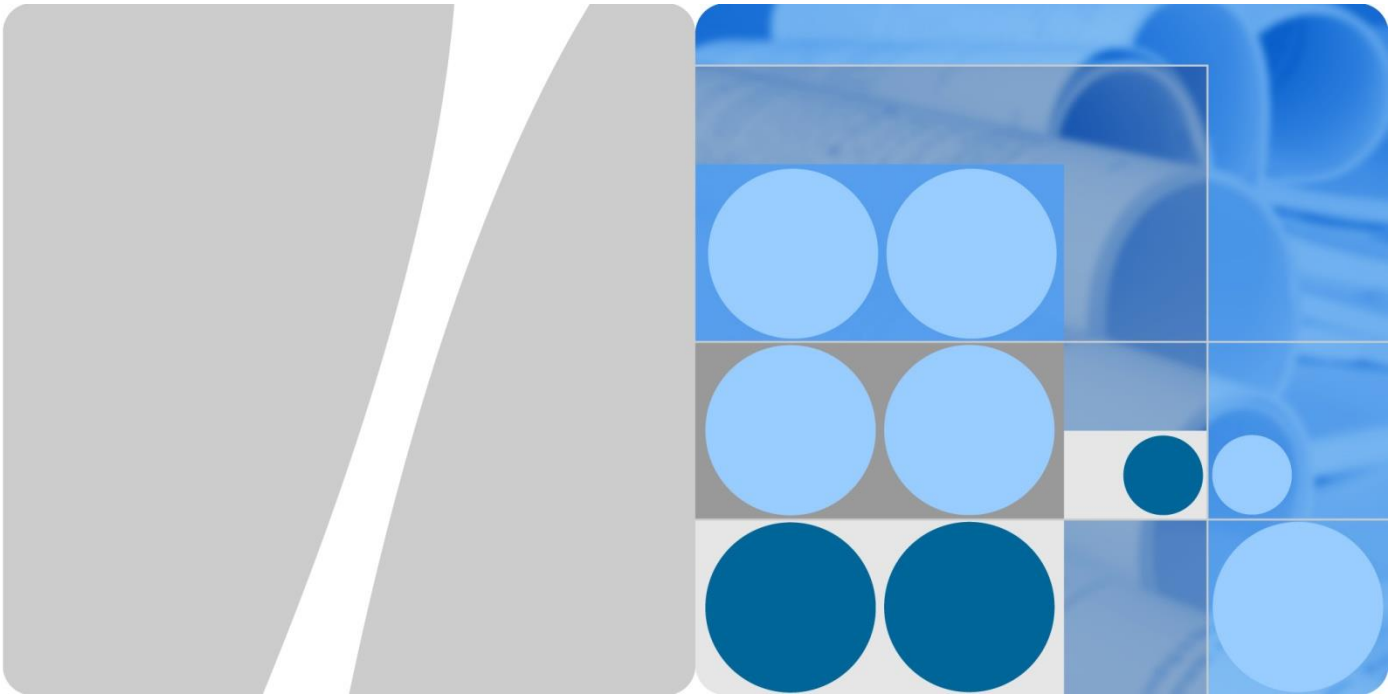

EMUI 5.0 安全技术白皮书

文档版本　V1.0

发布日期　2017-05-31

华为技术有限公司

商标声明

 和其他华为商标均为华为技术有限公司的商标。

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、服务或特性等应受华为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，华为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。

华为技术有限公司

地址：　深圳市龙岗区坂田华为总部办公楼　邮编：518129

网址：　http://www.huawei.com

PSIRT 邮箱：　PSIRT@huawei.com

客户服务电话：　8008308300　4008308300

客户服务传真：　0755-28560818

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。

图目录

1 概述

随着移动互联网的发展，移动智能终端已经成为主要的上网设备，设备中保存了包括用户个人信息在内的大量用户数据；同时，设备安装的应用越来越多，安装来源又不可控，这使得用户面临的隐私以及安全问题越来越突出，移动智能终端的安全问题日益成为消费者关注的焦点。

移动智能终端的应用来源于各种渠道，除了厂商预装外，还可能来自第三方，用户可能下载到带有恶意威胁的应用。恶意应用可能侵犯用户的隐私或窃取用户的财产等，给用户带来各种安全隐患。

华为非常重视移动智能终端的安全性，在保证良好的产品体验的同时，也为用户提供芯片级的安全保障。本文档将系统描述 EMUI（Emotion UI）提供的安全和隐私保护方案，重点介绍 EMUI 在 Android 的基础上做的增强和补充。

EMUI 是华为基于 Android 进行深度定制的移动终端系统。由于 EMUI 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。

安全是系统化的工程。EMUI 提供从硬件、系统、应用到云端的端到端安全保护（如图 1-1 所示），包括硬件芯片、系统内核、数据、应用、网络、支付、云服务和设备管理的安全以及隐私的保护。

EMUI 从底层硬件芯片开始提供安全启动机制来保证 EMUI 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，同时 Android 原生系统提供 Verified Boot 保证 Android 系统启动过程的安全性，防止启动过程中对 Android 的篡改和恶意代码植入，从而确保系统从硬件芯片到 Android 启动的安全。

为保证数据安全，用户数据基于硬件提供的 HUK（Hardware Unique Key，设备唯一密钥）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目录，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 EMUI 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 Android 安全沙箱和权限管理等安全机制外，EMUI 通过预置手机管家提供病毒查杀、骚扰拦截、流量管理、通知管理等功能，安装应用时会自动检测应用是否包含病毒木马，并对应用提供细粒度的权限管理、流量管理和通知管理功能。

