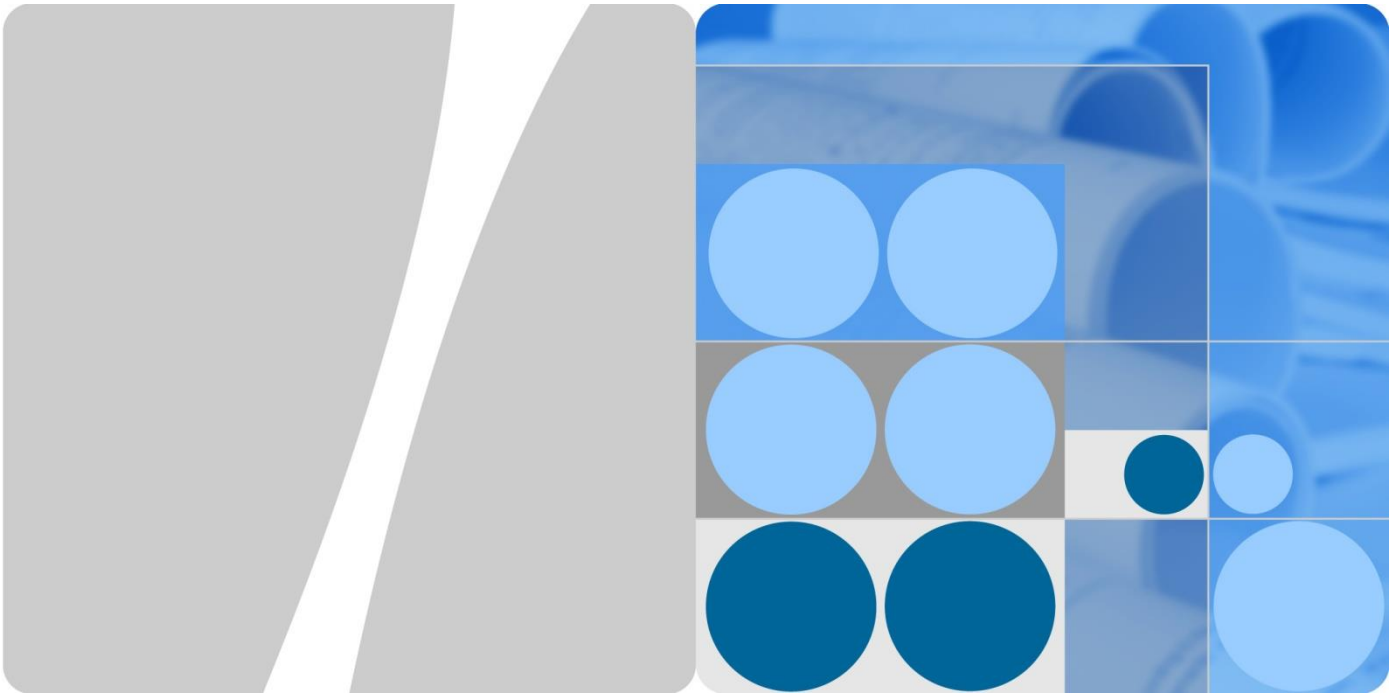
华为终端云服务（HMS）安全技术白皮书

文档版本 01

发布日期 2021-11-09



华为终端有限公司

华为终端云服务（HMS），安全，值得信赖

华为终端有限公司

地址：广东省东莞市松山湖园区新城路 2 号

网址：https://consumer.huawei.com/cn/

PSIRT 邮箱：PSIRT@huawei.com

客户服务传真：0769-23839866

目 录

1 简介

1.1 网络安全和隐私保护是华为的最高纲领

网络安全和隐私保护是华为公司的最高纲领，我们将公司对网络和业务安全性保障的责任置于公司的商业利益之上。结合消费者业务特点，我们提出消费者业务安全与隐私保护的“四大主张”和“三大承诺”。

从组织上，我们建立自上而下的组织治理架构，并将安全与隐私保护活动嵌入全业务流程；从产品设计之初，我们就制定了严苛的隐私安全原则，不符合原则和流程的业务不允许发布；我们与业界权威机构合作构建了独立的安全验证体系，以检验产品和服务的安全与隐私保护能力；我们还向生态伙伴开放了华为的安全与隐私保护能力，携手生态伙伴共建 1+8+N 全场景安全可信生态。

我们和生态伙伴所做的这一切，都是为了保护消费者的隐私安全。我们对消费者的隐私保护坚持三大承诺：第一，您的隐私安全是我们的最高优先级，我们坚持以创新科技，坚决捍卫您的隐私权；第二，未经您的允许，任何人都无法访问您的数据，你的数据唯你可见；第三，从开机到业务使用，每一步的数据和权限使用都需事先征得您的同意。

隐私安全是我们的首要关注，隐私保护的理念贯穿于产品设计、开发、运营和运维的全流程。我们始终遵循数据最小化、数据端侧处理、透明可控、身份保护和数据安全保障的隐私保护原则，通过多项创新的隐私保护技术的应用，构建了多重保障，守护您的数据安全。

- 数据最小化：坚持仅使用实现业务功能所必须的个人信息，以服务于您的需求
- 数据端侧处理：坚持尽可能在您的设备上完成个人信息的处理和分析
- 透明可控：当使用和分析个人信息时，清晰、明确地告知用户，并确保用户知道数据被如何使用，以及如何退出
- 身份保护：使用隐私增强技术，在数据离开您的设备时，隐藏您的身份
- 数据安全保障：坚实的数据安全是隐私保护的基础，我们围绕硬件、OS、应用及服务持续构建数据安全能力

我们在全球范围建立了独立的隐私安全团队，持续研究创新的隐私和安全技术，不断将最新的成果与 HMS 结合，同时监督并确保产品的严格遵从。我们从产品设计之初就开始构建隐私安全能力，并将其贯穿于整个产品研发、上市全流程。我们与客户保持良好的互动，积极听取他们在产品使用过程中对于隐私和安全的改进建议。

更多隐私安全信息，您可以访问 https://consumer.huawei.com/cn/privacy/

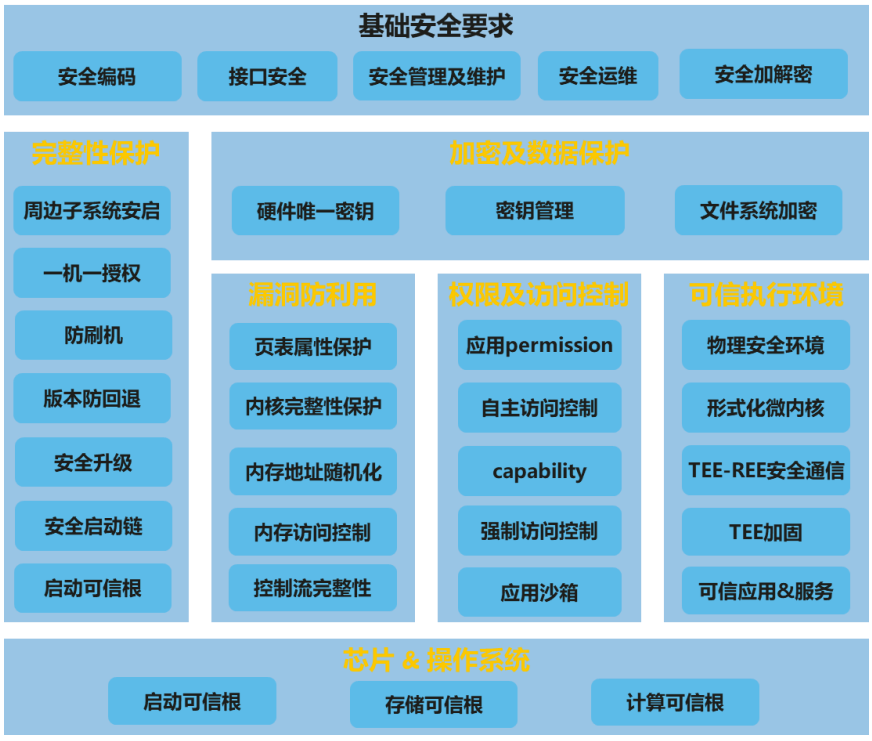
2 基于 HarmonyOS 的安全

HarmonyOS 是华为发布的新一代的智能终端操作系统，为不同设备的智能化、互联与协同提供了统一的语言。带来简捷，流畅，连续，安全可靠的全场景交互体验。

HarmonyOS 系统安全能力，根植于硬件实现的三个可信根：启动、存储、计算，以基础安全工程能力为依托，重点围绕设备完整性保护、数据机密性保护、漏洞攻防对抗构建相关的安全技术和能力。

