ColorOS 14 安全技术白皮书

2024 年 1 月

1 总述

随着移动互联网飞速发展，智能移动终端逐渐普及和融入人们的工作和生活。现代的智能移动终端是由多种软硬件组成的复杂系统，在提供给用户社交、购物、支付、出行、娱乐等丰富体验的同时，终端用户对于数据安全、隐私保护的诉求越来越突显。

ColorOS 产品安全与隐私

万物互融时代，全新的 ColorOS 产品将安全可信赖融入软件、产品和服务创新中。ColorOS 产品秉承让每一位用户对 ColorOS 产品的安全隐私防护可感知、可掌控、可信赖、人性化的理念，以全链路的数据安全与隐私保护能力建立起 ColorOS 产品与用户的充分联接，持续提升 ColorOS 产品安全与隐私体验与感知。

ColorOS 产品以用户数据安全和隐私保护为核心，建立了完善的内控体系和权限管理流程，实现用户数据存储加密，传输加密，应用行为记录，隐私替身等，全方位保护用户的数据与隐私。ColorOS 作为基于 Android 深度定制的手机操作系统，在设计时即考虑构筑全面的终端安全架构，进行了大量安全和体验性的功能创新，为用户提供端到端的安全保护，旨在为用户提供最高的安全和透明体验。同时，OPPO 的 Find 系列手机终端通过 CC MDFPP 认证；Reno 系列手机终端首发通过中国泰尔实验室移动智能终端安全能力测评，达到五级安全能力要求；一加手机终端通过移动智能终端安全认证证书（五级），一系列认证测评体现了 ColorOS 在产品终端通过软、硬件版本的不断迭代和优化，持续为用户提供全面的安全与隐私防护。

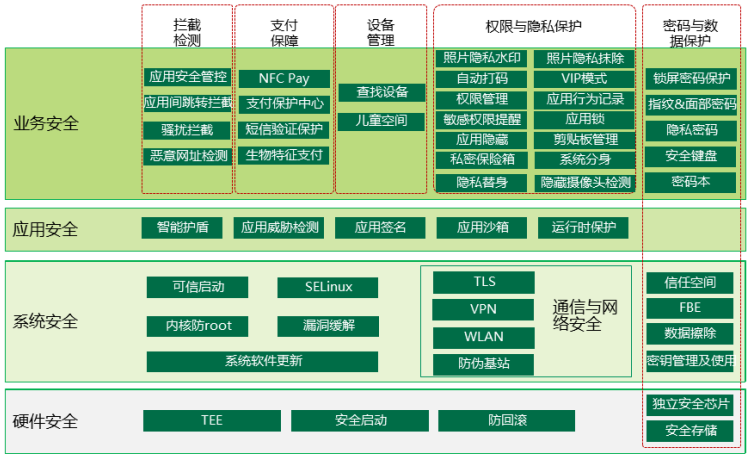

图 1-1　ColorOS 安全架构

ColorOS 以硬件信任根为起点，利用安全启动（Secure Boot）和 Android 启动验证（Verified Boot）机制在“信任根-引导加载程序-系统启动分区”等组件之间建立起完整信任链传递关系。在设备启动过程中，无论哪个阶段，在进入下一个阶段之前先验证下一个阶段的完整性和真实性，确保系统从硬件芯片到系统启动的安全。在系统安全方面，ColorOS 基于 Verified Boot，结合 SELinux、内核防 Root、系统软件更新等机制防止恶意篡改和非法访问，保障系统安全；在应用安全方面，通过应用安全检测、应用签名校验、安全沙箱、运行时保护等安全机制保障应用从上架、安装、运行整个阶段的安全性。

在硬件、系统、应用安全的基础上，ColorOS 开发了一系列安全特性提供拦截检测、支付保护、数据保护、隐私控制等业务安全能力，从而进一步保护用户隐私及数据的安全。

本文详细介绍了 ColorOS 安全性技术和功能，希望可以帮助用户和安全从业人员清晰地理解 ColorOS 安全架构与安全解决方案。本文主要分为以下几个章节：

- 硬件安全：包括可信执行环境、安全启动，防回滚等；
- 系统安全：包括可信启动、SELinux、内核防 Root、漏洞缓解、系统软件更新等；
- 通信与网络安全：包括 TLS、VPN、WLAN、防伪基站等；
- 应用安全：包括智能护盾、应用威胁检测、应用签名、应用沙箱、运行时保护机制等；
- 拦截检测：包括应用安全管控、应用间跳转拦截、骚扰拦截、恶意网址检测等；
- 支付保障：包括手机支付（NFC Pay）、支付保护中心、短信验证保护、生物特征支付等；
- 设备管理：包括查找设备、儿童空间等；
- 密码与数据保护：包括独立安全芯片、安全存储、信任空间、文件系统加密（FBE）、数据擦除、密钥管理及使用、锁屏密码保护、指纹&面部密码、隐私密码、安全键盘、密码本等；
- 权限与隐私保护：包括照片隐私水印、照片隐私抹除、自动打码、VIP 模式、权限管理、应用行为记录、敏感权限提醒、应用锁&应用隐藏、剪贴板管理、私密保险箱、系统分身、隐私替身、隐藏摄像头检测等。

2 硬件安全

硬件安全是整个终端安全的基础，为 ColorOS 提供底层的硬件安全支撑。ColorOS 通过可信执行环境 TEE、安全启动，防回滚机制（Anti-Rollback）等特性和服务来保障上层的系统、应用、数据及业务安全。

2.1 可信执行环境

可信执行环境（TEE, Trusted Execution Environment）是基于芯片级隔离技术，用于保证程序执行安全与数据存储完整性、机密性和真实性为目标构建的一种可信赖的软件运行环境。TEE 为 ColorOS 提供安全服务，使用户的关键数据在这个相对可信赖的环境中使用和运行。

图 2-1　可信执行环境

搭载 ColorOS 的终端设备基于芯片级隔离技术建立两个执行环境。其中，一个环境负责处

理对功能性、开放性等要求较高的业务，即富执行环境（REE, Rich Execution Environment），如上图的 ColorOS 执行环境。另一个负责处理对安全性、私密性要求比较高的业务，即可信执行环境。ColorOS 执行环境中的客户端应用可以与可信执行环境中的可信应用相互交互和协作完成对用户敏感信息的保护。

构建可信执行环境主要涉及硬件和可信软件两方面：

（1）硬件资源隔离

硬件资源隔离是构建可信执行环境的基础。用户的敏感信息可能存储在设备中的 CPU、内存、外设等硬件资源中，这些硬件资源在芯片级安全隔离机制基础上严格隔离。

（2）构建可信软件架构

在硬件安全扩展的基础上，构建可信软件架构，软硬件相结合提供一个安全的软件执行环境。

1）系统软件层：

提供了可信操作系统基本核心功能，包括进程调度管理、时间管理、中断管理、进程间通信管理和外设驱动管理；

提供了可信操作系统的系统级功能，包括用户态和内核态的定义，系统调用访问控制和权限管理；

充分利用安全硬件（如一次性可编程存储（OTP）、重放保护内存块（RPMB）、安全元件、硬件加密引擎等）的可信性，完成安全存储、安全加解密等各种系统服务；

可信操作系统与 ColorOS 之间的通信采用共享内存或消息方式。

2）应用软件层：

各种安全相关的可信应用，如指纹、支付、身份认证等，一般与对应的 ColorOS 应用交互，为用户提供既便捷又安全的用户体验。

2.2 安全启动

硬件的安全启动是系统利用签名私钥确保文件或程序完整性安全机制。在启动过程的任何阶段，所有启动镜像（包括启动引导镜像、内核镜像、基带固件等）必须通过签名公钥校验才可以加载运行，否则启动过程会被终止，以防止加载并运行未经授权的镜像。