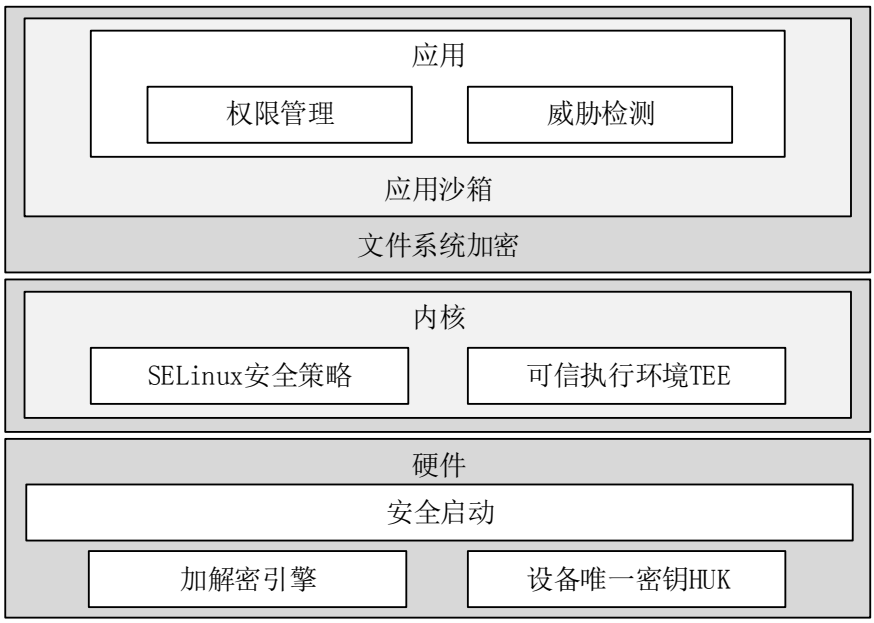

图1-1 EMUI安全架构

- 硬件芯片：安全启动、硬件加解密引擎、设备唯一密钥HUK、设备证明密钥对、TEE、安全存储、指纹认证
- 系统安全：完整性保护、SELinux访问控制、内核地址空间布局随机化、系统软件更新
- 数据安全：锁屏密码保护、文件系统加密、SD卡锁、安全擦除
- 应用安全：应用签名、应用沙箱、运行时内存保护、安全输入、应用威胁检测、恶意网址检测、流量管理
- 网络安全：VPN、SSL/TLS、WPA/WAP2、安全Wi-Fi检测
- 通信安全：防伪基站、骚扰拦截、短信加密
- 支付安全：Huawei Pay、支付保护中心、验证码短信保护
- 互联网云服务安全：华为帐号、双重认证、华为帐号消息、HiCloud、基于帐户的密钥、HiCloud云备份、防火墙、入侵（检测）防御系统、云数据安全存储及访问、云数据的备份及恢复
- 设备管理：查找我的手机、激活锁、MDM移动设备管理、移动设备管理API、设备证书授权
- 隐私保护：权限管理、位置服务、通知管理、应用锁、文件保密柜、隐私空间

2 硬件安全

本章节主要阐述华为设备的硬件芯片安全，包括如下关键安全特性：

- 安全启动
- 硬件加解密引擎
- 设备唯一密钥（HUK）
- 设备证明密钥对
- 硬件随机数生成器
- TEE可信运行环境

安全启动

安全启动是防止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，确保软件的可信性和完整性。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。

启动程序是驻留在硬件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，设备上电后最先执行此代码。

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）。片内引导程序利用保存在主芯片内部 Fuse 空间（熔丝熔断，可保护公钥数据不被恶意篡改）的公钥对二级引导程序镜像的数字签名进行校验，验证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，防止未授权程序被恶意加载运行。

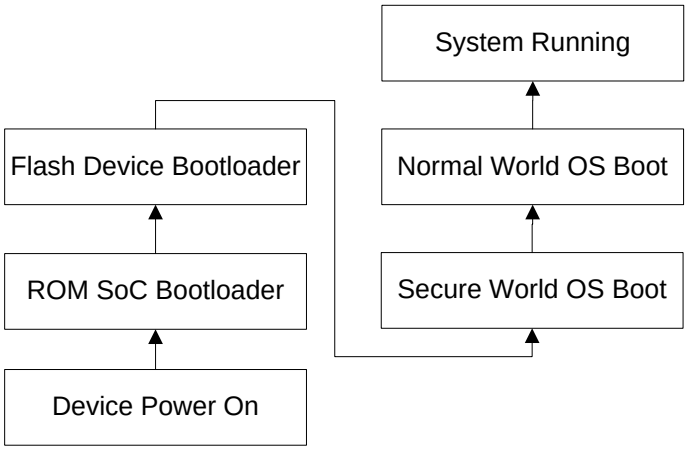

图2-1 安全启动

硬件加解密引擎

芯片提供了高性能的硬件加解密加速引擎，支持的主要算法有：

- 3DES
- AES128、AES256
- SHA1、SHA256
- HMAC-SHA1、HMAC-SHA256
- RSA1024、RSA2048
- ECDSA-256

设备唯一密钥（HUK）

设备唯一密钥（简称 HUK，Hardware Unique Key），保存在芯片内部 Fuse 空间，只有硬件加密引擎能够访问，每台设备都不相同，HUK 是设备的硬件信任根。

设备证明密钥对（Device Attestation Key Pair）

为了证明设备是可信的，EMUI 在可信执行环境 TEE 内部，派生与设备硬件、业务信息绑定的 RSA 和 ECC 的公私钥对，用于在不同场景下的设备身份证明。

硬件随机数生成器

对于会话密钥、初始向量的生成，以及以防重放攻击为目的的随机数生成，通常要求使用高熵值的随机数。为确保达到可接受的安全级别，华为手机芯片提供满足 NIST SP 800-90A 标准的 CTR_DRBG 随机数生成器，其种子来源为满足 NIST SP 800-90B 标准熵源要求的硬件熵源。

TEE

EMUI 支持不同芯片平台的 TEE（Trusted Execution Environment，可信执行环境）安全操作系统。海思平台上，TrustedCore 是基于 ARM TrustZone 设计的 TEE 系统。TEE 基于 TrustZone 的硬件隔离安全区域，将内存、运行环境和屏幕等与外部 Android 系统隔离，确保免遭恶意的软件攻击。

安全存储*

安全存储功能是基于 TEE 提供的安全文件系统（SFS）实现的安全功能，可以安全存储密钥、证书、个人隐私数据和指纹模板等。

TEE 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 AES-256 硬件的加解密，兼容 GP TEE 标准规范。安全存储的密钥通过设备 HUK 进行派生，密钥不出设备 TrustZone 安全区，经密钥加密过的数据安全区外部无法解密。

EMUI 进一步提供了基于 Flash 的 RPMB（Replay Protected Memory Block）分区功能来保护一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 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 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。