HarmonyOS 系统安全架构如下图所示：

图2-1 HarmonyOS 系统安全架构

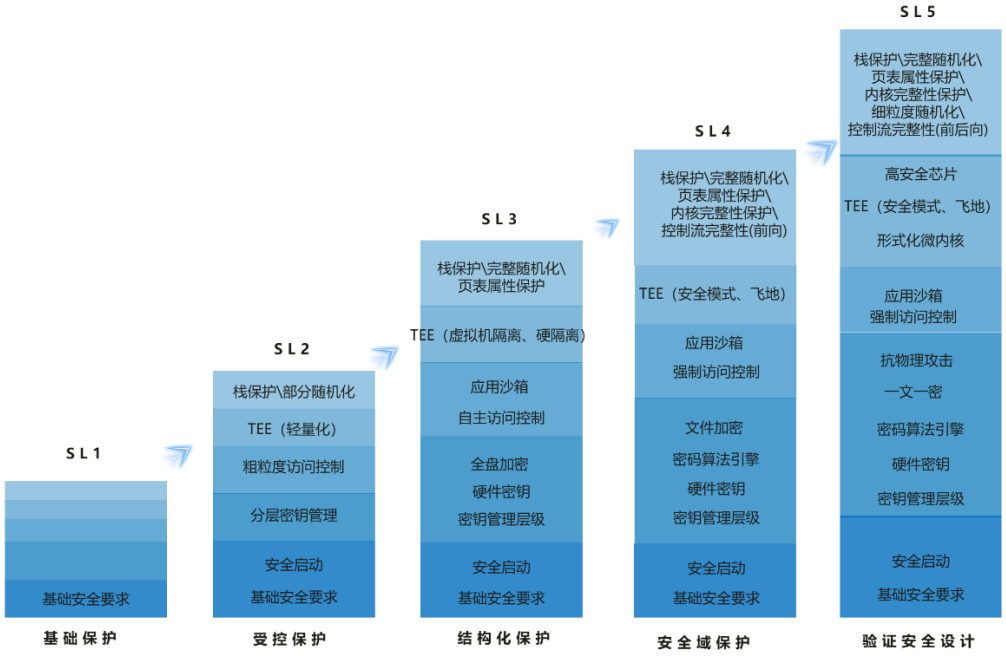


上图为典型的 HarmonyOS 单设备系统安全架构，在不同种类 HarmonyOS 设备上的实现会存在差异，取决于设备的威胁分析（风险高低）和设备的软硬件资源。

HarmonyOS 在参考业界权威的安全分级模型基础上，结合 HarmonyOS 实际的业务场景和设备分类，将 HarmonyOS 设备的安全能力划分为 5 个安全等级：SL1-SL5。HarmonyOS 操作系统生态体系中，要求高一级的设备安全能力，默认是包含低一级的设备安全能力。

分级概要可参考下图：

图2-2 HarmonyOS 设备安全分级



HarmonyOS 为消费者和开发者数据，提供了全生命周期的安全防护措施，确保在每一个阶段，数据都能获得与其个人信息敏感程度、系统数据重要程度和应用程序数据资产价值匹配的保护措施。基于分级安全模型的数据访问控制，在数据创建时严格指定数据的分级标签，并且基于标签关联上数据全生命周期的访问控制权限和策略。在数据存储时，基于不同的数据分级，采取不同的加密措施。在数据传输时，高敏感等级的数据，禁止向低安全能力的设备上传递；高敏感等级的资源和外设，禁止低安全能力的设备发出控制指令。

更多基于 HarmonyOS 的安全相关信息，请访问 HarmonyOS 安全技术白皮书：
https://consumer.huawei.com/cn/privacy/whitepaper/

3 安全业务访问

3.1 密码复杂度

华为帐号要求用户在设置密码时，使用长度至少为 8 个字符的强密码，包含大、小写字母和数字。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。另外，华为帐号通过限制密码尝试次数，防止暴力破解。

3.2 图形验证码

华为帐号通过集成 SafetyDetect 虚假用户能力检测到潜在的自动化攻击时，华为帐号将会弹出图形验证码，以阻断暴力破解。系统通过使用复杂度较高的图形，确保图形验证码无法被机器自动绕过。同时限制验证码的尝试次数，防止针对验证码的暴力破解。

3.3 帐号保护和多因子认证

通过帐号保护，华为帐号保障只有您的受信任设备才能登录您的帐号，首次登录新设备或用户开启了强制双重认证，则需要同时验证密码和第二因子。第二因子包括短信验证码、可信设备等。帐号保护显著增强了华为帐号以及华为终端云服务产品和服务的安全性。

安全验证码自动显示在您的受信任设备上。若验证通过，表示您信任此设备。如您已经有一部 HUAWEI Mate20，要在新购买的 HUAWEI Mate30 上首次登录您的帐号，HUAWEI Mate30 会提示您，输入密码和在 HUAWEI Mate20 上显示的安全验证码。

3.4 风险操作通知

用户在陌生环境登录、重置密码、修改帐号信息等风险操作时，华为帐号会通过短信、系统消息、IM 消息、邮件等方式通知用户，用户可根据提示进一步确认，防止帐号被盗用。

3.5 启发式安全认证

在找回密码和自助申诉的过程中，华为帐号提供了启发式的安全认证问题，协助您安全便捷的找回您的帐号；如果用户已实名认证，还支持通过活体检测和人脸认证找回帐号和密码。当帐号绑定的手机或者邮箱停用的时候，用户可以通过自助申诉更改帐号绑定的手机号或邮件地址。

3.6 儿童帐号

华为帐号支持您创建儿童帐号，为儿童提供更加安全和可靠的业务体验，创建和管理儿童帐号需要在相应家长帐号的授权下完成。家长可以通过儿童帐号帮助未成年人合理地使用设备和上网，呵护未成年人健康成长。HMS 将在各产品和服务中，为儿童提供附加的保护，包括在应用市场中，过滤不符合对应儿童年龄使用的内容，在支付活动中，限制儿童帐号的支付能力，在视频、阅读等业务中，过滤不符合儿童访问的内容等。

3.7 帐号反欺诈

华为终端在帐号登录、重置密码、修改帐号、申诉等环节设置了主动风险监测机制，主动识别风险，防范帐号盗用。

登录：针对钓鱼、木马、撞库等操作引起的帐号被盗问题，华为终端搭建了基于风险网络、设备环境、操作异常等多维识别策略与模型，快速精准地识别风险，防止黑产通过恶意手段盗号，导致用户信息泄露或资金受损，保障帐号安全。

重置密码：攻击者可能通过伪基站、短信木马等操作，恶意重置密码，占有用户的华为帐号，获取非法利益。而正常用户在忘记密码时需要便捷的重置密码，获取帐号使用权。针对这两种场景，风险控制平台结合操作信息、设备环境、网络环境等多重因素，区分正常用户和攻击行为，让正常用户方便快捷的找回密码的同时，防止攻击者占用华为帐号。

申诉：同重置密码环节相似，申诉环节也可以决定一个帐号的归属权。攻击者可以利用申诉环节占有用户的华为帐号，获取非法利益；正常用户也需要公共申诉便捷的获取帐号访问权。风险控制平台结合操作信息、设备环境、网络环境等多重因素，区分正常用户和攻击行为，加快正常用户的申诉进程，阻断攻击行为，在保障安全性的同时提升用户体验。

在抢购、秒杀、优惠券、礼包、抽奖等业务场景中，黑灰产试图通过各种渠道批量注册大量虚假用户参与活动并获取利益，华为帐号在注册时通过操作异常、手机号异常、邮箱异常、风险网络等多种手段识别风险，结合专家规则、机器学习识别虚假帐号，打击虚假注册，保护用户合法权益。

3.8 保护帐号的隐私

华为帐号在设备端不存储用户口令，用户名匿名化存储展示，不可还原。服务器存储用户的帐号个人信息时会根据用户 ID 进行隔离和加密存储，用 PBKDF2 算法保护用户

口令，不保存用户口令明文。华为帐号通过 HTTPS 通道传输数据，保证数据传输安全。

4 加密和数据保护

4.1 加密密钥管理和分发

HMS 为充分保护业务数据，在业务数据处理和交换过程中，使用端到端的加密方式。为更好的保护密钥，HMS 使用密钥管理服务（KMS），对密钥的申请、发放、使用、重置、回收进行统一的管理。

KMS 使用安全性达到业界领先水平的硬件加密机为生成密钥的根密钥服务，硬件加密机是经 FIPS level3 认证的具备物理防篡改能力的专用密码设备，向应用程序提供加密、数字签名、密钥安全管理等服务，并通过必须物理接触和多把物理钥匙，确保硬件加密机的根密钥安全。

KMS 采用多级密钥管理、分布式部署的方式，在保证密钥安全的同时满足业务对高性能的需求。KMS 采用国际标准或业界通用的安全算法(如 AES、RSA、SHA256 等)，严禁使用不安全算法（如 MD5、SHA1、DES 等）。另外，安全算法的密钥长度确保最低的安全强度（如 AES 禁止 128 位以下的密钥（不含 128），RSA 禁止 2048 位以下密钥），具体包含对称加密算法 AES-128/AES-256，非对称加密算法 RSA2048/RSA3072/RSA4096，ECC-p256/ECC-p384/ECC-p521。哈希算法 Sha-256/Sha-384/Sha-512。KMS 对于密钥、证书、授权认证的管理也有严格的流程。

- 在 HMS 业务中，针对需要加密保存的用户信息，如用户帐号注册信息，各业务向 KMS 申请密钥，KMS 向业务分发加密密钥后，HMS 业务使用密钥对要保存的信息进行加密，防止未授权人员读取。
- 对用户托管的用户数据，例如云空间中的文件，使用端侧加密处理和传输。通过 KMS 获取加密密钥，结合用户设备的加密因子，为每位用户提供独特的加密密钥，防止数据被未授权访问导致信息泄露。在音乐、主题、阅读等基于版权内容的服务中，当用户播放音乐，阅读书籍，下载主题时，将使用密钥保护内容的传递。当业务启动时，设备侧会产生与设备相关的一对公私钥对，不同设备的密钥对不相同。公钥将传递并保存在音乐服务器。当用户播放音乐时，服务端使用公钥，下发将用来加密该歌曲内容的对称密钥，并对传递给设备侧的内容，使用该对称密钥加密。设备侧接收到数据后，使用该设备唯一的密钥解密播放，不同设备的密钥不同，确保拥有合法版权的数据内容，不被未授权访问。
- 部分无独立认证界面的产品，如儿童手表，也使用受保护的认证密钥，进行手表与服务器的可信任通信。
- 针对需要保护的服务配置信息，例如服务间认证凭据，也使用加密密钥加密。