ColorOS 基于平台的 Secure Boot 架构，优化了其中的密钥管理策略、签名验证策略和下载认证策略，使得安全启动在 ColorOS 上更加的安全和稳定。通过 ColorOS 安全启动功能，提升了的安全性，包括但不限于：

- 禁止烧写未经授权的官方固件；
- 禁止运行非经授权的官方固件；
- 禁止非法追踪和调试代码，例如 JTAG（Joint Test Action Group）接口和故障转储；
- 对单个芯片设定 IMEI；
- 禁止不同设备（芯片、型号、版本等）固件的交叉写入；
- 对内部而言：密钥管理策略更加安全和保密，以最小权限为原则。普通工程师无法接触和获取到密钥。

2.3 防回滚

ColorOS 支持防回滚（Anti-Rollback）功能，在每台设备的主芯片内部 Fuse 空间中烧写 Anti-Rollback 值，同时在镜像签名中新增 Anti-Rollback 值。在 Secure Boot 鉴权签名的阶段，对 Anti-Rollback 进行检测，防止固件或者镜像降级烧入设备，避免引入低版本漏洞。

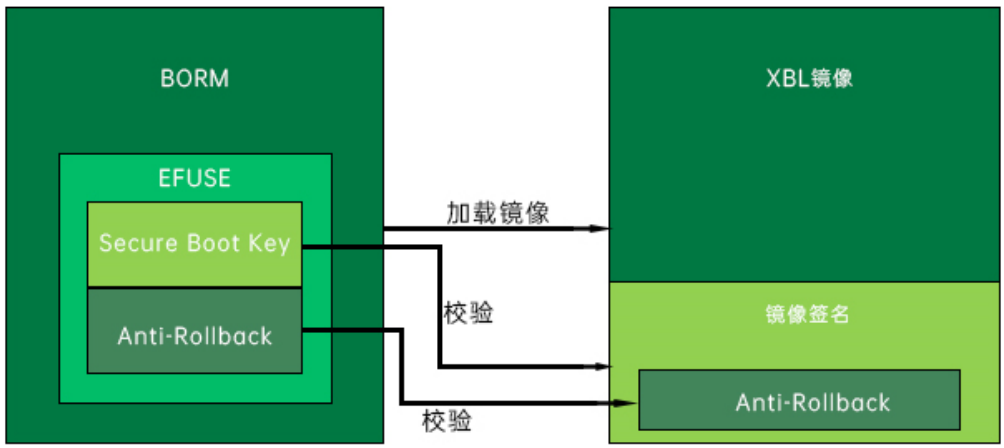

图 2-3 防回滚机制

3 系统安全

系统安全在硬件安全的基础上，结合 SELinux、内核防 Root、系统软件更新等机制防止系统被恶意篡改和非法访问，保障系统安全，主要从可信启动、SELinux、内核防 Root、漏洞缓解、系统软件更新等几个方面构筑 ColorOS 系统安全能力。

3.1 可信启动

安卓启动验证（AVB，Android Verified Boot）是保证终端用户设备上运行软件的完整性的安全机制。在 Secure Boot 的基础上，以通过已被鉴权的 LK（Llittle Kernel）镜像为起点，以信任链的方式确保镜像的合法性和完整性，防止篡改相关镜像入侵系统的行为，提高系统的抗攻击能力。

Secure Boot 和 Verified Boot 结合建立一条从信任根到引导加载程序，再到启动分区和其他已验证分区的完整信任链。在设备启动过程中，无论是在哪个阶段，都会在进入下一个阶段之前先验证下一个阶段的真实性和完整性。

ColorOS 支持 AVB 功能，增加了对 Boot、Recovery、System、Vendor 等镜像完整性和合法性的检测。同时，在 Android P 版本后，可信启动的校验增加了防回滚功能。

3.2 SELinux

SELinux（Secure Enhanced Linux，安全增强性 Linux）是 Android 安全模型的一部分，Android 使用 SELinux 对所有进程执行强制访问控制。ColorOS 支持 Android 原生的 SELinux 特性，通过预定义强制访问控制策略实现进程权限的控制，将进程对系统中的目录、文件、进

程等资源的操作权限最小化，防止绕过内核安全机制的攻击或未授权的数据读写，确保 Android 内核及上层应用的安全运行。

3.3 内核防 Root

ColorOS 致力于为用户提供安全可靠的操作系统，在内核层面上，ColorOS 根据内核非法 Root 后的特征行为设计了动态防御机制，以此来抵御恶意的 Root 手段。ColorOS 将持续对此进行优化，为用户提供更加安全的操作系统。

3.4 漏洞缓解

ColorOS 致力于提供卓越的用户体验，并同时竭尽所能提升安全保障。为此，ColorOS 不遗余力启动了一系列漏洞缓解技术，旨在确保增加安全性而不影响用户体验。这些技术包括但不限于：

- KASLR（Kernel Address Space Layout Randomization，内核地址空间布局随机化）特性：该特性使得内核在内存地址空间的位置变得不可预测，从而使攻击者无法精确定位内核，降低内核漏洞被利用的风险，提升系统安全性。
- PAN（Privileged Access Never，特权模式访问禁止）：这一功能实现了内核态无法访问用户态应用程序的数据，从而有效防止高权限内核窃取应用程序数据的情况发生，更好地保护用户数据安全。
- 内核完整性保护：这一保护机制专为内核设计，利用硬件 Hypervisor 虚拟化技术，实时保护内核完整性。它提供了防止内核代码段和系统重要寄存器篡改的功能，以保护关键位置免受特权模式下恶意代码等威胁的影响，从而提高系统的安全性。

- MTE（Memory Tagging Extension，内存标记扩展）：MTE 是 ARM v8.5 引入的一项特性，通过内存标签追踪常见的非法内存操作。通过应用内存标签，系统可以检测到并隔离非法的内存访问，为系统的安全性提供了更高的保障。

需要注意的是，内核完整性保护和 MTE 这两项技术受限于硬件，仅在特定平台、版本设备上提供。它们是 ColorOS 为提供更安全的系统而采取的措施之一。ColorOS 将继续努力改进和优化，以确保用户享受到更安全可靠的使用体验。

3.5 系统软件更新

ColorOS 定期发布系统安全补丁，并提供 Android 原生的 OTA（Over the Air，空中下载）机制，方便用户及时修复可能存在的漏洞。当用户通过 OTA 升级时，系统首先检验升级包的签名，只有校验通过的升级包才被允许安装。ColorOS 提供用户可知可控的系统软件更新管理机制，防止系统软件降级到存在漏洞的低版本，给设备造成风险。

4 通信与网络安全

ColorOS 采用业内标准网络协议并提供数据加密传输。提供 Wi-Fi 安全检测功能保障用户网络接入安全。提供防伪基站安全功能，减少不良来电和诈骗短信。

4.1 TLS

TLS（Transport Layer Security，传输层安全协议）通过在传输层对网络连接进行加密和认证，为网络通信提供机密性和完整性的一种安全协议。

ColorOS 支持更安全的 TLSv1.2、TLSv1.3。

4.2 VPN

VPN（Virtual Private Network，虚拟专用网）是在公网上使用隧道协议构建的点对点安全连接。用户可以通过 VPN 在共享或公共网络上实现安全的数据传输。

ColorOS 支持 PPTP、L2TP/IPSec PSK、L2TP/IPSec RSA、IPSec Xauth PSK、IPSec Xauth RSA、IPSec Hybrid RSA、IKEv2/IPSec MSCHAPv2、IKEv2/IPSec PSK、IKEv2/IPSec RSA 等协议类型。同时 ColorOS 支持 PPP 加密（MPPE）。

*注：Android S 及以后的版本出于安全考虑，只能新建 IKEv2/IPSec MSCHAPv2、IKEv2/IPSec PSK、IKEv2/IPSec RSA 这三种类型。

4.3 WLAN

ColorOS 提供 WEP、WPA/WPA2-Personal、802.1x EAP、WAPI PSK、WAPI CERT、WPA3 OWE、WPA3-Personal 等多种 WLAN 认证方式，满足用户不同安全级别的需求，有效提高无线网络通信的安全。