可信 UI（TUI）*

在 Android 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，基于 TEE 提供了 Android 侧无法截屏的 TUI（Trusted UI，可信 UI）显示技术（符合 GP 规范），使用 TUI 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 Android 侧对该显示区域的访问，可防止 Android 恶意应用对于显示和输入的劫持和篡改。

指纹认证

指纹是人固有的个人生理特征，主要用于身份认证等重要场合。

EMUI 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完全在 TEE 中，基于 TrustZone 的芯片硬件隔离，外部 Android 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。外部 Android 任何第三方应用无法获取到指纹信息，也不能将指纹数据传出。

指纹模板数据通过 TEE 的安全存储或 RPMB 进行存储，采用 AES256 级别的数据加密强度，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。

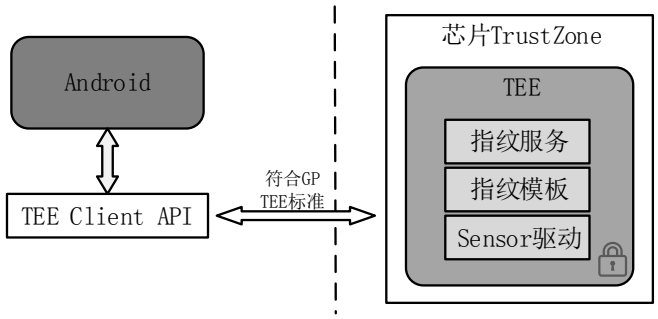

图2-2 指纹安全框架

3 系统安全

本章节主要阐述设备的系统安全，Android 系统本身已经有 Linux Kernel LSM、权限控制、进程保护等安全机制，EMUI 在原有系统安全的基础上做了进一步增强。

完整性保护

EMUI 支持 Android 的 Verified Boot 功能，提供基于块设备的完整性检查，有助于防止永久驻留的 Rootkit 恶意软件持有 ROOT 权限危害设备。此功能可帮助用户确保在启动设备时处于与上次使用时相同的状态。

内核安全

SELinux 访问控制

EMUI 支持 Android 原生的 SELinux 特性，对所有的进程、文件和操作等资源的访问实施强制访问控制，访问控制的策略无法被第三方更改，并在设备启动过程中被保护起来。SELinux 能够阻止进程读写受保护数据、绕过内核的安全机制或者攻击其他进程。

内核地址空间布局随机化（KASLR）

EMUI 支持内核地址空间布局随机化机制，将加载的 LKM 的加载地址和内核栈初始地址在一定范围内进行了随机化。

采用地址随机化技术，内存地址空间不可预测，攻击代码无法对内存中的地址进行硬编码，进一步提升了系统内核的安全性。

系统软件更新

EMUI 支持设备的 OTA 升级，以及时修复可能存在的漏洞。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，EMUI 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 Hash 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。

4 数据安全

本章节主要阐述 EMUI 的数据安全防护，EMUI 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。华为部分终端设备支持 SD 卡，SD 卡上存储了大量的用户数据，在设备丢失时 SD 卡可以被拔出并直接在其它设备读取，从而造成数据泄露，为了保护 SD 卡数据安全，EMUI 提供 SD 卡锁功能。

锁屏密码保护

锁屏密码通过设备唯一密钥 HUK 保护，对用户创建或者验证的锁屏密码处理完全在 TEE 环境中进行。EMUI 对用户的密码输入错误尝试进行限制，防止锁屏密码被暴力破解。密钥的处理主要在 TEE 中并通过与 Android 侧的 Keystore 模块来对外提供安全服务。为了防止密钥被恶意使用，在密钥创建时就增加了访问控制，例如身份认证、生命周期等安全特征。只有调用者通过了认证，才有权使用密钥。

文件系统加密

为防止手机丢失后，未授权用户通过对于设备的物理攻击（如直接读取 Flash）获取设备的内容，造成用户数据泄露，EMUI 提供了对于用户文件系统的数据加密保护。

EMUI 提供基于 Android N 版本的文件级加密功能，利用内核的加密文件系统模块和硬件加密引擎，采用 XTS 的 AES256 算法实现加密。同时用户数据的加密密钥使用用户锁屏密码和设备唯一密钥 HUK 派生的密钥共同保护，防止在无锁屏密码的情况下未经授权访问存储数据。当设备启动时，设备默认是被加密并锁定的，只有部分特定应用可以运行，例如可以打电话和使用闹铃，想要使用其他功能或访问用户数据就必须先解锁手机。此外，设备提供抵抗字典口令猜测攻击的安全机制，防止暴力破解。

为保障用户数据安全和应用体验，Android N 版本的存储区域分为三个部分：设备加密区（DE）、凭据加密区（CE）、非加密区（NE）。应用默认的存储位置一定是凭据加密区，以保证应用安全。

- 设备加密区（DE）在用户开机后但还没有解锁屏幕前，此区域数据即可访问，如Wi-Fi认证、蓝牙配对数据、闹钟、铃声等。
- 凭据加密区（CE）需要验证用户合法性（需要输入锁屏密码），如帐号密码、联系人、短信、日历、通话记录、位置信息等。
- 非加密区（NE）则完全不加密，这种情况极少，比如OTA升级包。

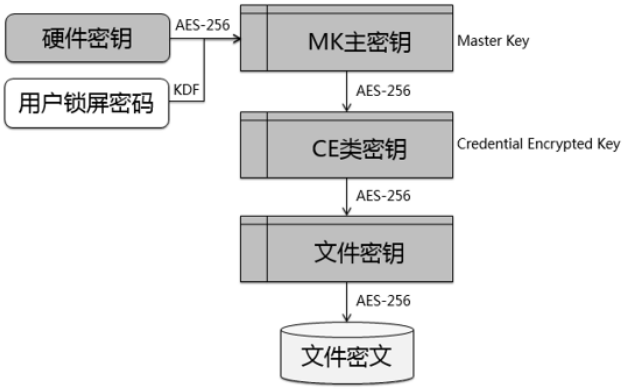

图4-1 文件加密

SD 卡锁*

SD 卡作为手机的主要存储设备之一，保存了很多用户的照片、日记、录音和视频等个人数据，但由于 SD 卡是可拔插的设备，且可以被拔出放入其他设备进行读取，SD 卡的数据安全非常重要。

