部分图片和视频的访问权限，而无需向应用授予对整个媒体库的访问权限。

隐私访问记录

移动智能终端设备应用软件的爆发式发展，使得应用软件的功能越发强大，同时为了实现丰富的功能服务，应用软件需要操作系统授予的权限也种类纷繁，其中不乏与用户隐私密切相关的权限。操作系统在授予应用软件权限后，缺乏有效的管控、监督机制，导致部分应用软件在获取权限后可以在用户无感知的情况下调用获取用户隐私数据的功能，即使发生隐私泄露事件，也无有效的记录查证。

MagicOS 5.0 对应用每次访问敏感数据的行为系统都会记录下应用名称、访问权限、访问时间和访问结果等信息。在“设置>隐私”主界面，展示访问位置，相机，麦克风，联系人和存储次数最多 TOP 5 的应用，方便用户快速了

解隐私数据被应用访问的总体情况。同时系统也提供了按照时间、应用和权限三个维度的展示页面，方便用户从多个维度查看隐私访问记录。

MagicOS 6.0 对应用访问存储数据的行为实现细粒度的记录。在隐私访问记录中把存储数据细分为图片，音频，视频和其他文件四种类型，把应用对文件的读取，新建，修改和删除四种操作进行记录。当图片和视频文件被三方应用删除时，系统会将删除的文件移动到图库回收站并及时通知用户以保护用户数据资产的安全。

录音/录像提醒

为了避免恶意应用通过欺骗的方式获取麦克风/相机权限，在用户不知情的情况下进行录音/录像，MagicOS 提供了录音录像提醒功能。当应用程序使用麦克风或者摄像头时，系统会在通知栏提醒用户有应用正在使用麦克风或者摄像头。用户点击该提示时，会跳转到该应用的界面或者该应用的权限管理界面。用户也可以点击提示中的关闭按钮，关闭正在录音/录像的应用。

定位服务

MagicOS 在设置中提供一个定位服务的开关，选择关闭定位服务后，将同时关闭 GPS/WLAN/蓝牙/基站信息的四种定位功能，彻底关闭用户的位置信息，保护用户的隐私安全。

如果应用需要通过定位服务获取位置信息，应用需要申请位置信息权限，用户可以根据应用功能场景，决定是否授予应用位置信息权限（禁止，仅本次运行允许，仅使用期间允许、始终允许）。当用户选择“仅本次运行允许”，

则应用停止运行或切换到后台一段时间后权限会被系统回收，应用将无法获取位置信息；当用户选择“始终允许”，则应用在前后台都可以获取位置信息；当用户选择“拒绝”，则应用不能获取到位置信息。

当用户选择始终允许时，系统检测到应用在后台获取位置信息，会定期通过通知询问用户是否允许后台访问，每个应用系统只会提醒一次。

MagicOS 5.0 在精确位置和粗略位置的基础上，跟进一步向用户提供模糊位置功能。用户可针对具体应用决定是否限制该应用只能获取模糊位置信息，将定位精度降低，无法获取用户精确位置，防止用户被精确定位追踪。

剪贴板内容自动清除

在日常使用手机的过程中，剪贴板难免会存留一些重要的信息，比如快递的收货信息、电话、邮箱，甚至密码。为避免用户隐私信息泄露，当剪贴板内容更新 15 分钟后该内容会被自动清除。当应用读取剪贴板内容时，系统通过消息提醒用户该应用的读取行为。

设备标识符体系

在系统处理过程中，都需要有唯一的辨识信息。荣耀 MagicOS 提供了多种具有不同行为特性的唯一标识符。应用根据不同的场景选择最合适标识符。这些特性涉及到隐私权。