4.2 认证和数字签名

HMS 向消费者提供服务时，为了保护数据不被恶意攻击者篡改并提供可信的交互服务，使用证书链信任关键校验、数字签名校验的方式，确保数据在传递过程中，不被恶意攻击者劫持或通过改变业务数据进行攻击。

HMS 使用云证书管理服务（CCS）来签发证书，并在业务服务器对证书持有者的身份进行验证。使用安全性达到业界领先的根证书硬件加密机，云证书管理服务能够提供用户级证书、微服务身份证书、应用签名证书等数字证书的签发、更新和吊销能力。根 CA 私钥保存在硬件加密机中，证书签发活动也在硬件加密机中完成，确保签名信息不可被假冒。

- 为确保应用的安全性，HarmonyOS 安装器在安装应用过程中，将对应用进行校验。通过证书对经过华为应用市场审核的应用签名，HarmonyOS 可以对签名进行校验，避免未授权的应用篡改。
- 在快应用服务中，开发者上传快应用包到应用市场后，应用市场会对快应用包进行签名。用户下载快应用到设备侧后，在快应用引擎加载快应用包时，会针对签名进行验签，如果签名不符合，将拒绝运行，保障快应用在安装和部署过程中不被篡改。
- 在用户开通支付服务的过程中，手机端将自己的设备证书对应的私钥签名提交到云端进行校验，换取用于支付服务的支付证书。CCS 云证书服务将为每一个设备发放唯一的支付证书，并存储在手机 TEE 中，确保支付证书的机密性。为了保障用户支付的安全性和完整性，在用户支付时，需要使用硬件保护的支付数字证书私钥对关键支付数据进行签名（如支付金额），并且支付的签名运算在 TEE 中进行，服务端收到关键交互信息后，对关键支付数据进行验签，确保从手机端发出的支付数据，在全服务流程中，未被恶意篡改，保障了用户的数据和支付安全。
- 第三方卡券（Pass）供应商会在华为终端申请 Pass 证书，并使用 Pass 证书对卡券数据进行签名；用户在华为钱包中添加卡券（如超市会员卡/航空会员卡/健身卡等）时，签名后的卡券数据传到钱包服务器进行验签，以确保卡券在传递过程中未被篡改，保障卡券的安全性和完整性，验证通过后将卡券信息写在华为钱包中，方便用户日常使用。
- 在 DRM（Digital Rights Management）客户端初始化的过程中，将手机端的设备证书提交到云端进行校验换取 DRM 客户端证书。云证书服务 CCS 将为每一个设备发放唯一的 DRM 客户端证书。在手机端使用 DRM 保护音视频等数字内容的播放安全时，DRM 使用证书对内容密钥进行加密保护，确保只有授权的设备和应用才能获取到内容密钥，保护数字内容不被泄露。

4.3 可信身份认证和完整性保护

当用户在 Huawei Pay 中使用指纹支付时，首先在手机可信执行环境（TEE）中验证指纹；指纹验证通过后，同样在 TEE 中使用数字证书 RSA2048 算法对支付消息签名保护，保证支付完整性。

当用户在进行交通卡删卡退余额操作时，交通卡余额在 TEE 中使用 RSA2048 算法签名后，传到服务器处理，服务器验证签名后，下发退余额指令，防止余额及公交卡状态在传输到服务器的途中被篡改。

4.4 信任环 TCIS

用户在华为终端设备上首次登录华为帐号时，会自动生成一个用于构建信任环的密钥对（公钥和私钥），把公钥上传到 TCIS 服务器。当一个帐号同时登录多台设备时，会在 TCIS 服务器上生成一个属于该帐号的公钥列表。服务器对公钥列表进行完整性保护，这个公钥列表称为信任环。信任环会发送到每台设备上，并进行完整性验证。

用户开通云空间服务时，服务器为每个用户随机生成一个用户级密钥。文件上传到云空间时，设备为每个文件生成一个文件加密密钥，用来加密文件内容，防止文件内容在传输和存储时被窃取。文件加密密钥使用用户级密钥加密后上传并保存在服务器中，受到用户级密钥的保护。

当用户使用 Huawei Share 传输文件时，信任环上的密钥对会用于对设备进行身份认证，建立设备间的安全传输通道。设备通过身份认证后，会协商一个临时密钥用于文件的加密传输，实现数据的加密传输和完整性保护。

5 网络安全

5.1 安全传输通道

在网络中传输的所有数据，如移动设备端与服务器的连接，都采用安全传输通道来保证数据的安全，并对应用下载进行完整性校验，确保移动设备端和服务端的网络连接中信息不会被窃取和篡改。

用户在移动终端上使用的应用，采用国际标准或业界公认的安全协议，如 TLS v1.2、TLS v1.3，在客户端中预置商用 CA 根证书、云端网络设备部署商用 SSL 证书，客户端强校验云端 SSL 证书通过后，才能和云端服务器建立连接，确保网络请求通道的安全性。

5.2 云网络边界防护

边界防护是云上数据防护的入口，多种边界防护措施协同保护云上数据入口安全。所有对互联网开放端口的主机都经过防火墙过滤，设置开放服务必须使用的端口供互联网用户访问，对进出系统网络的数据包进行过滤，避免系统受到网络层攻击。

在业务面，除主要通过传统网络技术和防火墙实现的安全区域外，还包括了下述增强边界防护能力。

- DDoS 异常和超大流量清洗：在每个云数据中心边界部署专业的 Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清洗。
- 网络入侵检测与防御（IDS/IPS －Intrusion Detection System / Intrusion Prevention System）：为了应对来自互联网以及不同网络安全域之间的攻击，在网络边界包括安全域边界部署了 IDS/IPS 设备。IDS/IPS 具备网络实时流量分析和阻断能力，防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。
- 在管理面，在全部通过 VPN 和 HTTPS 安全通道的基础上，从登录认证、权限管理，接入控制等各环节，进行全流程的访问控制。
- 接入管理：网络对系统进行集中管理，需使用身份帐号，且要求使用双因子认证，如短信动态验证码、USB Key。帐号用于登录 VPN、堡垒机及跳板机，实现用户登录、操作的深度审计。

- 权限管理：根据不同业务维度和相同服务不同职责，实行 RBAC（基于角色的访问控制）权限管理，并遵从最小化授权原则，仅分配给用户必须的权限。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维护、检测维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。

5.3 安全细粒度 VPN 保护

为了最小化云上网络攻击的影响，结合业界网络安全区域的划分原则和优秀实践，对云上网络进行安全分区和业务隔离。根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提升网络面对入侵时的分区自我保护和容错恢复能力。

- 外边界防护区：此区域主要部署了面向外网和租户的前置部件，如负载均衡器、web 容器服务器等，以及与外部公网存在连接的服务。
- 业务服务安全域：部署与公网无直接联系的业务服务器，每个业务划分独立的业务主机子网，业务主机与数据库主机隔离。
- 数据库托管安全域：此区域部署数据库系统、对象存储系统，存储用户数据和业务数据，并进行了分区隔离。每个业务划分独立的数据库集群子网，数据库通过控制应用层访问的信任关系，实现业务主机与数据库主机点对点可信访问。
- 运维网络安全域：该区域主要部署操作运维组件，通过虚拟专用网络（VPN – Virtual Private Network）接入该区域，并通过跳板机访问节点。

在横向针对不同攻击面划分网络的基础上，纵向根据不同的应用划分为不同的安全组，每个安全组都采用独立 VLAN 控制。

针对不同的信任面和按照业务划分的主机组区域，建立不同业务面的信任关系，只有授信的访问对象，才能够连接访问。禁止不被信任的可疑连接，例如针对业务主机的访问连接，只能来自于运维安全信任域。针对数据库的连接，只能来自与其一致的业务主机信任域。

5.4 主机和虚拟化容器保护

为保证系统安全，对主机操作系统进行最小化裁剪并对服务进行安全加固，并针对可能的入侵行为，部署入侵检测系统。

针对 web 应用和底层系统，采取分布式的数据采样和集中分析防护的模型，匹配入侵规则，进行报警和防护。包括主机防护、木马检测、帐号安全检测、追溯查询、入侵取证追溯、软件指纹采集、策略管理、自定义策略、白名单、下发脚本、升级服务、策略库等。

针对服务部署镜像，包括操作系统和已安装的软件，统一提供标准镜像，由专业团队制作并严格测试后发布。由基础操作系统和加固后的初始化组件构成，将内核升级至最新稳定版本，确保设备系统的完整性，不会被非法篡改。

主机部署 HIPS（主机入侵防护系统）对异常 shell、rootkit、web shell、帐号提权等攻击行为，进行实时检测。

5.5 多层入侵防护

云上网络除了入口防御外，还采取了纵深入侵检测系统，以数据为核心，立体化布防，建立了多层次的纵深安全防御系统。

- 应用防护：部署 Web 应用防火墙以应对 Web 攻击，如 Web 应用层 CC 攻击、SQL 注入、跨站脚本攻击（XSS-Cross-SiteScripting）、跨站请求伪造（CSRF – Cross-Site Request Forgery）、组件漏洞攻击、身份伪造等，以保护部署在 DMZ 区、面向外网的 Web 应用服务和后台核心逻辑系统和服务。
- 主机防护：主机部署 HIPS 检测异常 shell、rootkit、web shell、帐号提权等攻击行为。
- RASP(Runtime Application Self-Protection)： web 应用层入侵检测系统，可以检测主流的高风险 Web 安全威胁和部分未知漏洞攻击。
- 漏洞扫描：例行对主机和应用进行漏洞扫描和风险修复。
- DBF（Database Firewall）：支持数据库异常流量检测和审计