为防止监听器根据设备真实 MAC 地址生成设备活动的历史记录，ColorOS 提供随机分配 MAC 地址扫描并连接 WLAN 网络的能力，从而加强对用户隐私的保护。用户可因个人需要手动设置选择使用真实设备 MAC 地址。

同时 ColorOS 设备的 WLAN 个人热点功能默认关闭，一旦被用户开启，默认使用 WPA2 PSK 认证方式，保证连接安全。

4.4 防伪基站

近年通过伪基站进行诈骗手机用户钱财的案件呈增长势头，不法分子利用伪基站干扰屏蔽运营商信号，使用户手机连接上伪基站信号，继而冒充他人手机号码、特服号码等任意电信网号码向用户发起垃圾短信、钓鱼诈骗、中间人劫持等攻击。

为了避免用户接入伪基站遭受损失，我们针对性的研发出一套基于自研 modem 算法的伪基站防御方案，提供伪基站的拒绝服务攻击防御、降级攻击防御、超时攻击防御及 GSM 伪基站防御等能力，实时启动芯片级识别防御算法自动分析系统广播参数和伪基站行为特征，对伪基站进行识别和防御。

*注：上述功能仅适用于中国（港澳台地区除外）的运营商。

5 应用安全

ColorOS 通过智能护盾、应用威胁检测、应用签名校验机制、应用沙箱机制和运行内存保护机制，保证应用从安装到运行所涉及各个阶段的安全。

5.1 智能护盾

智能护盾是 OPPO 自研的应用全生命周期的安全隐私防护系统，全方位识别并拦截应用在上架、下载、安装、启动、运行、升级、卸载等各阶段的风险，为 ColorOS 提供应用安全的云端服务能力。

智能护盾通过对应用进行多维度检测和多模型交叉识别，精准识别应用包含病毒、恶意广告、安全漏洞、隐私合规等安全问题。结合 ColorOS，在应用威胁检测、应用安全管控、智能权限建议、支付保护中心等功能保障用户手机的应用安全。

5.2 应用威胁检测

ColorOS 提供的手机软件商店是官方的应用和游戏的下载及管理平台，提供安全的内容和丰富的各类应用。软件商店严格把控上线应用的安全，在应用上架前必须全部通过开发者资质审核、App 资质审核、自动化安全查杀、人工审核 4 个环节的检测程序。对于已上架的应用，实施 24 小时在线监控，并配合安全查杀工具自动回扫机制，定期人工复检，一旦检测到 App 存在病毒、木马等可能威胁用户安全的风险，则自动下架处理。ColorOS 提供的手机软件商店保证向用户提供安全可靠的应用，建议用户从官方手机软件商店下载应用。

ColorOS 系统默认禁止安装未经安全检测的、第三方未知来源（非官方软件商店）的应用，

以避免病毒木马等不必要的风险。ColorOS 允许用户手动开放未知来源应用的安装权限，并在第三方来源的应用安装时，对其进行安全性检查。同时，通过 USB 或其他途径保存到手机的 APK 应用安装包，ColorOS 也会对其进行安全性检查，以降低安全风险。

ColorOS 系统集成了多个知名安全厂商的病毒查杀引擎，提供本地及云端查杀能力，确保设备在有无联网的情况下都能发现应用的安全风险。病毒查杀引擎支持应用安装时检测和闲时体检，用户可在手机管家中手动触发设备病毒扫描功能，对恶意应用和恶意文件进行扫描。系统也提供后台自动体检功能，根据用户选择的自动体检频率（默认 1 天）触发后台体检任务。

5.3 应用签名

应用签名是一种校验机制，用以保证应用合法性和完整性，ColorOS 要求所有应用的安装/升级必须具有完整、有效的签名。

在程序安装时，ColorOS 对应用签名进行验证，以检查应用程序是否被篡改，验证不通过则不允许安装。

为了防止已安装应用被恶意应用通过升级的方式替换，ColorOS 要求新旧版本应用程序必须使用同一个证书进行签名，否则 ColorOS 认为是不同的程序，阻止应用升级。

5.4 应用沙箱

ColorOS 支持应用沙箱机制，利用基于用户的 Linux 保护机制来识别和隔离应用资源，将应用程序置于“沙箱”之内，实现应用程序之间的隔离，并设定允许或拒绝 API 的调用权限，限制应用程序对资源的访问，保护应用和系统免受恶意应用的攻击。

应用程序运行在它们自己的 Linux 进程上，在安装时被分配一个唯一的用户 ID 并永久保持，默认情况下对其他应用程序完全隔离。特殊情况下进程间可通过 Android 提供的共享 UID 机制建立相互信任关系，具备信任关系的应用程序可以运行在同一进程空间。

5.5 运行时保护

ColorOS 在继承 Android SELinux 和 Capability 权限管控外，启用了 CFI（Control-Flow Integrity）、PAN（Privileged Access Never）、PAX（Privileged Execute Never）等安全功能。如基于 Clang 的 CFI 将检查每次间接跳转的地址合法性，阻止非法和任意跳转，确保函数执行流始终处于预期范围，能有效缓解 ROP/JOP 等劫持函数流的攻击方式；如基于 ARMv8 的 PAN 和 PXN 安全防护技术，将禁止内核空间访问用户空间数据或执行用户空间代码，可有效阻止通过内核指针攻击用户空间。

ColorOS 在增强权限的隔离和细分的管控同时，还提高了对恶意行为的识别、防护能力，保障系统运行时的安全。

6 拦截检测

拦截检测是 ColorOS 针对应用安全、应用间跳转、电话骚扰、短信及浏览器中恶意网址威胁提供的安全功能，对用户电话、短信及浏览器应用的使用场景进行安全及隐私保护。

6.1 应用安全管控

ColorOS 提供针对应用安全管控的功能，该功能通过分析应用的恶意行为特征，并对恶意行为实施精准拦截，从而保护用户的安全隐私，提升用户体验。

用户可以在手机管家 > 应用安全管控 > 菜单 > 设置，开启风险行为拦截功能，并能够查看拦截记录和拦截详情，同时，针对被拦截的应用，可以选择卸载操作、开启隐私替身、禁用敏感权限或加入拦截白名单的例外处理。该功能能够及时反馈应用中的恶意行为，使用户直观感知风险并拦截安全隐患。

6.2 应用间跳转拦截

为了遏制部分应用恶意利用应用间相互拉起的能力，频繁向用户推送广告，或者彼此互相保活等损害用户体验的行为，ColorOS 通过 AI 智能算法分析，主动拦截应用 A 随意跳转至应用 B，并弹框询问用户是否允许打开。用户可点击弹框“取消”，拒绝应用 A 打开应用 B，此时系统将中断应用 A 的拉起行为。此外，用户也可勾选“以后总是允许”，并点击弹框“允许”，同意应用 A 直到卸载前都可以直接打开应用 B。

6.3 骚扰拦截

ColorOS 支持来电和信息骚扰拦截功能，骚扰拦截功能提供自定义拦截规则和拦截强度设置，并支持黑名单、白名单拦截机制，最大限度满足用户的拦截需求，减少骚扰来电和信息带给用户的困扰。

6.4 恶意网址检测

ColorOS 的浏览器和短信中的网址安全检测功能，可分辨潜在威胁，减少挂马网站、色情网站、暴力网站、诈骗网站等恶意网站给用户带来的影响。

使用 ColorOS 自带浏览器浏览网页时，系统将网址与内置网址信息库进行比对，若网址比对结果存在风险，浏览器会提醒用户该站点存在安全风险并建议停止访问。

ColorOS 的信息应用提供在线识别恶意网址的功能，能够及时反馈短信中网址链接的安全性，对网址的安全性进行标注，使用户能够直观感知，减少使用风险。

7 支付保障

ColorOS 致力于保障用户的支付安全。本章介绍了 ColorOS 在自有支付软件（NFC Pay）中对于安全所做的努力、以及为第三方支付 App 所做的安全性支持。NFC Pay 在用户、商家和发卡机构之间搭建了安全且私密的支付桥梁，支付过程并不会收集用户的任何交易信息。