作用域

MagicOS 标识符的作用域分三种，标识符授予的作用域越大，其被跟踪的风险就越大：

应用级 ID：仅限某个应用使用，其他应用无法访问。

应用组 ID：可供一组相关应用访问，例如同一应用开发者开发的多个不同应用

设备级 ID：可供安装在设备上所有应用访问。

重置性与持久性

重置性和持久性定义了标识符的生命周期。标识符保存时间越久，用户被长期跟踪的风险就越高。应用重新安装时或者手动重置标识符，能缩短其持续时间，减少被跟踪风险。

为了防止应用通过设备标识符对用户进行追踪，MagicOS 禁止第三方应用获取设备的永久性设备标识符，如 IMEI、SN、MAC。

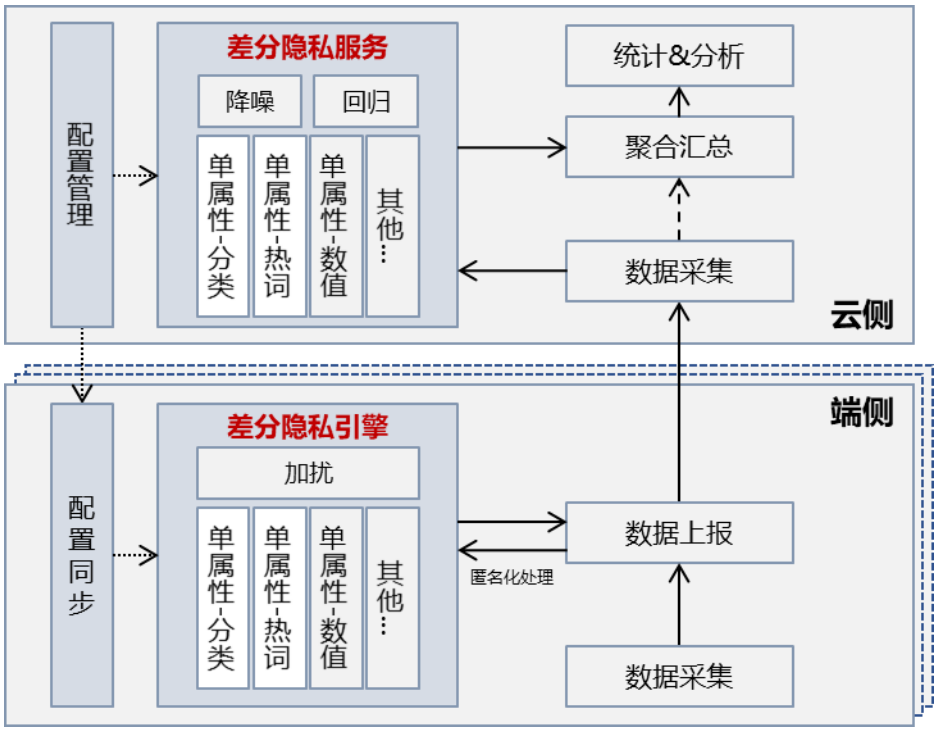
MagicOS 标识符体系包括：

ID 类型	ID 名称	使用场景&作用域	生成时机	重置性
随机标识符	UUID	可供应用关联随机标识符场景下使用	每次调用都生成一个随机数	每调用一次重新生成 UUID
用户 ID	Honor ID	荣耀账号 ID，用于荣耀云服务特性	创建荣耀账号时生成	销毁荣耀账号时删除

差分隐私

随着信息技术的快速发展和个性化服务的不断演进，MagicOS 为用户提供了智慧化推荐服务（YOYO 建议）。在征得用户隐私同意后，需要收集用户数

据和行为记录，以改善智慧化的推荐服务体验。我们会通过差分隐私技术，实现对用户隐私的保护。通过对用户共享上传云端的个人数据中添加随机噪声，使得云端无法获知用户真实数据。云端获取的被加噪数据，通过去噪声和数据聚合，可相对准确还原出统计类信息，以支持提升智慧化服务体验，同时无法推断或区分个人信息，达到用户隐私保护目的。



差分隐私平台框架

MagicOS 7.0，我们基于 YOYO 建议中的“复制直达”功能提供差分隐私保护，具体包括以下几个环节：

1. 个人数据加噪：“复制直达”功能会根据系统识别的不同类型（手机号码，快递单号，邮箱地址等）文本内容提供不同的功能操作（如手机拨打电话，发信息，复制和分享等功能），为了改善体验，云端需要收集用户的功能选择。在上报该数据时，手机会对用户功能操作记录加噪，使得数