通过基于风险构建的大数据安全分析系统，关联各安全设备的告警日志，支撑实时有序的分析，快速全面识别可能的攻击威胁。专职的安全团队，对安全设备产生的告警数据进行分析，及时发现和响应入侵事件。

大数据安全分析系统支持众多威胁分析模型和算法，结合威胁情报和安全咨讯，精准识别攻击，包括常见的暴力破解、端口扫描、傀儡机、Web 攻击、Web 未授权访问、APT 攻击等。并且分析潜在风险，并结合威胁情报进行预警。

5.6 零信任架构

在零信任网络环境中，应用需要鉴权后才能接入系统，系统会持续鉴权并采取动态访问控制。零信任架构对系统运行环境拥有实时感知的能力，并在感知到系统运行异常时即时决策和处置问题。

5.7 漏洞管理

依托华为安全应急响应中心 PSIRT 的技术支持，HMS 构建了一整套包括漏洞收集、漏洞处置和漏洞信息协同的完整漏洞管理体系，从系统漏洞、虚拟层漏洞、应用层漏洞各个层面进行全面而深入的研究，形成快速的漏洞处理能力，为用户提供更安全的产品及服务。

同时，我们与业界主流 OS 厂商保持密切的合作关系，有专门的组织和人员跟踪主流 OS/中间件的漏洞和补丁发布，并及时升级补丁；同时也关注操作系统安全策略的配置，保证系统权限的合理分配，关闭多余的服务和协议端口以及合理管理系统帐户等。同时定期使用系统漏洞检查工具对系统进行漏洞扫描，及时评估和修复操作系统中存在的安全风险。

完善的漏洞感知与收集渠道对于安全至关重要。华为 PSIRT 会主动通过合法的方式，同步业界知名漏洞库、安全论坛、安全会议等公开渠道的信息，尽可能第一时间感知安全威胁。您可以通过 psirt@huawei.com 与我们获得直接联系。为方便安全研究者、

租户更便捷地提交安全威胁，更直接、高效地进行漏洞响应，消减安全威胁，HMS 开辟了线上提交漏洞的入口。https://bugbounty.huawei.com/hbp/#/home

为保护用户的数据安全，秉承负责任的披露原则，对于涉及的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，我们会向最终用户及时推送漏洞的规避和修复方案。

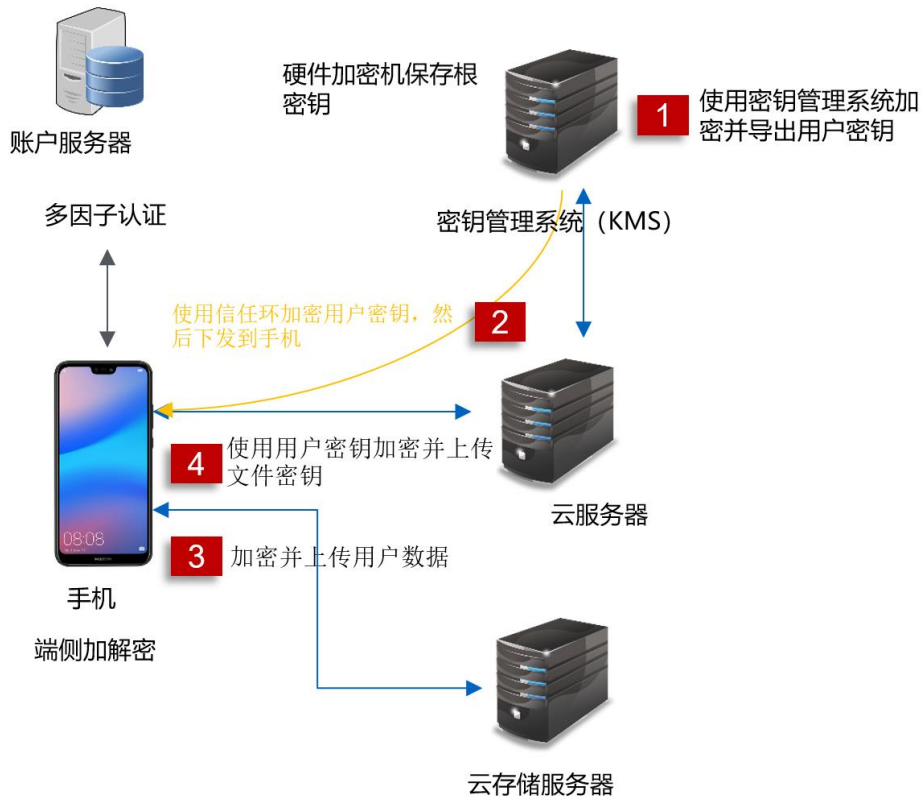
5.8 运营审计

通过集中、完整的日志审计系统，对可疑操作进行集中审计。该系统统一汇聚物理设备、网络、平台、应用、数据库和安全系统的操作日志,以确保危险动作被记录，可实时查询，支撑事后审计。

6 业务安全

6.1 云空间

云空间是华为终端云服务提供的用于用户数据存储的服务。在这里，用户可以安全存储照片、视频、联系人等重要数据，并且在各个设备上保持实时更新。云空间同步、备份的所有数据在传输过程中都进行了加密，在华为终端云的服务器上存储时也都经过了加密处理，帮助用户更安全、便捷地管理数据。



1. 用户密钥由密钥管理系统（KMS）生成，KMS 基于用户密钥 seed 和相关密钥素材导出用户密钥。
2. KMS 为每个用户生成密钥，应用必须通过用户合法身法获取密钥，防止密钥泄露

3. 用户数据在手机中使用文件密钥分块加密后上传服务器，明文数据不会传出手机。
4. 加密数据的密钥被用户密钥加密后上传云空间服务器，保证密钥安全传输和存储。

6.2 天际通

华为天际通为用户提供覆盖全球多个国家和地区的移动网络接入服务，满足用户在全球旅行过程中无需更换手机卡、只需购买并启用目的地套餐即可随时随地上网的需要。依赖多年底层芯片技术积累，天际通能够自动完成设备身份认证及软 SIM 卡数据安全下载，为用户提供高速上网体验。

天际通将需要缓存在手机侧的个人信息加密存储，业务敏感数据（如天际通套餐流量信息）则存储在 TEE 中，提供芯片硬件级的数据安全保护。

天际通的部分服务涉及与第三方平台的合作，在跳转合作方的 HTML 页面时，系统会对合作方的域名、HTML 页面可访问的接口进行白名单控制，对敏感接口进行黑名单控制。

6.3 查找设备

如果手机、平板、耳机等华为设备不慎丢失或被盗，用户可以尝试使用“查找设备”功能对丢失设备进行定位、响铃、锁定和远程擦除数据等操作。只有在征询您的同意后，在您使用“查找设备”功能时，我们才会收集您可能丢失的设备的位置信息。在您未登录华为帐号或主动授权同意前，我们不会收集您的任何位置信息。

打开查找设备功能后，用户可以定位设备的位置，以最大声音播放铃声。用户可以远程锁定设备并输入锁定信息，锁定信息设置成功后信息将会显示在锁定设备屏幕上。锁定功能会让设备进入锁屏状态，并自动上报位置数据。我们对用户设备的轨迹数据全部进行了加密处理，且仅保存最新的 24 小时记录。用户可以擦除设备，在输入华为帐号的登录密码确认后永久删除设备所有的数据（包括 SD 卡数据），保护设备的数据安全。

“查找设备”还为手机平板等设备提供了“激活锁”功能。当设备被远程擦除数据或非法重置后，只有输入设备绑定的华为帐号密码才能重新激活并继续使用您的华为终端设备，这在很大程度上可以阻止他人盗取后使用用户的设备。

查找设备的位置共享功能，用户可以主动授权给指定好友，查看自己共享的位置信息。共享发起方可以随时停止授权，停止授权后接收方将无法再定位到发起方位置信息。接收方也可以主动拒绝查看发起方共享的位置请求。

6.4 浏览器

华为浏览器为用户提供网页浏览、资讯推荐、网址导航、下载、搜索等服务，在帮助用户畅游网络世界的同时，最大程度地保护用户的安全与隐私。

华为浏览器具备强大的恶意网址检测和拦截能力，能及时识别钓鱼欺诈、网页挂马、恶意软件/木马、博彩/色情等黑灰色网址，并根据危害级别向用户展示不同的告警或拦截，保障用户的信息和设备安全，做到绿色浏览，安全随行。华为浏览器还向用户提供了举报网址的功能，通过“工具箱”内添加举报网址按钮，主动提交违规网址，用户还可以查看自己举报的网址列表。

华为浏览器提供的广告拦截能力，能及时识别访问地址是否为垃圾、骚扰等恶意广告页面，或者访问页面是否包含恶意广告内容或弹框并实施拦截，让用户获得优质浏览体验。华为浏览器通过添加手动标记网页广告的功能，增强了广告拦截的能力，进一步提升了用户的防骚扰的安全浏览体验。