EMUI 提供 SD 卡锁定功能，基于 SD 卡标准协议实现，为外置 SD 卡提供设置密码、修改密码以及取消密码等功能。密码支持数字以及大小写字母，长度最大可支持 128 比特。

SD 卡锁为用户提供静态数据保护能力，防止从设备上拔出后被非法读取。当 SD 卡被拔出时会自动锁定，只有输入正确的 SD 卡密码后才能对存储在 SD 卡的数据进行访问，保证用户数据的安全。为提高易用性，SD 卡锁支持记住密码功能，在本机使用时可避免重复输入密码。若用户忘记 SD 卡密码，可通过强制清除功能，将 SD 卡的密码和数据同时删除。

安全擦除

设备恢复出厂设置时，为用户提供了彻底删除用户数据的选项。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。

当用户选择格式化内部存储空间时，系统会对文件加密的密钥进行覆写操作实现对密钥的彻底删除，以实现无法恢复密文状态的用户数据。恢复出厂数据彻底删除功能能够保护用户设备转售、废弃后的数据安全。

5 应用安全

本章节主要阐述应用程序的安全。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，EMUI 提供了恶意威胁查杀、恶意网址检测等功能保证应用程序的安全性。

应用签名

EMUI 只允许安装具有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。

Android 应用程序采用自签名（self-signed）证书机制，该证书也不需要被认证机构签名。代码签名的目的在于：

- 检测应用程序的完整性（是否被篡改）及合法性（是否来自合法的开发者）；
- 应用升级时，只有新旧应用的签名证书一致，才允许进行升级；
- 在应用程序之间建立信任。具有相同用户 ID 的应用，基于这一信任关系可以安全地共享代码和数据。

应用沙箱

EMUI 使用 Android 原生提供的应用沙箱机制，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。

运行时内存保护

程序在运行时，若每次运行分配使用的内存的地址是相对固定的，容易被恶意应用通过查看内存的方式获取到，EMUI 支持 Android 原生的地址空间布局随机化 ASLR 及数据执行保护技术 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。提高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。

安全输入

在用户输入密码的场景下，EMUI 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，确保用户的密码输入安全。（注：部分银行 APK 会使用自己开发的输入法，安全输入法不会生效）

应用威胁检测

第三方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。Android 系统安装应用时支持检查应用来源是否合法，默认情况下，系统只允许安装华为官方应用市场提供的应用程序。建议用户将手机设置为不允许安装未知来源的应用，以免带来风险。

华为应用市场提供了超过 10 家顶级的恶意威胁查杀引擎以及人工审核的方式来保证官方应用来源的安全，建议用户从华为官方应用市场下载，保证应用的安全。

设备侧提供了手机管家功能，内置业界领先的杀毒引擎，依靠本地和云端两种强大的威胁查杀引擎，支持本地和联网两种扫描方式，能够及时发现用户下载的安装包以及正在运行的应用是否存在病毒。一旦发现病毒会立即警告用户，并提示用户删除病毒。

恶意网址检测

EMUI 提供了对浏览器网页以及短信等使用场景中的恶意网址的威胁检测功能，检测是否是钓鱼网站或者是带有恶意威胁的网址。EMUI 在用户浏览网页时，会检测访问的网址，浏览器能够及时拦截对此类网站的访问，并提醒用户网站中存在的安全风险。同时在接收短信时能够自动识别出短信中的恶意网址，提醒用户存在的安全风险。

流量管理

EMUI 提供了流量管理功能，包括移动数据和 Wi-Fi 所消耗的流量管理，两者分别统计，实现细粒度管理。流量管理功能实时监控各应用使用数据流量的情况，并将各应用消耗的流量展示给用户，同时可以控制各应用对应的联网类型，防止恶意应用在后台偷跑流量。

6 网络安全

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 EMUI 的网络连接与传输的安全机制。EMUI 采用标准的网络安全协议，如：VPN、SSL/TLS、Wi-Fi 等，保证设备在连接及数据传输时的安全。

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。VPN 网络用户可以进行安全的数据传输，可以掌握对网络的完全控制权。

设备支持 VPN 设置，用户可设置自己的 VPN 参数，从而在设备上安全的访问敏感信息。

设备支持的 VPN 模式包括：PPTP，L2TP，L2TP/IPSec PSK，L2TP/IPSec CRT。

SSL/TLS

设备支持 SSL v3 和 TLS v1.0,1.1,1.2。通过第三方 OpenSSL 协议栈支持 SSL/TLS 协议。

WPA/WPA2

对于 Wi-Fi 连接支持 WEP，WPA/WPA2 PSK，802.1x EAP，WPS，WAPI 等多种认证方式供不同安全级别需求的用户选用。

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。

安全 Wi-Fi 检测

公共场所等外部 Wi-Fi 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。EMUI 提供了对 Wi-Fi 接入点的威胁检测引擎。对需连接的 Wi-Fi 进行检测，一旦发现风险将会提示用户 Wi-Fi 热点的安全风险，用户可以进行对应的操作，确保用户的 Wi-Fi 连接的安全。

7 通信安全

本章节主要阐述EMUI对于设备通信所提供的安全防护。用户经常收到骚扰电话、诈骗短信，为了防止用户上当受骗，EMUI 提供了防伪基站、骚扰拦截和短信加密功能来确保通信安全。

防伪基站*

伪基站短信不仅给用户带来骚扰，通常还可能带有恶意网址等信息，容易造成用户上当受骗。EMUI 基于海思芯片（其它芯片平台不支持）提供芯片级伪基站防护功能，通过对 GSM 伪基站的参数特征以及周边正常基站的分析，识别最安全的基站进行驻留，Modem 侧在尝试驻留解码系统消息时，识别出伪基站，不驻留满足伪基站特征的小区。

同时 EMUI 与银行进行网址的官方认证合作，对接收到的银行类伪基站短信，若网址中带有“XX 银行”的短信时，EMUI 会针对该银行的网址进行校验是否来自官方的地址，防止伪基站短信的钓鱼。