7.1 手机支付（NFC Pay）

NFC Pay 是钱包提供的手机支付服务。用户在受支持的 ColorOS 终端设备通过 NFC Pay 绑定银行卡即可享受安全、便捷的支付体验。使用 NFC Pay，无需使用实体银行卡，可用于线上支付、线下 POS 机支付及地铁公交出行等应用场景。为保证支付安全，在硬件层面，终端设备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，发起支付时会自动检测支付环境是否安全可靠。

NFC Pay 组件

安全元件（Secure Element，SE）是经过工业标准认证的、运行在 Java Card 平台（Java Card Platform，JCP）、符合金融行业电子交易要求的安全元件。安全元件在带有近距离无线通信 NFC（Near Field Communication）模块的手机中存在。

NFC 控制器：NFC 控制器负责处理 NFC 协议，支持应用程序处理器和 SE 之间以及 SE 和 POS 系统（Point of Sale）之间传输信息。

NFC Pay 应用：在支持 NFC Pay 的设备上承载该服务的应用指“钱包”，用户可以在钱包中添加和管理银行卡，及查看添加的卡片和发卡机构提供的其他信息（如设备卡号、最近的交

易明细等）。

NFC Pay 服务器：NFC Pay 服务器负责管理 NFC Pay 中的银行卡的状态，以及储存在 SE 中的设备卡号，同时与设备以及支付网络中的服务器进行通信。

NFC Pay 如何使用 SE

手机 SE 中有专门管理 NFC Pay 的应用，或通过与支付网络或发卡机构认证的小程序，来实现与支付网络或银行卡发卡机构之间数据安全传输。加密后的银行卡数据安全存储在 SE 中。交易期间，POS 系统使用银联专用网络通过 NFC 控制器直接与 SE 进行通信。

NFC Pay 如何使用 NFC 控制器

作为 SE 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入。NFC 控制器只会将来自射频场内终端的支付请求标记为非接触式交易。当用户使用指纹或密码授权支付，NFC 控制器会将安全元件 SE 准备的非接触式响应专门发送给 NFC 射频场。交易的支付授权详细信息通过 SE 加密后直接发送给支付网络，不会透露给应用程序处理器。

添加银行卡

添加银行卡前，用户需要完成实名认证，并授权姓名、身份证号、手机号等信息给银联进行活体认证和人证比对，确认为本人后才能进行绑卡。用户在 NFC Pay 中可以通过两种方式添加银行卡：

方式一：手动输入银行卡号。用户需输入银行卡号，仅当银行卡在支持的银行列表并校验

通过后，继续进行活体认证和人证比对，确认为本人。验证通过后，通过银联服务进一步校验手机号、储蓄卡取款密码或信用卡有效期、CVV 码等信息，在所有要素信息均校验通过后进行绑卡。用户可以在钱包中手动输入或使用摄像头来识别填充银行卡号信息。银行卡号信息输入完成后，钱包会将卡号发送到 NFC Pay 服务器再透传到发卡机构进行验证。验证通过后，手机钱包将向用户返回银行协议，仅当用户同意后才能继续进行添加流程。

方式二：免输入银行卡号添加。用户先授权实名信息给银联进行活体认证和人证比对，验证通过后钱包会将信息加密从银联获取用户的银行卡号信息让用户选择绑定。

用户后续填写的银行卡相关其他信息，将通过“银联可信安全服务控件”加密后发送到 NFC Pay 服务器，并再次由 NFC Pay 服务器透传给发卡机构。同时，OPPO 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 NFC Pay。

支付授权

SE 仅在接收到来自手机的授权，确认用户已使用指纹或支付密码认证后，才会允许进行支付。如果开启了指纹支付，指纹即为默认的支付方式，指纹验证有效性只限当次交易，若用户失败次数超过系统指纹连续识别上限，将暂停指纹验证对该卡的操作，提示用户使用支付密码进行支付。

暂停使用或移除银行卡

用户可以登录钱包，手动移除已添加的银行卡。也可退出欢太账号从而锁定银行卡，将其设置为不可用状态。针对已添加的“NFC Pay 银行卡”，即使设备未接入网络，发卡机构或支付

网络也可停用其支付功能，用户可通过致电发卡机构来暂停使用或移除该银行卡。

*注：上述功能中提到的 NFC Pay 包含 ColorOS 终端设备的手机支付，OPPO Pay、OnePlus Pay、realme Pay 功能。

7.2 支付保护中心

ColorOS 支付保护中心为支付应用提供安全的支付环境隔离空间，并对支付环境进行全面检测，确保支付环境安全。启用支付保护中心后，系统会在支付类 App 前台运行时检查运行环境，一旦发现安全隐患，立即进行风险展示并对用户进行修复提醒，最大限度保护用户的财产安全以及相关数据安全。

支付环境隔离：

- 应用隔离：屏蔽相关接口，防止恶意应用感知到支付类应用。
- 支付环境隔离：如果支付应用在后台运行超过 1 分钟，则结束进程。

运行环境检测：

- 系统安全环境检测：检测设备是否 Root、安全补丁是否安装、默认短信应用是否为受信任的应用、是否允许 USB 传输数据。
- WLAN 安全检测：如果连接 WLAN 且开启定位服务，则检测 WLAN 是否加密、是否为虚假 WLAN。
- 应用安全检测：查看病毒扫描的结果。病毒扫描发生在用户手动触发及应用安装等时机。

7.3 短信验证保护

短信验证码已经成为可信操作的重要验证因子，一旦泄露可能导致用户遭受严重财产损失及重要信息被泄露。很多第三方应用在安装时申请短信读取权限，用户授权后，很少关注或调整对应权限，导致第三方应用可随时读取短信中的重要或敏感信息。

ColorOS 提供验证码保护功能，以有效降低验证码泄露的风险。当 ColorOS 接收到短信时，短信应用会对该短信进行智能解析。如果判断为验证码，将禁止除了支付应用之外的所有第三方应用读取。避免由于短信读取权限误授权给恶意应用，导致验证码泄露的风险。

7.4 生物特征支付

ColorOS 支持指纹支付和人脸支付，用户的指纹和人脸信息保存在终端设备的安全区域中，不会传输到云端。ColorOS 对用户的支付信息采取高强度保护措施，以保证用户支付信息的安全。

8 设备管理

为应对用户丢失手机和儿童沉迷手机等场景，ColorOS 提供查找设备、儿童空间等设备管理功能。

8.1 查找设备

考虑到用户丢失设备时需查找设备及防止隐私数据泄露，ColorOS 提供定位设备、锁定设备、激活锁、抹除数据等功能。设备联网的前提下，开启“查找”功能后，当前设备会与已登录的欢太账号形成绑定关系。如果设备丢失，用户可登录云服务网页 cloud.heytap.com，或者使用其他 ColorOS 的设备使用查找设备功能对丢失的设备进行定位、播放声音、锁定手机和抹除数据等操作。此外，用户在绑定邮箱地址和紧急联系人后，在登录“查找”时需要进行额外身份验证，以避免他人盗取欢太账号后恶意定位和控制设备。

ColorOS 提供了设备激活锁功能，用于激活设备，此功能在启用“查找”功能后会同步开启。若设备被强制清除数据，手机重启后，在开机向导中会进入“激活设备”界面，需要验证原欢太账号密码或者设备原锁屏密码，重新认证机主身份后方可使用。激活设备时，设备需要连接有效网络（插入能正常上网的 SIM 卡或连接有效 WLAN）。