华为浏览器为用户主动识别网页浏览过程中碰到的网页跟踪器，默认拦截跟踪型cookie，阻止其保留用户的个人信息或者在网络上跟踪用户。

在用户浏览过程中，华为浏览器会管控页面内 App 拉起，用户点击拉起 App 时需用户主动授权。防止页面内自动或者诱骗用户误点击拉起恶意 App。

华为浏览器向用户提供了隐私与安全的可视化报告，用户能够浏览华为浏览器完成的广告过滤、拦截的跟踪型 Cookie 等事件详细信息，让用户安心浏览。

用户可以设置无痕浏览模式，在该模式下华为浏览器不会记录用户的任何浏览信息，让用户放心浏览，隐私无忧。

华为浏览器提供了基本功能服务模式，默认开启限制个性化内容开关，提供空白主页，为用户提供最纯净的浏览环境。

华为浏览器为用户提供密码箱功能，网站自动保存的用户名密码、银行卡号均加密后存储在手机可信执行环境（TEE）中。加密使用的密钥存放在 TEE 中。用户可放心将网站自动保存的用户名密码等敏感数据安全存储在华为浏览器中。华为浏览器将标记为自动填充的网页凭证加密保存，并使用 TEE 存储加密密钥，实现多级加密保护。当用户需要查看或者修改自动填充的网页凭证时，要求用户进行锁屏密码或者指纹验证，防止自动填充的网页凭证泄露或者恶意篡改。

华为浏览器支持儿童模式，该模式下取消了首页信息流推荐，孩子不会看到内容推荐。而且，华为浏览器在儿童模式下还会自动禁止访问有风险的网站，家长也可以自定义添加一些不希望孩子访问的网站。华为浏览器通过技术手段的应用，为儿童打造了更加绿色健康的互联网环境，让儿童上网时多了一层防护，也让家长多了一份安心。

6.5 钱包/支付

Huawei Pay 支持将各类交通卡、银行卡、门钥匙、eID 等统统装进华为手机里，手机碰一下就可以购物、乘车、开门、进行身份认证等，是一款安全、便捷、智慧的手机电子钱包。

华为钱包不会存储银行卡 CVV（信用卡磁条背面三位数字）、有效期等敏感信息，仅在安全芯片中存储银行卡号 Token 化信息。为了保证持卡人的数据安全，Huawei Pay 绑定银行卡的过程中，信息经由卡组织提供的安全控件传输到卡组织，将卡号进行 Token 虚拟转化后，才返回到安全芯片进行存储，手机内储存的并不是真实的银行卡号。安全芯片为敏感数据提供隔离的运行空间，保护其避免遭受在非隔离空间下可能发生的恶意行为。

用户使用 Huawei Pay，需要通过支付密码或生物认证校验身份，校验通过才能进行支付；生物特征数据比对过程在可信执行环境（TEE）完成，包括华为钱包在内的任何应用都无法获取用户原始生物特征信息，生物特征数据不会上传到服务器。

Huawei Pay 服务器与设备和支付网络服务器通信时通过 TLS 安全通道。

Huawei Pay 支付消息采用数字证书签名，保障支付消息完整性，用户支付不会被恶意扣款和篡改。

IAP（In-App Purchases 应用内支付）面向全球开发者提供应用内支付功能，为应用提供统一简洁的商品定义、商品订单和订购、服务交付等能力。

通过 HMS 的 IAP，用户可以以方便、安全和保密的方式在应用中进行付款（使用银行资金或花币支付）。

用户授权 IAP 开通指纹/人脸支付功能时，IAP 指纹/人脸支付功能基于云证书服务 CCS，通过校验手机的设备证书（key Attestation）验证身份合法后，由 PKI 系统服务器为集成 IAP Kit 的应用签发应用支付证书，在支付过程中该证书会对指定的敏感数据签名，完成设备、应用、用户的三重安全验证，保证消息完整性。

用户在 Huawei Pay 上通过指纹/人脸验证支付时，系统首先验证用户输入的指纹/人脸的特征数据与手机可信执行环境（TEE）中存储的指纹/人脸的特征数据是否一致，验证通过后，交易数据需要在 TEE 中经过 PKI 数字证书签名后才会上传至服务器，保证用户支付的安全。在整个支付过程中，用户的指纹和人脸信息只保留在 TEE 中，不会上传云端，保障用户个人隐私数据的安全。

IAP Kit 服务器遵循金融行业标准的加密存储方式，在手机上显示银行卡号时，只展示前六位和后四位；存储用户的花币余额记录时，保存当前余额值摘要，防止数据被篡改；存储用户支付密码时，采用 PBKDF2 算法导出摘要保存，不存储原始用户密码。

Huawei Pay 和 IAP 通过了国际金融 PCI-DSS 认证，中国银联 ADSS 认证，BCTC 认证。

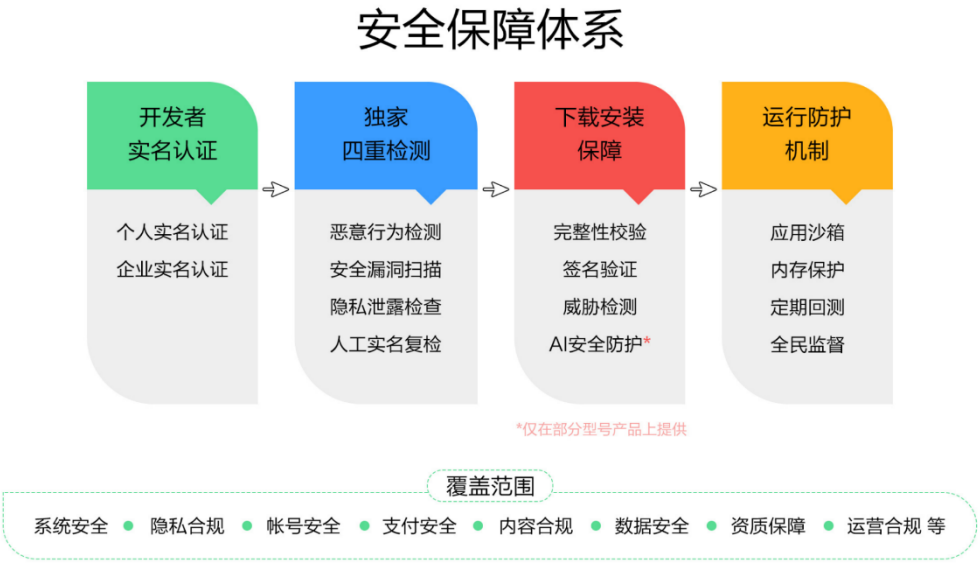
6.6 业务反欺诈

业务反欺诈专注业务安全领域，使用大数据和机器学习技术解决撞库、盗号、薅羊毛、刷单、业务欺诈等问题，保护用户虚拟资产的安全，保障用户获取公平、便捷的业务体验。HMS 具备营销活动反作弊能力，精准、实时地识别“羊毛党”、“黄牛”等欺诈行为，防范批量刷优惠券、恶意抢购、薅羊毛等作弊行为，为用户创造公平、便捷的业务体验。同时 HMS 会识别钱包和支付行为中的盗刷、欺诈行为；识别交易中的黄牛抢购、刷榜、刷单等行为

7 应用市场和应用安全

7.1 应用市场和应用安全概述

华为终端严格管理通过应用市场分发的应用，从开发者资质审核、到应用上架前安全检测、到应用上架后定期复测和用户反馈跟踪，提供应用全生命周期的安全保障。



7.2 开发者实名认证

为了切实保障用户信息安全及权益，我们对开发者进行严格的资质审核。对于个人开发者，需要开发者提供有效的身份证明等个人身份信息；对于企业开发者，开发者需提供营业执照原件扫描件和法定代表人身份证照片，用来证明其合法身份。保障开发者提交的应用程序出现恶意行为时，我们可以对恶意行为进行有效的追溯。

7.3 四重恶意应用检测系统

我们在上架前对每一款应用都使用华为杀毒云的 Secdroid 安全检测平台进行严格的安全测试，结合动态执行技术与静态特征分析技术，对应用的敏感行为进行检测分析、安全漏洞扫描、隐私泄露检查，确保开发者 App 的上架安全，给开发者提供便捷的安全检测服务。

恶意行为检测：面对海量应用上架申请，华为应用市场推出云端 Android 移动应用自动化扫描平台—SecDroid，SecDroid 与业界多家知名杀毒引擎厂商合作，对 APK 进行病毒检测；此外，基于 SecDroid 沙箱动态执行技术与静态特征分析技术，对恶意吸费、恶意消耗用户流量、恶意篡改个人信息等敏感行为进行检测分析。

安全漏洞扫描：华为应用市场采取静态和动态相结合的方式进行安全漏洞扫描。静态漏洞分析主要对 APK 进行静态扫描分析，拥有组件安全、数据安全、流量消耗检测、不安全的命令执行检测、密码输入框自动补全、开启服务检测、WebView 安全、敏感行为检测等检测类型，覆盖数十项分析检测点，全面分析 APK 潜在漏洞。动态漏洞分析通过动态检测在沙箱运行的待分析的 APK，基于捕获的动态运行日志分析 APK 中存在的安全漏洞。

隐私泄露检查：包括静态隐私分析和动态隐私分析。静态隐私分析采用数据流跟踪技术，通过分析 APK 静态数据流，对污染源及泄露点添加检测，检测隐私数据(例如电话号码，短信，位置等)泄露的完整路径。动态隐私分析通过扫描常见的密钥泄露、危险函数、不安全算法等问题，通过设置后缀、类型等过滤条件对扫描对象进行精细控制，输出精确匹配位置，上下文输出以及将匹配内容高亮显示。

人工实名复检：华为应用市场对所有上架应用都进行真人、真机、真实场景测试。真人指华为应用市场拥有专职安全测试团队，团队成员经过专业训练，并定期培训、学习最新安全测试方法，提升技能。真机测试覆盖华为的全部设备类型和操作系统版本，确保应用在各种设备上的兼容性。真实场景指对应用逐一进行真实场景测试。