骚扰拦截

在日常生活中，很多用户会收到广告推销、房产中介、银行贷款等短信或电话，给用户带来骚扰。EMUI 提供对于骚扰电话和短信的拦截能力，能够及时有效地对骚扰短信、电话进行拦截和记录，并支持对记录的清空或者恢复。此外，用户可以在接到骚扰电话后，将来电号码标记为不同种类的骚扰类型，以及将其加入骚扰号码黑名单，防止再次被骚扰。骚扰号码黑名单支持快速从联系人、通话记录、短信等添加，用户也可以手动创建黑名单。

EMUI 提供了以下骚扰拦截规则，用户可以根据需要进行配置：

- 智能拦截：根据云端更新的骚扰号码数据库进行智能拦截；
- 拦截黑名单：根据本地用户自身设定的黑名单进行拦截；
- 拦截陌生人：对通讯录以外的所有号码进行拦截；
- 拦截未知号码：对私人号码和未知号码进行拦截。

短信加密

短信作为用户使用的通信手段之一，短信内容属于个人隐私数据，在网络传输过程中以及设备存储上可能会被窃取，带来信息泄密的风险。EMUI 为了保护短信的通信安全，在 EMUI 默认的短信客户端中提供短信加密的功能。用户可以在短信客户端的设置中启用，由于短信加密需要基于密钥管理服务器，因此短信加密功能的激活需要使用用户的华为帐号，且需要接收方和发送方均为支持 EMUI 的短信加密功能的设备才能支持。短信加密基于对方的电话号码作为公钥进行加密，用户可以在不需要提前告知对方的情况下，给对方发送加密短信，只有接收方才能解密出明文，第三方无法解密。

8 支付安全

本章节主要阐述 Huawei Pay 以及其他移动支付的安全防护。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，EMUI 提供对支付环境的隔离保护以及验证码加密等措施来保证支付安全。

Huawei Pay

通过 Huawei Pay，用户可以使用受支持的华为终端设备以方便、安全和保密的方式进行付款。Huawei Pay 在硬件和软件中都进行了安全的增强设计。

Huawei Pay 的设计还可以保护用户的个人信息。它不会收集可绑定到用户的任何交易信息。付款交易只在用户、商户和发卡机构之间发生。

Huawei Pay 组件

安全元件 (Secure Element)：安全元件是业内公认、经过认证的芯片，它符合金融行业对电子支付的要求。

NFC 控制器：NFC 控制器处理“近距离无线通信”协议，并发送应用程序处理器和安全元件之间以及安全元件和 POS 机之间的通信。

Huawei Pay 应用：在支持 Huawei Pay 的设备上 Huawei Pay 应用指“钱包”，钱包被用来添加和管理信用卡、借记卡，并通过 Huawei Pay 进行支付。用户可以在钱包中查看其付款卡以及关于发卡机构的其他信息等内容。还可以将新的付款卡添加到 Huawei Pay。

Huawei Pay 服务器：Huawei Pay 服务器负责管理 Huawei Pay 中银行卡的状态，以及储存在安全元件中的“设备卡号”。它们同时与设备和支付网络服务器通信。

Huawei Pay 如何使用安全元件

加密的银行卡数据会从支付网络或发卡机构发送到安全元件，此数据储存在安全元件中，并由其安全性功能进行保护。交易期间，终端使用专门的硬件总线通过“近距离无线通信”(NFC) 控制器直接与安全元件进行通信。

Huawei Pay 如何使用 NFC 控制器

作为安全元件的入口，NFC 控制器确保所有非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 控制器只会将来自场内终端的支付请求标记为非接触式交易。

一旦持卡人使用指纹或密码授权支付，控制器会将安全元件准备的免接触式响应专门发送给 NFC 场。因此，免接触式交易的支付授权详细信息会包含在本地 NFC 场中，绝不会透露给应用程序处理器。

银行卡绑定

当用户将银行卡添加到 Huawei Pay 时，华为会安全地将付款卡信息以及关于用户帐户和设备的其他信息，发送给发卡机构。发卡机构将使用此信息，决定是否批准将付款卡添加到 Huawei Pay。

Huawei Pay 使用服务器端调用命令来发送和接收与发卡机构或网络间的通信，发卡机构或网络使用这些调用命令来验证、批准付款卡并将其添加到 Huawei Pay。这些客户端服务器会话使用 SSL 加密。

完整的付款卡号码不会储存华为服务器上。相反，会创建唯一的“设备卡号”并进行加密，然后储存在安全元件中。此唯一的“设备卡号”采用华为无法访问的方式加密。“设备帐号”是唯一的，与通常的银行卡号码不同。发卡机构可以阻止在磁条卡、电话或网站上使用“设备卡号”。安全元件中的“设备卡号”与华为手机是分开的，永不会储存在 Huawei Pay 服务器上或备份到 HiCloud。

将银行卡添加到 Huawei Pay

要手动添加付款卡，需要使用姓名、信用卡号码、过期日期和 CVV 码来辅助绑定过程。用户可以在钱包中键入或使用摄像头来输入该信息。摄像头捕获到付款卡信息后，钱包会尝试填充卡号。在填写好所有栏位后，流程会验证 CVV 码以外的栏位。这些信息会通过加密方式发送到 Huawei Pay 服务器。

如果“核对付款卡”流程返回条款与条件，华为会下载发卡机构的条款与条件并向用户显示。

如果用户接受该条款与条件，华为会将所接受条款以及 CVV 码发送到发卡机构，并执行“绑定”流程。有关您设备的信息（例如，姓名、设备型号以及绑定 Huawei Pay 所需的华为手机，以及添加付款卡时您大致的位置（如果启用了“定位服务”）。发卡机构将使用此信息，决定是否批准将付款卡添加到 Huawei Pay。

“绑定”流程会执行以下两项操作：

- 设备下载代表银行卡的凭证文件。
- 手机将付款卡与安全元件绑定。

额外验证

发卡机构可以决定是否需要对银行卡进行额外验证。根据发卡机构提供的功能，用户可能有以下选择进行额外验证：短信验证。

用户可以选择发卡机构存档的联系信息来获取短信通知，并在钱包中输入收到的验证码。

支付授权

安全元件只有在接收到来自手机的授权，确认用户已使用指纹或设备密码认证后，才会允许进行支付。如果可用，指纹即为默认的支付方式；但是用户可随时使用密码来代替指纹。如果尝试通过匹配指纹 1 次不成功，会自动提供密码输入选项。