当设备丢失且连不上网时，仍然可以通过查找网络追踪位置。遍布世界各地的欢太设备会组成一个查找网络，当网络中的欢太产品发现离线设备出现在附近时，会安全地将其所在位置传给云端，然后就能在控制端看到自己设备的位置了。整个过程完全匿名并经过加密，以充分保护每个人的隐私。

*注：上述功能仅适用于在中国（港澳台地区除外）销售的设备。对于在其他国家地区以及中国港澳台地区销售的设备，您可参见由 Google 提供的“查找我的设备（Find My Device）”功能。

8.2 儿童空间

为防止儿童沉迷手机或误操作致话费损失等，ColorOS 提供“儿童空间”功能。机主用户可设置“儿童空间”内的移动网络、可用应用、使用时间等。启动“儿童空间”后，他人将只能在机主用户指定时长内使用用户指定的应用。机主用户可选择关闭或开启儿童空间中的移动网络。

9 密码与数据保护

本章节介绍 ColorOS 的数据安全防护机制。ColorOS 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，普通应用无权限访问；对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。同时，针对用户分区，ColorOS 提供包括独立安全芯片、安全存储、信任空间、文件系统加密（FBE）、数据擦除、密钥管理及使用、锁屏密码保护、指纹&面部密码、隐私密码、安全键盘、密码本等数据保护功能和措施，从硬件、系统、应用提供整体的数据保护机制。

9.1 独立安全芯片

ColorOS 部分产品在主芯片外集成了独立安全芯片，该芯片拥有独立的处理器、内存、持久化存储、硬件加解密引擎等硬件资源，以及独立的操作系统软件，符合 CC EAL5+级安全认证标准。同时该芯片还支持了国密算法功能，并通过了国密二级认证，是业界首次在手机产品上应用的国密二级认证安全芯片。

主芯片只能通过 TEE 可信执行环境访问独立安全芯片。TEE 与独立安全芯片之间使用 SCP 协议安全通信，通信密钥在设备生产安全环境中预置。

基于独立安全芯片，ColorOS 在设备查找（手机锁定状态）、生物特征数据保护、VIP 模式、私密保险箱等场景下，进一步增强用户隐私和敏感数据保护。

*注：独立安全芯片及上述功能，仅在部分型号产品上提供。

9.2 安全存储

ColorOS 基于 TEE 提供安全存储能力，将数据加密存储在安全存储器中，并对数据访问进行严格管控，防止数据被非法访问。ColorOS 提供以下安全存储实现机制：

（1）安全文件系统（Secure File System，SFS）

TEE 中运行的可信应用（Trusted Application, TA）通过 SFS 接口加密并存储密钥、证书、指纹模板等敏感信息，加密密钥由设备唯一密钥（HUK）和可信应用、ID 等信息在 TEE 下进行派生，并始终存储在设备 TEE 内，经过加密的数据只有 TA 可以访问。

（2）重放保护内存块（Replay Protected Memory Block，RPMB）

RPMB 是 eMMC/UFS 中具有安全特性的分区，通过提供防重放和认证保护，防止存储在 RPMB 中的密钥、证书等敏感信息被恶意篡改、删除。RPMB 提供比 SFS 更高的安全性。

数据进行加密存储，加密密钥由设备唯一密钥（HUK）等信息在 TEE 下进行派生。使用 RPMB 前需要在安全环境下进行 key provision，将 Authentication Key 预置到 eMMC/UFS 中，这把 Authentication Key 参与 MAC（消息认证码）计算。写数据时 Counter 参与 MAC 计算，用于防重放攻击，读数据时 Nonce（随机数）参与 MAC 计算，用于数据认证。

（3）一次性可编程存储器（One Time Programmable, OTP）

OTP 是一块特殊的存储区域，该区域基于熔丝位烧断的硬件原理，可以被多次读取，但仅可被烧写一次，用于存储设备唯一密钥（HUK），安全启动信任链根公钥 hash 等敏感信息。OTP 仅允许在 TEE 中访问，没有对外提供导出接口。

（4）安全元件（Secure Element，SE）

ColorOS 安全元件是防物理攻击的电子元件，用于密钥和数字证书等敏感信息的存储和密码运算。TEE 提供 SE 访问的基础服务，仅对可信应用提供调用接口。

9.3 信任空间

安第斯信任空间，是 OPPO 自研的端云协同可信安全平台，为 OPPO 生态统一提供账号、设备、数据的鉴权与认证安全核心服务，验证设备环境、账号状态等敏感数据的安全性，用以简化用户操作，提升体验。

安第斯信任空间包含账号安全能力（如 OPPO 身份密钥、远程锁屏密码验证）、设备安全验证能力（如可信设备服务）、数据安全加密能力（如端到端加密）三部分。

（1）OPPO 身份密钥

ColorOS 用户统一身份密钥服务（OPPO 身份密钥），通过基于生物特征（人脸、指纹等）进行账号的创建和登录、验证，在不增加用户学习和使用成本的同时解决用户众多密码无法记住以及容易泄露的问题，实现用户更安全、便捷的无密通行体验。

身份密钥使用非对称密钥加密技术，私钥存储在终端设备的 TEE 或安全芯片中，公钥不涉及机密信息存储在服务器端。用户登录时，只需用生物特征授权（指纹/人脸），由浏览器或 App 使用已注册的身份密钥完成登录。

身份密钥通过密码本云同步实现在设备之间的同步，并采用端到端技术，以支持用户账号跨设备安全使用身份密钥。

（2）远程锁屏密码验证

信任设备锁屏密码作为用户身份认证因子，为 OPPO 账号和用户数据云同步提供安全验证和便捷体验，其主要应用在陌生设备登录账号、找回密码、登录态下敏感操作以及端到端加密云同步用户数据等场景。

（3）可信设备服务

基于安第斯信任空间的可信设备服务，能够为开发者提供设备风险评估结果，unlock（设备解锁）、root（设备被 root）、emulator（模拟器）、attack（其他风险，比如多开、被调试、云真机等），协助开发者判断设备环境是否安全，用于账号安全保护、支付安全性检测等场景。

（4）端到端加密

端到端加密技术提供当前最高级别的数据安全性，保护用户数据安全的密钥是在用户信任的设备上通过只有用户自己知道的密码派生而来。只可在用户信任的设备上才能解密自己的数据，任何其他人（包括 OPPO）都无法解密这些数据。

9.4 文件系统加密（FBE）

ColorOS 支持 Android 的文件级加密（File-Based Encryption，FBE）功能特性。FBE 可使用不同密钥对不同文件进行加密，并且可以对文件进行单独解密。在启用了 FBE 的设备上，设备有两类可供应用使用的存储位置：

- 凭据加密（CE）存储空间：默认存储位置，只在用户解锁设备后才可用；

- 设备加密（DE）存储空间：在直接启动模式期间以及用户解锁设备后均可用。

ColorOS 使用凭据加密（CE）存储空间作为默认存储位置，保证应用和数据在用户认证通过后才能使用；同时将闹钟、铃声、短信、无线等应用数据保存在设备加密（DE）存储空间，这些应用能够在设备通电但用户尚未解锁设备时访问数据，利用系统能力保护用户个人信息和隐私安全。

9.5 数据擦除

当 ColorOS 用户使用“彻底清除全部数据”操作时，数据擦除功能不仅可以删除用户数据的逻辑地址，还会对存储空间进行安全彻底的格式化操作，彻底删除数据，以保障用户数据安全。

用户可以在 设置>系统设置>还原手机>彻底清除全部数据中彻底删除所有用户数据，包括应用数据（/data/data、/data/user 下的数据）、用户数据图片（/sdcard/下的数据）等。

9.6 密钥管理及使用

ColorOS 支持 Keystore 特性对应用所使用的密钥和证书的全生命周期进行管理，密钥管理具有如下功能：

（1）密钥生成和存储

支持硬件加解密引擎，TEE 根据应用指定的密钥生成算法，生成对称密钥和非对称密钥，生成的密钥由 TEE 维护，由加密密钥进行加密后安全存储。

（2）密钥导入和导出

业务密钥和其他需要外部生成的密钥通过安全的方式导入到 TEE 的安全存储区域，并用密钥加密密钥进行保护；根据业务需求，可以导出非对称密钥公钥，完成对此私钥签名数据的验证功能。