7.4 下载安装保障

完整性校验：采用 SHA256 信息摘要算法，通过核对安装包上传时与下载后摘要值的统一性确保应用安装包的完整性。对于分块上传的应用安装包，采取边下载边校验的实时校验方式；而对于整包上传的应用安装包则在下载后进行整包校验。

签名验证：HarmonyOS 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。

威胁检测：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。HarmonyOS 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。HarmonyOS 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。系统支持本地病毒查杀和联网病毒查杀两种方式，确保用户设备在联网和不联网的状态下，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。

AI 安全防护：HarmonyOS 在设备侧提供了基于 AI 计算平台的安全防护功能，内置业界领先的 AI 杀毒引擎，其中包含经过深度学习训练的安全防护 AI 模型。HarmonyOS 通过实时观测未知应用软件的行为（未知恶意软件包括：新病毒、病毒新变种、恶意程序动态加载等），在设备侧运行 AI 模型对未知软件的行为序列进行分析，能够快速有效地发现威胁，提升应用威胁检测能力。AI 安全防护一旦检测到存在恶意行为的风险应用，立即警告用户，提示用户处理该风险应用。（此功能仅在部分芯片型号的产品上提供）

7.5 运行防护机制

应用沙箱：HarmonyOS 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，系统给应用分配了一个私有的存储目录，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。

内存保护：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，HarmonyOS 支持地址空间布局随机化及数据执行保护技术(DEP)，提高攻击者在利用内存漏洞上的难度，防止内存漏洞攻击。

定期回测：已上架的应用每个月定时进行安全扫描、回测，识别出有问题的应用自动下架。安全运营团队定期更新敏感字库，积极关注热点事件，对通过开发者的云端开关控制恶意行为执行的应用进行处理；

全民监督：用户可通过应用市场客户端、电话等渠道反馈问题应用。华为应用市场工作人员核实后第一时间对应用进行处理。

7.6 应用分级

不同国家或地区政策对应用分级有不同的要求，华为应用市场在不同国家或地区，提供满足当地要求的应用分级方案。

华为应用市场应用分级分为年满 3 周岁、7 周岁、12 周岁、16 周岁、18 周岁 5 大梯度，根据用户设置，自动屏蔽非适龄应用。

此外，华为应用市场还推出了针对儿童的“下载提醒”功能，家长可在华为帐号中心创建儿童帐号，孩子安装非适龄应用时，家长会收到弹窗提醒。

7.7 快应用安全

华为终端快应用引擎在客户端提供了一系列安全机制，竭力保障用户使用到稳定的、可靠的、安全的快应用。

快应用不向开发者提供设备标识符。针对不同的快应用，生成不同的 ID 标识符，对用户数据进行隔离，降低数据的可关联性，保护用户隐私。

为保证快应用包不被恶意篡改，华为终端会对快应用包的完整性进行验证，每个快应用都需要通过应用开发者的私钥进行签名，快应用的安装流程和升级流程均会进行签名校验，保证快应用包没有被篡改。

在快应用需要用到个人信息提供服务时，我们提供了业界标准的 RSA、AES 等安全算法接口进行数据的加解密操作，确保开发者可以使用此技术对用户数据加强安全保护。

华为终端提供快应用的权限管理，涉及用户个人信息的接口均需要用户独立授权，并提供权限管理界面供用户管理授权信息。

7.8 开放安全云测试

华为应用市场联合华为 2012 实验室，在中国北京、德国杜塞尔多夫设立终端开放实验室，打造 DevEco 系统（应用检测系统）并开放华为终端云侧能力。

1. 兼容性测试：最快 8 分钟输出一款应用测试报告，提供安装故障、启动故障、崩溃、无响应、闪退、黑白边、无法回退、UI 异常、运行错误、帐号异常、卸载失败共 11 种问题检测类型。
2. 稳定性测试：采用基于控件识别技术的随机遍历测试。
3. 性能测试：实时监测应用内存及手机 CPU 消耗等指标。
4. 功耗测试：通过记录分析应用后台对设备的占用频次和时长，综合衡量应用功耗。
5. SecDroid 安全测试：基于华为杀毒云 SecDroid 扫描系统可检测病毒、漏洞、广告、恶意行为、恶意扣费和隐私问题，通过端云结合的 AI 未知威胁防护技术，实时防护未知恶意软件。

8 HMS Core（开发者工具包）

8.1 HMS Core 框架

HMS Core 遵循 GDPR 等隐私法律法规要求，对开放的各项能力制定统一的隐私保护规范，严格保护用户隐私。按照消费者所在区域、遵循根据消费者所在区域（即应用分发地）决定签约主体和数据存储地，不同区域数据存储物理隔离的 3+X 部署策略，严格管控数据跨境风险。采取数据隔离（华为作为数据处理者的数据与华为作为处理者的数据隔离、不同开发者之间的数据隔离）机制，确保用户数据不被滥用。

在华为作为数据处理者的业务中，如帐号服务、支付服务，在 OOBE（Out-of-box experience 系统初始化）开机阶段或应用内告知个人信息处理信息，并授予用户充分的数据控制权限，包括下载个人信息副本、控制统计数据上报、关闭自动更新等。

在华为作为数据处理者的业务中（如分析服务），响应开发者请求，公开子数据处理者信息，记录数据处理过程，支持开发者的数据主体权利义务达成，严格落实数据处理义务。

当开发者选择依托 HMS 构建应用时，首先需要注册成为华为开发者，申请相应开放能力。HMS Core 框架为开发者提供注册、开放能力申请、开放能力访问凭证设置、以及云端开放能力 Token 生成/验证能力。HMS Core 框架通过 AES 算法加密存储保护开发者注册时的身份信息、银行帐号等数据。

HMS Core Kit 有两种发布方式，一是随 HMS Core 打包一同发布，二是独立发布并由 HMS Core 动态加载。随 HMS Core 打包一起发布的 Kit，由 HMS Core 统一打包后发布到应用市场，由用户自行选择是否升级更新，更新时需要获取用户授权。升级更新时会验证 HMS Core 签名信息，只有通过签名验证后才能对 HMS Core 进行覆盖安装。对于独立发布的 Kit，Kit 发布到应用市场后由 HMS Core 框架进行下载更新，更新时 HMS Core 会校验 Kit 的签名证书指纹，判断是否在其白名单中。如果证书指纹不在白名单中则禁止加载，如果在白名单中则继续验证 APK 签名信息，只有通过签名验证后才允许 Kit 覆盖更新。

8.1.1 认证凭据

开发者访问 HMS Core 的开放能力时，需要先在开发者联盟网站创建认证凭据，开发者应用通过携带的认证凭据访问 HMS 开放能力。当前支持的凭据有 API Key、OAuth2.0 ClientID、Service Account Key。

API Key、OAuth2.0 Client ID 和 Client Secret 使用安全随机数生成，生成后在服务器使用 AES-GCM 加密后存储，防止认证凭据泄露。Service Account Key 公钥由 HMS Core 保存，私钥由开发者保管。认证凭据的使用场景分别如下：

1. API Key：API Key 是一个简单的加密字符串，可在调用访问公开资源的 HMS 开放能力时使用，例如开发者使用 API Key 访问位置服务（Site Kit）和地图服务(Map Kit)。

   开发者可以对 API Key 设置使用限制，包括应用限制和 API 限制。应用限制包括限制指定网站或限制指定的 Android 应用使用 API Key。API 限制指限制 API Key 能访问的 HMS 开放服务列表。

2. OAuth2.0 ClientID：开发者应用在访问需要华为帐号用户登录的 HMS 开放能力时，可以通过华为帐号服务（Account Kit）以 OAuth2.0 协议标准获取用户的授权访问 Access Token，开发者应用携带 Access Token 访问用户相关的 HMS 开放能力。例如开发者应用使用 OAuth2.0 ClientID 和 ClientSecret 访问云空间服务(Drive Kit)、运动健康服务(Health Kit)。

   开发者应用可以通过移动应用和 Web 应用两种方式访问 HMS 开放服务，开发者应用在获取到用户登录的授权票据(Authorization Code)后，通过开发者服务器携带授权票据和 ClientID/ ClientSecret 到 Account Kit 服务器获取 Access Token。当安卓移动应用通过 HMS Core 访问开放能力时，HMS Core 可以通过开发者配置的安卓 APK 证书指纹及 ClientID 对安卓移动应用进行认证，防止 APK 身份被仿冒。

3. Service Account Key：用于开发者服务器与 HMS Core 服务器间对接认证，开发者服务器生成 JWT（JSON Web Token）并使用 Service Account Key 私钥进行签名，HMS Core 服务器对 JWT 认证通过后返回接入 Access Token，开发者服务器具备通过接入 Access Token 访问 HMS CORE 服务器的开放能力。例如开发者使用 Service Account Key 访问近距离通信服务(Nearby Service)。

8.1.2 安全沙箱

基于多种系统级安全隔离技术和虚拟化容器技术构建 HMS Core Kit 安全沙箱，运行在安全沙箱的 Kit 将具有完全隔离的文件命名空间，对系统资源的所有请求也将被强制鉴权，这些资源包括网络、外部存储、如地理位置、联系人、录音等。借助安全沙箱能力，Kit 故障、漏洞利用的影响将被有效隔离和缓解，HMS Core 整体安全性得到极大提升。

8.1.3 业务容灾

HMS Core 服务器采用多站点容灾部署，数据周期性同步到容灾站点。数据库采用主从方式定期同步备份，生产环境与容灾环境之间使用专线保障数据传输。在容灾切换时，使用 DNS 切换域名解析，将业务流量切换到容灾站点。定期进行容灾演练，以确保容灾环境的可用性。