使用 Huawei Pay 进行非接触式支付

如果华为手机已开机且检测到了 NFC 场，它会向用户显示相关的银行卡。用户还可以前往 Huawei Pay 应用并选取一张银行卡，或在设备锁定时使用特定指纹触摸指纹感应器唤起付款页面，之后才会传输支付信息。

如果用户不认证，则不会发送支付信息。用户认证后，在处理支付时会使用“设备卡号”和交易专用动态安全码。

暂停使用、移除和抹掉付款卡

即使设备未接入蜂窝移动网络或无线局域网络，发卡机构或者各自的支付网络也可停用或移除设备上 Huawei Pay 付款卡的支付功能。

支付保护中心

支付保护中心提供对支付应用的安全保护，支持支付应用的隔离、应用来源的检测以及支付环境威胁的检测，以保证金融、财产、保险等支付应用的安全性。

应用来源检测：支付保护中心的应用必须来自华为应用市场的支付专区或通过华为应用市场支付专区认证的支付应用；

访问控制和隔离：支付保护中心提供对于空间内外的应用相互调用进行管控或隔离；由于部分支付应用（比如支付宝、微信）与外界有频繁的交互需求，对这类应用只禁止区域外非可信应用（被检测出来的恶意应用）对这部分支付应用的调用；而另外一部分金融财产类应用（如招商银行、同花顺）和区域外无交互需求，这类应用将被深度隔离，不能和区域外的第三方应用相互调用；

威胁检测和系统防护：包含对于恶意威胁、Wi-Fi 威胁、短信验证码、ROOT 等的检测以及输入法安全的保护。

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，EMUI 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。

EMUI 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 EMUI 系统中设置的默认短信客户端，若默认短信客户端为 EMUI 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：此功能只在 EMUI 系统短信应用客户端设置为默认短信应用时生效）

9 互联网云服务安全

华为构建了一系列强大的云服务来帮助用户更充分有效地使用设备，这些互联网服务在设计上继承了 EMUI 在整个平台中推行的安全目标。 无论数据存储在互联网上，还是在网络中传输，云服务都保护用户的个人信息，防范威胁和网络攻击，阻止对信息和服务进行恶意或未经授权的访问。华为云服务采用统一的安全架构，在保护用户数据安全的同时，丝毫不会影响 EMUI 的整体易用性。

华为帐号

华为帐号由用户名和密码组成，用来登录华为的互联网云服务，例如 HiCloud、应用市场、游戏中心、华为视频、华为音乐等等。对于用户而言，保障其华为帐号的安全，防止未经授权访问用户的帐户十分重要。为了达成这一目标，华为要求使用长度至少为 8 个字符的强密码，同时包含字母和数字，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，让密码变得更加安全。在帐户发生重大更改时，华为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华为帐号登录。如有异常发生，华为会提示用户立即更改其华为帐号密码。另外，华为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，以及定期回顾策略以让我们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

为帮助用户进一步保护帐户的安全性，华为提供双重认证功能。双重认证是为华为帐号提供的一层额外安全保护，它的目标是确保仅帐户所有者能访问帐户，其他人即使知道密码也无法访问。有了双重认证，只能在受信任设备上（例如，用户的手机、Pad 或个人 PC）上访问用户的帐户。在任何新设备上首次登录需要两种信息：华为帐号密码和 6 位数的验证码，验证码自动显示在用户的受信任设备上或发送到受信任的手机号码。输入验证码即表明用户确认他们信任新设备，且在该设备上登录是安全的。双重认证意味着已经不能仅靠密码来访问用户帐户，因而提高了用户的华为帐号以及所有通过华为储存的个人信息的安全性。

华为帐号消息

华为帐号的消息功能是一项适用于华为设备的信息收发服务。消息支持文本和附件，例如照片、联系人信息和位置信息。信息会显示在用户所有注册的设备上，

这样用户就可以在其他设备上继续对话。华为不记录信息或附件，同时其内容受端到端的加密服务保护。

HiCloud

HiCloud 提供储存用户的通讯录、信息、相册、通话记录、备忘录、日历和其他内容的功能，并让这些信息在其设备间自动保持最新。用户可以通过登录华为帐号来设置 HiCloud 并选取想要使用的服务。当用户退出华为帐号时，HiCloud 会在获取用户的确认后，将与退出华为帐号相关的 HiCloud 数据删除，以保证您的个人数据不在不使用的设备上保存，您可以在新认证的设备上使用华为帐号登录，从而恢复 HiCloud 数据。

基于帐户的密钥

HiCloud 每个文件被分为区块，并由 HiCloud 使用 AES-128 为每个区块内容进行加解密。HiCloud 加解密的前提是登录华为帐号。在用户成功登录华为帐号后，HiCloud 为用户派生该帐户的加密因子，该因子及每个区块的元数据被传送到硬件加解密系统，HiCloud 文件区块在硬件加解密系统中完成加解密，再通过安全传输通道发送到用户的设备上。当用户的数据存储到 HiCloud 时，它受到与华为帐号绑定的密钥保护。这样意味着任何人（包括华为）均无法读取用户的数据。

HiCloud 云备份

HiCloud 通过无线局域网将信息（包括设备设置、应用数据、设备中的照片和视频等）备份。HiCloud 会在您通过互联网发送内容时对其进行加密、使用基于帐户的秘钥模式进行加密，只有通过无线局域网访问互联网时，“HiCloud 云备份”才会工作。

防火墙

华为互联网云服务根据不同的应用划分为不同的安全组，每个安全组都是一个独立的 VLAN，需要通过配置不同的端口访问策略才能访问。

所有对互联网开放端口的主机都经过防火墙过滤，开放业务必须使用端口供互联网用户访问；通过 IP 黑白名单设置，对进出互联网云服务系统网络的数据包进行过滤，避免业务系统受到网络攻击。

入侵（检测）防御系统

检查进出互联网云服务网络的每一个数据包，及时发现并阻止网络攻击行为，保障所有用户安全、可靠的使用互联网云服务。

云数据安全存储及访问

- **权限控制：**对不同的用户分配不同的权限以限制对数据的访问；
- **数据加密：**通过对数据加密防止非法访问；
- **安全存储：**对数据库采用的是读写分离，主从同步的策略，主服务器采用双机策略，从服务器采用的是多从服务器，从而避免可能出现的单点故障。