（3）加解密服务

加解密服务提供密码算法接口，可信应用通过该服务接口执行密码运算，密码运算在 TEE 中运行。

（4）密钥销毁

可信应用运行时产生的密钥数据，在生命周期结束后进行销毁。

（5）密钥认证

ColorOS 产品生产时在设备中注入了由 Google 公司颁发的证书，目的是确保设备是可信的，生成的密钥都可以使用 Google 的证书进行校验。在线认证时，密钥认证功能可以对 ColorOS 设备进行认证。

除了提供对应用所使用的密钥和证书的全生命周期管理功能外，Keystore 还增加了密钥提取防范和身份验证等安全功能，避免在 Android 设备之外以未经授权的方式使用密钥。

（1）密钥提取防范

为防止攻击者在 ColorOS 设备之外提取密钥，ColorOS 通过 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，ColorOS 将密钥

绑定至 ColorOS 设备的 TEE 的安全硬件中，使密钥永远不会暴露于安全硬件之外。即使 ColorOS 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

为避免在 ColorOS 设备上以未经授权的方式使用密钥，在生成或导入密钥时，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 Keystore 强制执行授权。

ColorOS 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。

9.7 锁屏密码保护

ColorOS 支持三种锁屏密码：绘制图案、数字密码和字母数字混合密码。

锁屏密码通过设备唯一密钥 HUK 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。针对手机锁定的情况，ColorOS 设计了多种安全策略，防止锁屏密码被暴力破解，从而保障用户的个人信息和隐私安全。

设置锁屏密码的方法是通过设置>指纹、面部与密码>锁屏密码。

9.8 指纹&面部密码

ColorOS 设备的指纹识别功能，要求用户的指纹采集、注册、识别和认证都在设备端的 TEE 内部进行，保证指纹数据安全，其中对指纹图像的处理过程（预处理，特征提取，录入及认证）均在 TEE 内完成，指纹相关数据不会被传出 TEE 区域外。外部的应用无法获取指纹数据，仅能通过框架的接口进行认证和获取认证结果。如下图所示用户可以注册一个或多个指纹，并使用这些指纹来解锁设备以及执行其他任务。ColorOS 会利用 Fingerprint HIDL（硬件接口定义语言）连接到供应商专用库和指纹硬件（例如指纹传感器）。FingerprintService 会通过 Fingerprint HAL 调用专用库，以便注册指纹以及执行其他操作，TEE 中 Keystore API 和 Keymaster/Keymint 组件提供由硬件支持的加密功能，以便在 TEE 中安全地存储密钥。

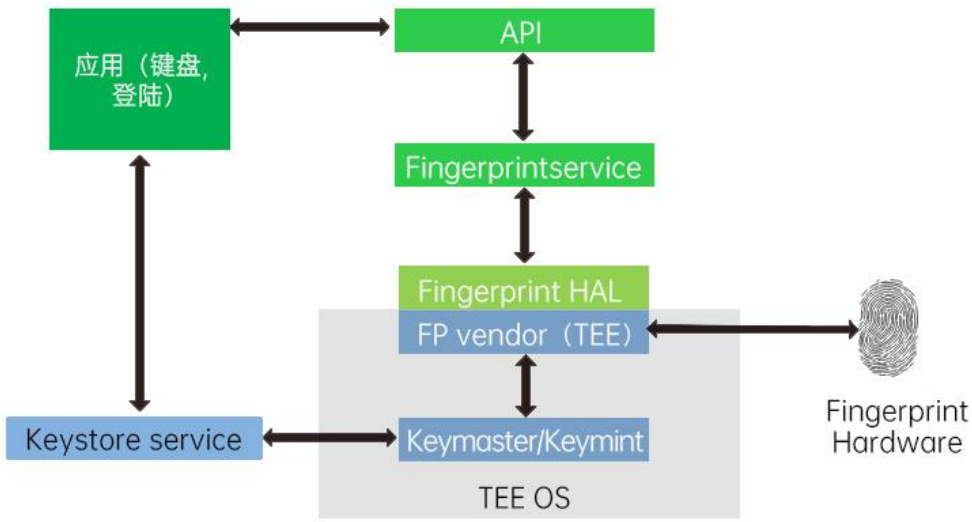

图 9-8 指纹安全原理

ColorOS 提供人脸识别功能。人脸识别技术可支持原生支付应用，不同的终端设备型号根

据其产品定位选择器搭载的人脸识别类型。

ColorOS 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，特征提取、活体检测、特征比对等处理也在 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，不接触人脸原始数据。

人脸模板录入时，为了保证录入模板的质量，录入时会对用户的录入距离以及录入角度进行限制，同时，出于解锁安全性的考虑，ColorOS 提供了解锁时眼神注视功能，增强用户解锁安全性。人脸特征数据通过 TEE 进行安全存储，通过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，确保用户的人脸特征数据不被泄露。

ColorOS 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后必须输入密码解锁设备。

9.9 隐私密码

隐私密码用于 ColorOS 中应用锁、应用隐藏、私密保险箱等入口的密码校验。密码存储与安全模块，系统级应用均无法获取。隐私密码可设置数字密码、混合密码、图案密码三种类型。

用户可以为隐私相关功能及空间单独设置隐私密码，确保隐私信息得以安全存储，并被独立保护，保障用户的个人信息和隐私安全。

9.10 安全键盘

安全键盘旨在对用户的密码输入形成保护，避免用户的密码信息泄露。启用安全键盘功能

后，当系统检测到输入内容为密码类型时，会自动调起 ColorOS 终端设备的安全键盘（银行、支付类应用优先使用应用自有键盘），系统在安全键盘被调起时禁止任何应用（包括系统应用和第三方应用）进行截屏和录屏操作。安全键盘无任何联想及记忆功能，没有联网权限，不会处理用户的密码数据。

9.11 密码本

ColorOS 提供密码本功能，旨在提升用户对当前设备众多应用的账号、密码维护效率，降低账号或密码被遗忘风险。功能开启后，当用户首次在 App 中输入账号密码时，密码本对用户的账号、密码进行集中保存。同时密码本可以进行指纹识别和锁屏密码关联，在用户登录应用时自动填充登录信息，方便用户进行账号、密码管理。

存储在密码本中的用户密码使用 AES256 位加密算法进行加密，密钥保存在 TEE 或独立安全芯片*中，保障用户的个人信息和隐私安全。

开启云同步功能后，存储在密码本中的用户密码密文将实时同步到云端，以帮助用户实现登录同一账号的多台设备间的账号、密码数据多端协同。

*注：独立安全芯片仅在部分型号产品上提供。

10 权限与隐私保护

本章节主要阐述对用户的隐私保护机制。ColorOS 终端设备中会处理用户的个人信息，如：联系人、短信、音视频资料等。为了保护用户的隐私，ColorOS 的预置应用满足国家法律法规和行业主管部门对个人信息隐私合规的要求，同时提供对照片隐私水印、照片隐私抹除、自动打码、VIP 模式、权限管理、应用行为记录、敏感权限提醒、应用锁及应用隐藏、剪贴板管理、私密保险箱、系统分身、隐私替身、隐藏摄像头检测等隐私保护技术和功能。

10.1 照片隐私水印

手机中经常存储了常用的证件照，ColorOS 12.1 及以后版本的相册提供了随身卡包自动归集证件照。

保护自己的证件不被盗用是用户强烈的需求，在没有互联网证件提交的年代，纸质证件同样存在手写使用用途的方式，防止被受理方二次使用。

为了能够保护拍摄的证件/卡类图片不被滥用，增加图片水印被视为较好的保护形式。添加水印在法律上是有效的，有水印的证件被利用到范围之外，证件所有者可以免责。

基于此背景，在相册提供对证件照类型的图片增加隐私水印的功能。当用户在相册中通过大图浏览图片，当浏览到证件和卡类图片或者在“随身卡包”图集中浏览图片时，实时的出现添加水印的入口和提示。用户可通过点击“添加隐私水印”按钮，进入添加隐私水印的页面，对图片添加水印，以达到避免图片滥用风险。在提供快捷添加水印方式的同时，在相册编辑内的水印功能中，可以为任意图片添加隐私水印。