8.2 华为帐号服务（Account kit）

8.2.1 授权开发者登录

Account kit 为开发者提供了通过华为帐号登录开发者应用的能力，开发者通过 Account Kit 获取华为帐号用户身份认证信息(ID Token)或用户的临时授权票据(Authorization Code)后，即可通过华为帐号安全登录应用。

Account kit 遵循 OAuth2.0 和 OpenID connect 等国际标准协议为开发者提供帐号登录能力,基于华为帐号的安全能力，具备高安全性密码验证和手机短信验证码保障帐号安全性，帐号安全状态发生变化时快速通知开发者，助力开发者提升业务安全。

Account kit 遵循 GDPR 等隐私法规要求，严格保护用户隐私，支持用户数据主体权利。登录第三方应用时，在用户同意的情况下仅分享经过用户授权的帐号信息，用户可以在帐号中心随时撤回授权登录。基于 OpenId 授权，做到不同应用间隔离。

8.2.2 反欺诈

在抢购、秒杀、优惠券、礼包、抽奖等业务场景中，黑灰产试图通过各种渠道批量注册大量虚假用户参与活动并获取利益，Account Kit 在注册时通过操作异常、手机号异常、邮箱异常、风险网络等多种手段识别风险，结合专家规则、机器学习识别虚假帐号，打击虚假注册，减轻后端业务风险。

开发者应用接入 Account Kit 后，可以在服务端订阅华为帐号风险状态同步接口。系统识别到垃圾帐号后，将第一时间通过风险状态同步接口通知华为帐号登录的开发者应用，便于开发者应用及时作出响应。

8.3 通知服务（Push Kit）

Push Kit 是华为终端给开发者提供的消息推送平台。Push Kit 建立了从云端到手机端的消息推送通道，让你可以将最新信息及时的通知你的用户；如果开发者服务器实现了 XMPP 连接协议，则可以接收从应用发送至 Push 服务器的消息，Push Kit 通过云端和手机端之间的信息推送与接收，帮助开发者构筑良好的用户关系，提升用户的感知和活跃度。

Push Kit 为开发者提供精准消息推送功能，为每个应用分配不同的标识（AAID），做到应用间的数据隔离。我们不会保留开发者发送给用户的消息，在消息发送成功后，立即删除。

8.3.1 身份认证

开发者应用运行时申请 Push Token，HMS Core 框架会校验应用的 AppID 和 APK 签名证书指纹。通过校验后，Push Kit 客户端与服务器间基于 TLS 协议，在验证服务器证书后建立长连接，由 Push Kit 服务器为开发者应用分配唯一的 Push Token。Push Token 包含了开发者应用的 AppID 和安全随机数，并且在服务器端加密保存。

开发者通过 Push 服务器发送 Push 消息到客户端时，需要使用认证后获取 Access Token，Push 服务器通过 Access Token 认证 Push 消息请求，同时会校验 Push Token 中

的 ClientID 与 Access Token 中的 ClientID 是否匹配，若不匹配则丢弃 Push 消息，匹配后才会发送 Push 消息。

8.3.2 Push 消息保护

应用可以通过定向广播或 AIDL（安卓接口定义语言）接口从 Push Kit 获取推送的 Push 消息，定向广播的安全性由 Android 保护，AIDL 接口会使用 HMS Core 框架提供的应用身份校验机制进行认证。只有通过校验的应用才能读取该应用的 Push 消息，如果应用没有及时获取 Push 消息，Push Kit 会对消息加密后存储在私有目录下。

应用通过 Push Kit 客户端发送订阅消息到 Push Kit 服务器时，HMS Core 会验证该应用是否拥有发送消息的能力。Push Kit 客户端会使用与服务器协商的密钥，通过 HMac-Sha256 对订阅消息生成消息验证码，服务器对消息验证码进行校验，防止订阅消息被篡改。

Push Kit 服务器在发送消息前会审核消息是否合法、合规，审核通过后才进行消息推送。

8.3.3 Push 消息安全传输

Push Kit 客户端与服务器间除了基于 TLS 协议保护传输内容安全，还在客户端与服务器建立连接时协商 Session Key，对发送的消息进行加密，连接中断再次建立时会协商新的 Session Key。

8.4 应用内支付服务（In-App Purchases）

IAP Kit 面向全球开发者开放，提供应用内支付功能，为开发者提供统一简洁的商品定义、商品订单和订购、服务交付等能力。

8.4.1 商户和交易服务认证

为保障用户的支付安全，商户在发起支付请求时，在商户服务器使用 RSA 私钥对支付消息进行签名，签名后的支付订单发送给 IAP 服务器进行验签，保证消息完整性。

8.4.2 防截屏录屏

IAP Kit 在关键信息界面（如支付密码输入界面）提供了防止截屏、录屏的功能。当用户在关键信息页面触发截屏时，系统会提示当前页面不允许截屏；当用户在关键页面触发录屏时，若录制的视频涉及关键信息，则录制的页面会变为黑屏，防止用户关键隐私数据泄漏。

8.4.3 防悬浮窗监听

拥有悬浮窗权限的应用可以悬浮在任何其他界面上。在涉及到用户需要使用键盘等交互界面进行信息录入的场景时，此类应用可以通过记录用户触摸屏幕的位置，来推测并破解出用户输入的口令信息。

IAP Kit 提供防悬浮窗监听的能力。系统判断用户进入支付收银台页面后，若检测到页面上方有悬浮窗（如视频通话悬浮窗），会将悬浮窗隐藏，避免悬浮窗监听用户操作屏幕，保护用户的输入安全和支付安全。

8.4.4 指纹/3D 人脸支付

IAP 指纹和 3D 人脸支付为用户提供安全便捷的支付体验。IAP 本身不会收集和处理用户的指纹和人脸数据，用户在手机本地完成指纹和人脸认证，授权使用用户级支付私钥对本次支付数据签名，IAP 服务端通过验证签名确保本次支付是用户授权后，完成扣款。

8.4.5 禁止口令密码输入控件提供拷出功能

部分应用提供输入控件拷出功能，可以读取用户最近一次拷贝的信息并上传到后台识别分析，易造成用户隐私数据泄露。IAP Kit 在部分关键敏感数据输入界面（如花币卡号密码界面）设置防护，卡号密码输入框禁止数据拷出，以防卡号密码等信息泄露引发资金损失。

8.5 广告服务（Ads Kit）

Ads Kit 为开发者和泛生态合作伙伴提供广告展示服务，帮助合作伙伴与用户建立连接，向用户传递价值信息和品质服务。

华为终端向用户提供众多免费、优质的服务。为保护用户的隐私，广告服务不收集用户的健康、支付、通讯录、通话记录等敏感信息，用户的任何信息都不会透露给广告主，当使用用户信息进行细分投放个性化广告时，您所在的组别至少会有 5000 人。如果用户启用了“限制广告跟踪”，包括华为终端在内的所有广商均无法获取用户设备的广告 ID，因此无法向您投放个性化广告。同时保护未成年，对于注册的未成年人，不投放任何广告。

8.5.1 高质量的广告选择

Ads Kit 希望为用户提供高质量的广告选择，并持续增强机器筛选能力和覆盖范围，如肖像权检测，违禁品检测，儿童保护等。

Ads Kit 为开发者提供广告内容防篡改的能力，Ads Kit 服务器对要展示的广告图片和视频进行 SHA256 摘要，摘要和广告图片分别通过两个不同的业务流和 HTTPS 通道连接传输，并在 Ads Kit SDK 校验摘要，防止广告传输过程中被篡改。

8.5.2 反作弊系统

Ads Kit 为开发者提供反作弊系统，当系统识别出作弊设备、IP 等信息时，将对作弊流量进行无效化处理。反作弊系统通过 AI 技术对数据完整性、黑白名单、数据关联性和合理性、用户行为合理性、屏蔽策略等进行分析识别出作弊行为。

8.5.3 数据安全

Ads Kit SDK 为开发者提供用户数据存储保护，手机侧的所有用户数据都存储 HMS Core 私有目录下，其中重要数据均加密后存储，为开发者提供基于操作系统的私有数据隔离机制，保证集成 Ads Kit 的开发者应用的数据不会被其他应用访问。

Ads Kit 服务器为开发者提供用户数据分级分类保护功能，高影响个人信息和重要系统数据（例如 IMEI、三方监测服务地址）都进行加密保护；其他数据如设备标识符（OAID）都基于加密算法进行假名化处理，确保无法通过数据直接识别并定位到用户。

当开发者应用涉及向第三方广告投放平台、第三方监测服务、媒体应用的服务器分享数据（例如广告相关的点击、下载、安装等事件）时，Ads Kit 一般基于预共享密钥机制和 HTTPS 加密传输通道，确保第三方广告投放平台服务器的身份合法性和数据传输安全。

8.6 云空间服务（Drive Kit）

Drive Kit 允许开发者创建使用华为云存储的应用程序，华为云存储可以为您的应用提供云端存储功能，将用户在使用您的应用时产生的文件保存到云盘，也可以下载、同步和搜索在华为云盘中的所有文件，包括照片、视频以及文档等。同时 Drive Kit 为各类数据提供了安全保障，让用户更安全、便捷地管理数据。

Drive Kit 通过华为帐号登录认证后获得的用户级 Access Token，确保用户存放在云空间的私有文件只有用户本人才可以访问，共享文件只有授权的用户才能访问，同时对于存放在云空间的文件进行文件级密钥加密存储，防止存储数据泄露。