云数据的备份及恢复

云服务网络实时对数据库进行异地同步，用以应付紧急的特殊情况，会定期对数据进行备份，并对备份数据进行合理保护。一旦有需要能够及时进行数据恢复，保证用户正常的使用。

10 设备管理

本章节主要阐述 EMUI 的设备管理功能，对于企业用户，EMUI 支持 Android 原生的 Android for Work 框架，提供对于第三方 MDM 平台进行企业证书的申请和授权等能力。对用户手机丢失的场景，EMUI 提供了查找我的手机、远程锁定、远程擦除等功能。

查找我的手机 & 激活锁

EMUI 提供了查找我的手机功能，此功能需用户手动开启才能使用。一旦启用，当用户的手机丢失后，用户可通过网页或手机应用登录华为帐号进行查找设备，擦除数据以及远程锁定等操作，保护设备的数据安全。（注意：此功能只在提供了华为帐号和云服务的国家和地区才能使用。）

此外 EMUI 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华为帐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。

MDM 移动设备管理

MDM 完全继承 Android 原生的 Android for Work，通过创建 work profile，企业 IT 系统可以轻松实现对 Android 设备的控制和管理。Android for Work 支持主流的第三方 EMM 厂商，通过在设备上安装的“设备策略控制器”应用软件实现和 EMM 服务器进行通信，实现对设备的配置和管理策略的下发。

另外，EMUI 对 EMM 厂商开放设备管理的授权 API 接口，在无法提供谷歌移动服务的地区或者不想依赖谷歌移动服务的场景下，设备上安装第三方 MDM 客户端软件，通过调用这些开放的 API 对设备进行管理和控制。API 接口调用需要授权使用，保证接口调用的权限管控和安全性。

移动设备管理 API

针对 EMM 厂商和一些应用开发商需要实现对设备的配置 和访问限制控制，当前 EMUI 提供以下访问限制接口：

- 允许/禁止应用打开蓝牙
- 允许/禁止应用拨打电话
- 允许/禁止应用发送短信
- 允许/禁止应用发送彩信
- 允许/禁止应用获取联系人
- 允许/禁止应用修改联系人
- 允许/禁止应用删除联系人
- 允许/禁止应用获取获取短信和彩信内容
- 允许/禁止应用读取通话记录
- 允许/禁止应用修改通话记录
- 允许/禁止应用删除通话记录
- 允许/禁止应用读取日程信息
- 允许/禁止应用读取个人位置信息
- 允许/禁止应用读取手机设备信息
- 允许/禁止应用打开摄像头
- 允许/禁止应用打开麦克风
- 允许/禁止应用联网访问请求
- 开启/禁用WLAN
- 开启/禁用WLAN热点
- 开启/禁用USB调试模式、数据传输
- 开启/禁用存储访问（MicroSD卡）
- 开启/禁用NFC
- 开启/禁用数据连接
- 开启/禁用通话
- 开启/禁用短信
- 开启/禁用状态栏下拉菜单
- 允许/禁止挂断当前通话
- 允许/禁止关机
- 允许/禁止重启
- 允许/禁止获取ROOT状态
- 允许/禁止保持应用始终运行
- 允许/禁止阻止应用启动运行
- 允许/禁止停止应用进程
- 允许/禁止静默安装某应用

- 允许/禁止静默卸载应用
- 允许/禁止删除应用数据
- 开启/关闭仅以指定应用商店安装应用功能，屏蔽其他应用商店安装，同时屏蔽其他安装方式，如屏蔽ADB和SD卡安装方式
- 允许/禁止应用被安装，屏蔽其他应用安装
- 允许/禁止应用被卸载
- 允许/禁止配置华为邮箱的Exchange参数

设备管理证书授权

对于企业移动办公客户所需的设备管理 API，EMUI 通过签名企业证书的方式来进行权限的授权,企业可以在华为开放平台上申请设备管理 API 的使用授权。

对经过华为审核过的应用开发者，华为通过华为开放平台颁发设备管理证书，开发者在开发的 APK 中集成此设备管理证书后，其 APK 就可以在华为的设备上正常调用授权的 API 接口。

用户安装带有设备管理证书的 APK 时,EMUI 系统会解析并校验证书的每一项内容,所有签名信息通过校验后,证明该证书是华为颁发和真实的,APK 才能通过授权、正常安装，证书校验不正确时，设备管理 APK 会提示安装失败，以保证华为设备的安全。

11 隐私保护

本章节主要阐述对用户隐私的保护。在华为设备中可能存在用户的隐私，如：联系人、短信、照片等；为了保护用户的隐私， EMUI 对预置的应用确保完全符合隐私合规要求，同时提供应用的权限管理、通知管理以及位置服务等隐私管理功能，此外为了进一步保护个人隐私，EMUI 提供文件保密柜，隐私空间，位置信息关闭等扩展功能。

权限管理

Android 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，Android 应用程序没有被授予权限，通过不允许它们访问

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时由应用程序请求，由用户决定授予或不授予。

由于应用程序权限仅在初次安装时提示用户，用户必须同意授权才能完成安装，导致用户对某些应用申请了多余权限束手无策。

针对 Android 现有权限控制的不足，华为对现有应用权限管理进行了扩展增强，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，可单独的允许 / 禁止使用某个权限，权限管理功能能够管理的权限主要包括：

Android定义的权限：

- 电话
- 网络
- 短信
- 联系人
- 通话记录
- 摄像头
- 位置数据
- 录音
- Wi-Fi
- 蓝牙
- 日历

EMUI定义的权限：

- 发送彩信
- 获取运动数据
- 使用呼叫转移
- 获取浏览器上网记录
- 获取已安装列表
- 悬浮窗
- 创建桌面快捷方式

位置服务

为保护用户位置隐私信息，EMUI 基于 Android 原生的位置服务进行了增强，除了可以关闭 GPS 定位服务以外，也能够防止 Wi-Fi 和移动基站的定位，选择关闭位置服务后，将关闭掉 GPS/Wi-Fi/基站信息的三种定位功能，彻底关闭用户的位置信息，保护用户的隐私安全。