据分享到云端后，个人的数据变成不可区分，个人潜在用户隐私（行为和习惯）得到了保护。

2. 降噪和回归：云端收集来自不同用户的功能选择记录，需要对这些数据进行降噪、聚合和回归处理，最终得到相对准确的群体用户对特定类型文本内容功能操作的选择倾向，期间特定个人选择倾向无法被推断和区分；而这些统计信息将被用于 YOYO 建议-复制直达的 AI 算法体验改进。

3. 隐私预算：个人分享的数据，会根据隐私敏感程度的不同，会进行不同力度的数据加扰，以消除个人数据分享的顾虑。这里，数据加扰的力度是隐私预算。隐私敏感程度越高，隐私预算分配的越小，数据加扰的力度越大；反之，隐私预算分配的越大，数据加扰的力度越小；另外，隐私预算在分享数据频次(如每天、每月)，也是关键的衡量因素，预算花销随频次线性累加。YOYO 建议-复制直达，参考业界水平，隐私预算 Epsilon = 4。

4. 用户感知：个人数据分享到云端，最大的顾虑是上云数据，通过数据本身或是三方的信息能够反推到具体某个人，伴随就是个人（隐私）信息的泄露。而差分隐私从最开始手机侧分享时，就通过技术手段，保证了分享上云的数据为非个人数据。

隐私计算平台，在保护用户隐私的技术手段上除了差分隐私，还包括联邦学习、安全多方计算和基于 TEE 机密计算等一系列的技术，未来伴随着这些技术的不断成熟，会结合不同的应用场景和领域，使得在用户隐私保护的前提下，用户体验得到不断的改进。

隐私政策声明

MagicOS 在系统中有明确的隐私政策声明，在开机向导时会明确提示用户进行查看和确认，除此之外在设置中可以查看隐私政策声明，由于每个国家隐私政策会有所不同，请以每个国家发布的 MagicOS 版本中对应的隐私声明政策为准。

隐私政策声明请参考： https://www.hihonor.com/privacy-policy/worldwide/

结语

荣耀非常重视用户的设备安全和隐私安全， MagicOS 提供从底层芯片、操作系统至应用的端到端安全保护能力：基于芯片硬件构建设备可信的基础架构，依托设备硬件更高的安全性与良好的计算性能，打造安全和用户体验兼顾的安全体验。

在提供安全解决方案的同时，荣耀非常重视安全流程和安全能力的建设，以实现对产品生命周期的安全管理。荣耀设立了专门的安全应急响应中心（Security Response Center，SRC），致力于提升产品的安全性。任何发现荣耀产品安全漏洞的组织或个人，可以通过以下方式联系荣耀：security@hihonor.com。荣耀安全应急响应中心的同事会在最短的时间内与您取得联系，同时组织内部漏洞的修复，并进行发布漏洞预警和推送补丁更新，荣耀真诚与您共同构筑荣耀设备的安全。

缩略语表/Acronyms and Abbreviations

缩略语清单

英文缩写	英文全称	中文全称
2D	Two Dimension	二维
3D	Three Dimension	三维
3DES	Triple Data Encryption Standard	三重数据加密标准
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用软件编程接口
APK	Android application Package	Android 安装包
ARM	Advanced RISC Machines	高级精简指令集计算机器
ASLR	Address Space Layout Randomization	内存地址随机化机制
BLE	Bluetooth Low Energy	低功耗蓝牙
BTI	Branch Target Identification	分支目标识别
BYOD	Bring Your Own Device	携带自己的设备办公
CA	Certificate Authority	证书颁发中心
CC	Common Criteria	通用标准
CE	Credential Encryption	凭据加密
CFI	Control Flow Integrity	控制流完整性
CNN	Convolutional Neural Network	卷积神经网络
DE	Device Encryption	设备加密
DEP	Data Execution Prevention	数据执行保护
CMP	Certificate Management Protocol	证书管理协议