10.2 照片隐私抹除

用户在使用相机 App 的打开地理位置等功能，通过手机拍摄的照片往往都会附带位置信息、拍摄数据（例如包含照片名称、时间、拍摄的型号、参数）等个人信息，这样当用户将原照片进行分享出去时可能会导致个人隐私的数据泄露。ColorOS 在相册分享照片或视频时，默认抹除照片位置信息和照片拍摄数据，从而保护用户个人信息及隐私私密数据安全。

10.3 自动打码

自动打码功能（仅在部分型号产品上支持）为用户提供自动打码头像、昵称、数字、敏感信息等隐私信息的功能，从而避免用户的隐私信息泄露。该功能目前主要面向聊天截图（微信、QQ、钉钉、WhatsApp、Messager），分享类（App 国内（微信朋友圈、QQ 空间）、海外（Ins、Facebook））的分享页面截图，票据照片（火车票（中）、登机牌（全）），汽车照片，证件照片等类型，对昵称、头像、敏感信息等执行自动打码，对文字区域实现用户点击一键手动打码。

用户在截图或者相册中，选择要分享的图片，点击编辑>马赛克，可实现对头像、昵称、群名称、数字、敏感信息等的自动打码操作。该功能为用户提供便捷的打码操作，从而有效避免了用户个人隐私的泄露。

10.4 VIP 模式

VIP 模式技术上通过全局禁用摄像头、麦克风、定位功能，能很好的支撑用户在特定场景下的隐私诉求。与友商相比，OPPO 使用硬件三段式开关进行切换，有便捷性优势。开启 VIP 模式后，OPPO 针对权限受阻时应用可能出现的功能异常为用户进行智能提示，避免三方兼容

性问题。此外 OPPO 还结合安全芯片对系统安全进行增强，具有更高的安全性。

10.5 权限管理

Android 的权限管理要求应用程序运行时访问敏感接口需提示所需的权限，并经过用户同意授权才能访问权限保护的用户数据，以限制应用程序对敏感的接口和资源的访问。

ColorOS 继承了 Android 的权限管理机制并进行扩展增强，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。用户可以在设置 > 权限与隐私 > 权限管理菜单查看已安装的 App 申请的权限集或者某项权限被申请的 App 清单，管理某个应用拥有的所有权限，可以对权限进行单独允许或禁止，也可以管理某项权限允许哪些应用拥有或关闭。

在 Android 原生系统基础上，ColorOS 对权限管理进行进一步的管理：

使用时允许功能：位置信息、相机、麦克风等权限支持“使用时允许”授权，避免应用获得权限后，在用户未使用相关功能应用期间，窃取用户个人信息及其他隐私数据。选择“使用时权限”选项后，应用不能在后台访问相应权限。

仅本次使用时允许功能：位置信息、相机、麦克风权限支持“仅本次使用时允许”授权，当设置为该状态时应用仅可在当前进程中调用该权限，再次启动该应用时，应用需重新获得用户授权，即“每次使用时询问”。

后台禁用录屏截屏功能：当用户正在进行涉及隐私的操作时（如使用安全键盘、使用私密保险箱），截屏、录屏功能将暂时无法使用。

定位服务功能：为保护用户位置隐私信息的安全，ColorOS 提供 GPS、WLAN 和移动基

站的位置服务关闭功能。选择关闭位置服务后，将同时关闭 GPS / WLAN / 移动基站信息这的三种定位功能，不再获取彻底关闭用户的位置信息，保护用户的隐私安全。

用户可以在设置>权限与隐私>位置信息选项中开启或关闭定位服务位置信息，或者在下拉菜单状态栏中快捷管理定位服务功能位置信息。此外，用户可以查看最近请求位置信息的应用。

另外，在 Android S 及以后版本上，ColorOS 的位置功能提供模糊定位和精准定位 2 个选项，并且在应用申请定位权限时，弹框让用户自行选择，用户可以不提供自己精准的位置信息就可以正常使用应用，且用户可以自行控制定位信息的精确度，以保护自己的位置信息的安全，从而 ColorOS 可以有效保护用户的隐私安全。

智能权限建议功能：ColorOS 产品为用户提供智能化的权限建议功能，即当应用想要调取用户终端设备的相关权限时，可以指导用户合理授权，有效引导用户在不影响使用体验的基础上，更加合理地授权，避免过度授权导致的隐私泄露风险。

*注：此功能仅限在中国（港澳台地区除外）销售的手机。

10.6 应用行为记录

ColorOS 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。用户可以在设置 > 权限与隐私 > 权限页面查看已安装的 App 近期使用相关权限的记录。

针对手机上非系统应用最近 30 天的权限使用行为进行详细记录，包括应用名称、允许状态、调用时间。支持以全部记录、行为、应用三个维度查看，并可筛选已允许、已禁止、隐私替身的权限使用记录。基于权限使用记录功能，用户可以查询应用最近使用了哪些权限，增加

了应用行为对用户的透明性，保障用户隐私。

10.7 敏感权限提醒

ColorOS 会对敏感权限的使用进行提示。当非系统级应用在调用摄像头、麦克风、定位信息等权限时，状态栏右侧会立即出现对应权限的调用状态图标，对用户进行提示，增强用户感知。用户可以通过下拉状态栏，在通知中心点击敏感权限图标，查看正在使用敏感权限的所有应用信息。用户可在弹框中直接点击应用，快速跳转到权限管理页面，对该应用进行权限管理，也可通过“查看详情”选项跳转到权限使用记录页，获取更详细的权限使用情况。

10.8 应用锁&应用隐藏

为了防止用户将手机借出时，他人未经允许访问涉及隐私的应用，ColorOS 提供了应用锁机制。用户可以为应用软件设置访问密码、指纹、人脸验证保护，设置后用户必须通过验证才能访问被应用锁保护的应用，从而可以有效保护用户的隐私。

ColorOS 提供应用隐藏功能，用户可以通过此功能隐藏应用的桌面图标、消息通知、最近服务，从而实现部分应用不可见、不可被访问的效果保护应用。若用户需要访问被隐藏应用时，在拨号盘输入特定的访问号码即可。

10.9 剪贴板管理

ColorOS 剪贴板权限管理，针对应用尝试读取或修改剪贴板数据时提醒用户，并将读取剪贴板行为加入到权限使用记录中，使应用读取剪贴行为一目了然，另外，用户可以管理应用读取剪贴板行为，禁止应用读取剪贴板的内容，确保用户对应用访问或修改剪贴板的行为访问或

修改授权可知。

10.10 私密保险箱

ColorOS 私密保险箱提供基于用户密码加密的保护空间。用户可以将一些敏感或重要的个人文件（照片、音频、视频、文档等）添加到私密保险箱中进行加密保护。

用户可以通过设置隐私密码开启该功能，私密保险箱的隐私密码受芯片级安全保护（TEE或独立安全芯片*），从而能有效防止密码被窃取，并且会对添加到私密保险箱中的个人文件进行全文件级加密，进一步保护用户数据的安全。目前私密保险箱支持密码、指纹、人脸认证方式，只有通过验证的用户才能打开私密保险箱，三方应用和他人无法访问私密保险箱内的资料。当用户正在使用私密保险箱时，截屏、录屏功能将暂时无法使用，降低用户私密数据泄露的风险。