通知管理

基于应用频繁的通知对用户所造成的困扰，EMUI 提供了通知管理的功能，用户可以允许或者禁止应用弹出通知，同时在用户允许通知的情况下，EMUI 提供了进一步细粒度的管理，用户可以根据需要设置是否允许应用在状态栏、锁屏界面或在屏幕顶部以横幅方式显示，是否允许响铃或者振动，从而避免应用频繁的通知对用户造成不必要的困扰。

应用锁

为了保护用户手机在借给其它人使用时的隐私安全，EMUI 提供为应用软件设置访问密码，当启动应用时，必须输入正确的密码校验身份，才能使用应用，防止他人未经允许访问锁定应用，保护用户的隐私。

文件保密柜

EMUI 提供了文件保密柜功能，用户可以将一些敏感或重要的个人数据添加到文件保密柜中进行保护。文件保密柜是一个使用用户密码加密的空间，所有的内容都是基于用户的密钥进行加密和保护，只有用户自己才能进入，任何其它人无法访问。

文件保密柜的文件加密采用随机产生的随机密钥以及 AES256 加密算法，加密的密钥使用用户输入的保密柜密码进行加密保护，用户的密码不保存，无法还原。

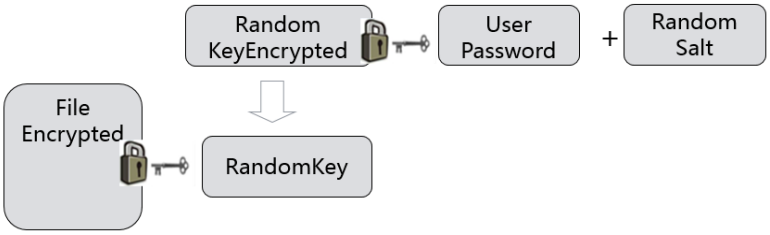

图 11-1 文件保密柜

隐私空间*

为了保护用户的重要隐私，EMUI 提供了隐私空间。隐私空间基于 Android 原生的多用户机制设计，作为一个与主用户隔离的加密、独立用户空间，它的应用数据是独立存储的，与其他用户的应用数据相互隔离。隐私空间提供了存储在 Flash 的数据以及应用的隔离保护，暂不支持 SD 卡上数据的隔离保护。

同时隐私空间还提供了隐藏入口的功能。隐私空间的入口隐藏之后，其他用户空间会完全感知不到隐私空间的存在，除非在主用户锁屏界面输入隐私空间的密码或者指纹进行切换。快速切换用户空间的功能，是指使用不同的指纹或密码进入不同的用户空间：输入机主的指纹或者密码进入主空间，输入隐私空间的指纹或者密码则进入隐私空间（注：隐私空间的指纹不能和主空间的指纹相同）。

隐私政策声明

EMUI 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 EMUI 版本中对应的隐私声明政策为准。

隐私政策声明请参考（更新日期，2016 年 9 月）：

http://consumer.huawei.com/minisite/worldwide/privacy-policy/cn/index.htm

12 结论

EMUI 非常重视用户的设备安全和隐私安全， EMUI 基于芯片硬件提供从底层芯片、系统至应用的端到端安全保护能力。EMUI 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。

EMUI 基于 Android OS 系统开发，在系统层，EMUI 通过内核安全增强来提升系统的安全性，基于底层的可信平台以及系统的安全增强，为上层提供更安全的系统控制能力。在应用层，EMUI 提供了病毒查杀、骚扰拦截、流量管理以及通知管理等功能，同时结合云端来构建 EMUI 的安全。

在提供安全解决方案的同时，华为非常重视安全流程和安全能力的建设，以实现对于产品生命周期的安全管理。

华为设立了专门的 CERT 组织，致力于提升产品的安全性。任何发现华为产品安全漏洞的组织或个人，可以通过以下方式联系华为：PSIRT@huawei.com。华为 PSIRT 应急响应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，华为真诚与您共同构筑华为设备的安全。

13 缩略语表/Acronyms and Abbreviations

表13-1 缩略语清单

英文缩写	英文全称	中文全称
3DES	Triple Data Encryption Algorithm	三重数据加密算法
ADB	Android Debug Bridge	Android 调试桥
AES	Advanced Encryption Standard	高级加密标准

API	Application Programming Interface	应用程序接口
ARM	Advanced RISC Machines	高级精简指令集架构
ASLR	Address Space Layout Randomization	地址空间布局随机化技术
CERT	Computer Emergency Response Team	计算机安全应急响应组
HiCloud	HiCloud	华为终端云服务
DEP	Data Execution Prevention	数据执行保护
ECB	Electronic Code Book	电子密码本模式
ECC	Elliptic Curves Cryptography	椭圆曲线密码编码学
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
EAP	Extensible Authentication Protocol	扩展认证协议
EMM	Enterprise Mobility Management	企业移动管理
EMUI	Emotion UI	华为 EMUI 系统
GP	GlobalPlatform	全球平台国际标准组织
HMAC	Hashed message Authentication Code	哈希信息认证码
HOTA	Huawei Over The Air	华为 OTA
HUK	Hardware Unique Key	硬件唯一密钥
IPSec	IP Security	IPSec 安全协议
L2TP	Layer Two Tunneling Protocol	第 2 层隧道协议
LKM	Loadable Kernel Module	可加载内存模块
LSM	Linux Security Modules	Linux 安全模块
MDM	Mobile Device Management	移动设备管理
NFC	Near Field Communication	近距离无线通信
NIST	National Institute of Standards and Technology	美国国家标准技术研究所
OTA	Over The Air	空中升级
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

ROM	Read-Only Memory	只读内存
RSA	Rivest Shamir Adleman	公开密钥密码体制
RPMB	Replay Protected Memory Block	防重放保护内存
SD	Secure Digital Memory Card	安全数字存储卡
SELinux	Secure Enhanced Linux	安全增强 Linux
SHA	Secure Hash Algorithm	安全哈希算法
SSL	Security Socket Layer	安全套接层
TEE	Trusted Execution Environment	可信执行环境
TLS	Transport Layer Security	安全传输层协议
TUI	Trusted User Interface	可信用户界面
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 安全保护设置