DAC	Discretionary Access Control	自主访问控制
DRM	Digital Rights Management	数字版权保护
EAP	Extensible Authentication Protocol	可扩展认证协议
ECB	Electronic Code Book	电子源码书
ECC	Elliptic Curve Cryptography	椭圆加密算法
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
eID	electronic IDentity	电子身份标识
EMM	Enterprise Mobility Management	企业移动管理
eMMC	Embedded Eultimedia Card	嵌入式多媒体卡
MagicOS	MagicOS	荣耀 MagicOS 系统
GP	GlobalPlatform	全球平台组织
GSM	Global System for Mobile Communications	全球移动通信系统
HKIP	Honor Kernel Integrity Protection	荣耀内核完整性保护方案
HMAC	Hash-based message Authentication Code	散列信息认证码
HOTA	Honor Over The Air	荣耀空中升级
HTEE	Honor Trusted Execution Environment	荣耀可信执行环境
HUK	Hardware Unique Key	硬件唯一密钥
HUKS	Honor Universal Keystore	荣耀通用密钥库系统
ID	Identifier	标识符
IMEI	International Mobile Equipment Identity	国际移动设备标识
IoT	Internet of Things	物联网

IPSec	Internet Protocol Security	因特网协议安全协议
IT	Information Technology	信息技术
JOP	Jump Oriented Programming	跳转导向编程
L2TP	Layer Two Tunneling Protocol	第 2 层隧道协议
LKM	Loadable Kernel Module	可加载内核模块
LSM	Linux Security Module	Linux 安全模块
LTE	Long-Term Evolution	长期演进
LTO	Link Time Optimization	链接时优化
MAC	Mandatory Access Control	强制访问控制
MAC	Media Access Control	媒体接入控制（MAC 地址即媒体接入控制地址）
MDM	Mobile Device Management	移动设备管理
MPPE	Microsoft Point-to-Point Encryption	微软点对点加密协议
NFC	Near Field Communication	近距离无线通信技术
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
NPU	Neural Processing Unit	神经网络处理单元
OS	Operating System	操作系统
OTA	Over The Air	空中升级
P2P	Peer to Peer	点对点
PA	Pointer Authentication	指针认证
PAN	Privileged Access Never	特权模式访问禁止
PIN	Personal Identification Number	个人身份识别码
PKI	Public Key Infrastructure	公共密钥基础设施
POS	Point of Sales	销售点

PPTP	Point-to-Point Tunneling Protocol	点到点隧道协议
PRNG	Pseudo-Random Number Generator	伪随机数生成器
PSK	Pre-Shared Key	预共享密钥
PXN	Privileged Execute Never	特权模式执行禁止
REE	Rich Execution Environment	普通执行环境
ROM	Read-Only Memory	只读存储器
ROP	Return Oriented Programming	返回导向编程
RSA	Rivest Shamir Adleman	RSA 加密算法
RPMB	Replay Protected Memory Block	重放保护存储区
SCEP	Simple Certificate Enrollment Protocol	简单证书注册协议
SCP	Secure Channel Protocol	安全通道协议
SD	Secure Digital Memory Card	安全数字存储卡
SDK	Software Development Kit	软件开发工具包
SELinux	Security-Enhanced Linux	安全增强 Linux
SFS	Secure File System	安全文件系统
SHA	Secure Hash Algorithm	安全散列算法
SN	Serial Number	序列号
SOTER	Standard Of auThentication with fingERprint	指纹授权认证开源方案
SRC	Security Response Center	安全应急响应中心
SSL	Security Sockets Layer	安全套接层
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境
TLS	Transport Layer Security	传输层安全性协议

TSM	Trusted Service Manager	可信服务管理
TUI	Trusted User Interface	可信用户界面
UDID	Unique Device Identifier	设备唯一标识符
UID	User Identifier	用户身份标识符
UUID	Universally Unique Identifier	通用唯一标识符
VM	Virtual Machine	虚拟机
VPN	Virtual Private Network	虚拟专用网
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础结构
WEP	Wired Equivalent Privacy	有线等效加密
WLAN	Wireless Local Area Network	无线局域网
WPA	Wi-Fi Protected Access	Wi-Fi 保护访问
WPS	Wi-Fi Protected Setup	Wi-Fi 保护设置

修订记录

日期	修改描述
2021-08-12	初始版本
2022-03-08	MagicOS 6.0版本更新
2022-11-18	MagicOS 7.0版本更新
2024-01-10	MagicOS 8.0版本更新