*注：独立安全芯片仅在部分型号产品上提供。

10.11 系统分身

为了满足用户隐私保护的高要求，我们提供工作生活双系统的系统分身功能，用户既可以提升工作效率，又能在工作结束后快速切换到生活状态。

系统分身基于多用户技术开发，用户可在主/子系统分别设置不同的密码或指纹，并通过特定的密码或指纹快速在双系统间切换，同时双系统间支持各个系统应用和数据隔离，系统间数据导入导出、通知共享，在主系统隐藏系统分身入口。系统分身实际是独立于主系统空间的一个私密空间，可直接克隆主系统应用，无需重复下载，可满足用户将工作/生活/娱乐应用隔离

使用，无痕隐藏私密数据，快速在双系统间切换的需求。

10.12 隐私替身

用户在使用不同应用时，会担忧自己的个人信息被超目的、超范围收集使用，针对某些应用必须获取权限才可使用的情况（如读取通话记录、联系人、账号信息、日程信息等），ColorOS 为用户应用提供隐私替身功能以保护用户的隐私信息。

如果用户针对某应用开启隐私替身后，即使该应用已经获得相应权限授权，当该应用读取“通话记录”、“联系人”、“信息”、“日程”等信息时，系统将自动提交空白信息，解决了部分应用不给权限不允许使用的问题，该功能在尽量不影响应用正常使用的同时，又能避免真实信息泄露，保障用户的部分个人信息不被应用获取。

隐私替身功能开启后，对应用的保护就会生效，此时用户将收到来自隐私替身的静默通知。若开启该功能的应用因无法读取真实用户信息数据而导致运行异常，用户可以点击通知中心的隐私替身通知或者从“设置>隐私>隐私替身”进入主页进行功能关闭切换。

*注：此功能需要依赖“通信应用（拨号盘、联系人）”，若无集成通信套件则无法提供此功能。

10.13 隐藏摄像头检测

用户在入住宾馆、酒店、出租屋等场所时，会担心这些场所私藏摄像装置，导致个人隐私泄露。不法分子通过这种方式获取用户个人隐私并获利的行为，不仅严重侵害了用户个人隐私，而且会造成不良的社会影响。基于此，ColorOS 产品为用户提供隐藏摄像头检测功能，应用尚未预置在手机出厂系统中，用户如有需要可以自行在应用商店下载使用，下载后无需连接局域

网，即可检测房间是否存在隐藏摄像头设备，并且协助用户找到可疑设备的位置。

*注：此功能仅限在中国（港澳台地区除外）销售的部分手机。

11 安全认证与隐私政策

ColorOS 终端安全持续构筑面向用户体验和关键场景的安全业务与能力，致力于为消费者提供更好的安全隐私体验。在安全隐私实践上，我们的产品和服务通过了国内、国际多项安全隐私领域的权威认证，持续提升 ColorOS 产品的可信赖品牌形象。

OPPO 终端安全在 ColorOS 研发生命周期，结合微软的 SDL 流程，建立海内外安全&隐私合规机制，提升安全与隐私工程能力成熟度，进一步保障 ColorOS 产品在研发阶段消除潜在的安全风险。OPPO 终端安全联合新思科技对自身软件安全工程能力进行评估，目前软件安全成熟度已达到行业较领先水平。

OPPO 手机（Find 系列）获得 CC MDFPP 认证，该证书获得 CCRC 组织的 31 个国家认可，MDFPP 是基于 CC 标准为移动设备定义的全面安全评估框架，通过该认证意味着 OPPO 终端产品得到全方位评估和验证。

OPPO 的手机获得移动智能终端安全五级认证（5 级最优），该认证依据通信行业标准 YD/T 2407-2021《移动智能终端安全能力技术要求》和 YD/T 2408-2021《移动智能终端安全能力测试方法》实施，荣获五级认证，意味着 ColorOS 12.1 及以上版本可为用户提供该标准最高等级的安全和隐私保障。

OPPO 隐私管理体系、重点产品及服务的实践通过美国隐私认证机构 TrustArc 的审核与认证；OPPO 数据隐私合规通过欧洲权威隐私认证机构 ePrivacy 的审核与认证。

安全与隐私相关认证证书获取情况请访问如下网址查询：

https://privacy.oppo.com

我们致力于保护和尊重用户的隐私，并通过个人信息保护政策向用户详细说明 ColorOS 处理（收集、存储、使用、加工、传输、公开、删除等）产品收集和使用用户个人信息的目的、方式和范围，用户拥有管理个人信息的权利和实现方式，以及向用户阐述我们为保护信息安全所采取的安全保护措施。由于每个国家/地区的个人信息保护政策会有所不同，请以每个国家/地区发布的 ColorOS 版本中对应的个人信息保护政策为准。

相关的个人信息保护政策请参考以下链接，并请选择对应的国家/地区：

https://privacy.oppo.com

*注：部分产品、应用有单独的个人信息保护政策，可在对应产品、应用页面查看。

12 漏洞奖励计划

我们非常重视自身产品和服务的安全性，致力于打造安全可靠的产品理念和保护用户的隐私。同时，我们意识到安全研究者们在保护 ColorOS 产品与消费者中发挥了重要作用，故发布 OSRC（OPPO Security Response Center）漏洞披露计划。漏洞披露计划为研究人员上报企业安全问题提供一个安全通道，并且包含一些用于分类和缓解这些安全漏洞的有效措施。我们对于遵守披露计划，未在解决漏洞的所需时间内提前将漏洞信息对外披露的研究人员表示衷心的感谢。为了保护我们的用户，在完成调查并全面推出任何必要的更新之前，OPPO 不会透露、讨论或确认安全性问题。

详细的奖励规则请参考：

https://security.oppo.com

13 术语表

英文缩写	英文全称	中文全称
AES	Advanced Encryption Standard	高级加密标准
API	Application Programming Interface	应用程序接口
APK	Android Application Package	应用程序包
ASLR	Address Space Layout Randomization	地址空间配置随机加载
AVB	Android Verified Boot	安卓启动验证
CE	Credential Encrypted	凭据加密
CFI	Control-Flow Integrity	控制流完整性
CVV	Card Verification Value	信用卡验证值
DE	Device Encrypted	设备加密
eMMC	Embedded Multi Media Card	嵌入式多媒体存储卡
FBE	File-Based Encryption	文件级加密
Fuse	Filesystem in Userspace	用户空间文件系统
GPS	Global Positioning System	全球定位系统
HIDL	HAL Interface Definition Language	硬件接口定义语言
HUK	Hardware Unique Key	硬件唯一密钥
IMEI	International Mobile Equipment Identity	国际移动设备识别码
IP	Internet Protocol	网际互连协议
IPSec	IP Security	IPSec 安全协议
JCP	Java Card Platform	Java Card 平台
JTAG	Joint Test Action Group	联合测试工作组
KASLR	Kernel Address Space Layout Randomization	内核地址空间布局随机化

L2TP	Layer Two Tunneling Protocol	第 2 层隧道协议
MAC	Message Authentication Code	消息认证码（带密钥的 Hash 函数）
MAC	Mandatory Access Control	强制访问控制
MPPE	Microsoft Point-to-Point Encryption	微软点对点加密术
MTE	Memory Tagging Extension	内存标记扩展
NFC	Near Field Communication	近距离无线通信
OTA	Over the Air	空中下载
OTP	One Time Programmable	一次性可编程存储器
PAN	Privileged Access Never	特权模式访问禁止
POS	Point of Sale	销售终端
PPP	Point to Point Protocol	点对点协议
PPTP	Point-to-Point Tunneling Protocol	点到点隧道协议
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	富执行环境
RPMB	Replay Protected Memory Block	重放保护内存块
RSA	Rivest Shamir Adleman	公开密钥密码体制
SE	Secure Element	安全元件
SELinux	Secure Enhanced Linux	安全增强性 Linux
SFS	Secure File System	安全文件系统
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境
TLS	Transport Layer Security	传输层安全协议
UID	User Identify	用户 ID
USB	Universal Serial Bus	通用串行总线

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