8.6.1 认证授权

用户登录华为帐号并授权后开发者应用后才能访问 Drive Kit 服务。开发者应用先通过华为帐号服务（Account Kit）获取用户登录的访问令牌（Access Token），在调用 Drive Kit 服务接口时，还需要用户授予应用访问用户云存储空间的权限。Drive Kit 服务器对访问令牌进行认证，只有通过验证才能访问云存储中对应用户的数据。

8.6.2 数据完整性

应用在上传文件时，如果应用提供文件的 hash 值，Drive Kit 服务将对上传文件进行完整性校验；应用下载文件时，Drive Kit 服务提供文件的 hash 值，应用可以进行文件完整性校验。

8.6.3 数据安全

用户上传到 Drive Kit 服务的数据，每个文件都会被自己独有的密钥加密后存储，文件密钥会被基于硬件加密机保护的 KMS 系统加密后保存。

8.6.4 业务双活与数据容灾

Drive Kit 服务采用双活方式部署，同时对数据进行物理容灾，持续提升为用户提供服务的能力。通过定时同步的方式将数据同步到容灾站点，数据库采用主从同步方式进

行数据同步，主站与容灾站点之间均有专线保障数据传输。当主站业务不可用时，则启用容灾站点的业务环境，继续提供业务服务。

8.7 游戏服务(Game Kit)

Game Kit 通过游戏 App 给系统提供精细化场景信息、配置信息、网络信息等，系统给游戏 App 反馈系统状态信息等，使得双方能够利用这些信息进行更紧密和深入的协作，在系统资源有限的情况下进一步改善玩家的游戏体验。

为了保证用户数据的安全，无论是存储在个人设备的数据，还是传输过程中的数据，以及存储在云端的数据，Game Kit 都会对个人信息进行加密处理，用户的个人信息仅在用户授权同意的情况下分享给第三方游戏，用户可以随时撤销对第三方游戏的授权。Game Kit 提供独立的游戏用户 ID 体系，与华为帐号其他服务中的个人信息隔离。

8.7.1 数据保护

游戏服务在设备侧处理个人信息时，使用了业界标准的 AES、RSA 等安全算法对用户数据进行加解密/签名操作，确保用户设备侧数据的安全性。

对于排行、成就、事件和玩家信息统计，会发送到华为终端云服务器保存。数据保存时根据应用标识来做隔离，不同的应用使用自己的应用标识访问自己的游戏服务数据，无法访问到其他应用的游戏服务数据。

游戏存档记录通过 HTTPS 通道上传到华为终端云服务器后，按照用户和应用维度隔离存储，并采用 AES 高级加密标准进行加密保存，加密方式采用两层加密，第一层密钥（即文件加密密钥）根据文件的属性值来派生，用来加密文件；第二层密钥（用户加密密钥）使用用户属性值来派生，用于加密第一层密钥。保证用户仅能使用自己的加密密钥加密保存自己的游戏数据。

8.7.2 用户授权

涉及用户个人信息授权给第三方使用的场景，均需用户进行独立的显式授权。游戏服务使用手机系统的敏感权限时，会明确提示用户并要求用户授权后才可使用。

8.8 用户身份服务(Identity Kit)

Identity Kit 为开发者提供统一的地址管理服务，第三方应用经过用户授权后可直接获取地址信息，主要提供地址管理和地址选择两个能力。

Identity Kit 通过 ClientID 和 APK 证书指纹对开发者应用进行接入认证，防止仿冒应用调用。采用 HTTPS 通道对地址数据进行加密传输保护，并对开发者服务器证书进行绑定校验，防止地址数据发送到仿冒的服务器。

Identity Kit SDK 不存储用户地址信息。用户地址信息在 Identity Kit Server 采用 AES-128-CBC 算法加密存储，不同用户的地址数据使用用户级的访问权限控制进行逻辑隔离，用户访问前，需要验证用户级的访问 Access Token。

Identity Kit 为用户提供轻松便捷的地址管理能力，用户的个人信息仅在用户授权同意的情况下分享给第三方应用。用户的地址信息在云端加密存储，访问前需要用户身份鉴权。

8.9 钱包服务（Wallet kit）

华为钱包包含 Huawei Pay 和电子钱包，聚焦卡/证/券/票/钥匙的归集和开放投放渠道，为商户和用户提供便利。

Wallet Kit 提供基于 SE 的开放能力，集成 Wallet kit 的应用可使用手机模拟银行卡或者公交卡，在支持 NFC 刷卡的读卡器（银行 POS 或者公交闸机）上完成支付；提供应用内支付能力，集成 Wallet kit 的应用可基于钱包中绑定的银行卡完成支付。

同时，用户可将集成了 Wallet Kit Pass SDK 的应用所产生的卡/证/券/票/钥匙信息，添加至华为钱包，通过华为钱包 Card Store、情景智能、华为推送服务等统一管理。

8.9.1 系统环境安全识别能力

Wallet Kit 为开发者提供系统级 Root 安全检测能力，实时检测手机系统是否被 Root。若手机系统被 Root，提示用户使用 wallet 存在安全风险，用户可自行决定是否继续支付。

8.9.2 卡券数据安全（仅中国支持）

开发者应用在将卡/证/券/票/钥匙等卡券数据写入华为钱包时，使用 RSA 私钥对卡券数据签名后发给华为钱包 App。华为钱包 App 将签名后的卡券数据发送至钱包服务器进行验证，验证卡券数据的合法性和完整性。

8.10 运动健康服务（Health Kit）

Health Kit 为开发者提供运动健康数据平台和服务开放能力，开发者通过集成 Health Kit SDK，为用户提供健康关怀和运动指导等服务体验。

Health Kit 通过硬件级的文件加密保护用户的运动健康数据，并为用户提供细粒度的数据读写访问控制，保证用户数据安全的同时，实现用户对自己的数据可知可控可管理。

8.10.1 用户数据访问控制

开发者应用或服务在没有获得用户明示授权之前，无法访问用户在 Health Kit 中的运动健康数据。Health Kit 的访问授权支持将用户的运动健康数据按 23 类进行细粒度划分，并且每类数据的读取和写入权限可以分开控制，没有用户对每类数据读取和写入权限的主动勾选，就无法访问用户对应类型的数据。为了确保重要数据的准确性，当开发者在华为开发者联盟上申请与医疗相关的健康类数据写入权限时，还需通过额外审批。手机锁屏状态下，用户的个人信息只能写入不能读取，防止用户数据在后台泄露。

8.10.2 数据加密存储

EMUI8.1 以上版本的华为手机，运动健康数据采用基于系统硬件的文件加密保护机制。手机锁屏 10 秒后，不能再读写加密后的运动健康数据，避免数据被恶意滥用，此时写入的运动健康数据只能通过临时库保存，手机解锁后才会被转存到正式的运动健康数据库中。

Health Kit 云上的运动健康数据通过高级加密算法 AES 加密存储，每个用户都有独立的数据加密密钥，密钥会被基于硬件加密机保护的 KMS 系统加密后保存。

8.11 线上快速身份认证服务（FIDO）

FIDO 为开发者提供线上快速身份认证开放服务，提供本地生物特征认证和 FIDO2 线上用户身份认证能力，为开发者提供安全易用的免密认证服务。

FIDO 规范成熟，支持广泛，生态完善，使用生物特征或外部设备完成身份验证，降低密码泄露风险。生物特征等用户个人隐私在手机端完成验证，数据不出终端设备，保护用户隐私。

8.11.1 本地认证（BioAuthn）

BioAuthn 包括指纹认证和 3D 人脸认证。为开发者提供安全易用的免密认证服务，并保障认证结果安全可信。开发者在调用前，需先调用 Safety Detect SysIntegrity 确认设备运行环境安全。

BioAuthn 提供安全的指纹/3D 人脸认证能力。如果系统安全存在问题，则返回错误码；如果设备运行环境安全，则执行指纹/3D 人脸认证。

EMUI 5（API Level 24）以上版本支持指纹认证，EMUI 10（API Level 29）以上版本支持人脸认证，使用前请确保设备硬件支持指纹和 3D 人脸认证。

8.11.2 线上用户认证（FIDO2）

在线用户认证的特性包括：

1. 基于安卓平台实现符合 FIDO2 规范（包括 WebAuthn 和 CTAP2）的客户端和基于本地生物特征认证的平台认证器组件，帮助开发者实现免密码用户认证体验；
2. 支持通过 USB、BLE、NFC 等通讯方式对接 FIDO 安全密钥硬件，完成用户认证过程；
3. 提供安卓 SDK，帮助安卓应用开发者接入使用；
4. 与华为浏览器集成，提供 WebAuthn JS API，帮助 Web 应用开发者接入使用；
5. 支持把具有本地生物特征认证能力的手机作为 FIDO 安全密钥，辅助其他设备完成用户认证过程

1. FIDO2 客户端在处理请求前，会先调用 Safety Detect SysIntegrity 确认设备运行环境是否安全。如果安全，才会继续处理请求，否则返回未通过系统完整性检查错误。

8.12 数字版权服务（DRM Kit）

DRM Kit 向开发者提供内容的数字版权保护能力，包括增强硬件级、硬件级与软件级的 DRM 能力，支持客户端证书在线申请，多种内容加密格式与加密算法，在线与离线播放等多种场景。第三方应用使用密钥对内容进行加密，用户播放加密的内容时，需要使用密钥解密后才可以观看对应内容。

DRM Kit 基于用户设备 ID（UDID 或 DIEID）进行 DRM 证书申请，并下发证书到设备芯片。

8.12.1 硬件级安全运行环境

DRM 客户端的核心模块运行在华为手机的 TEE 中，TEE 为 DRM 客户端提供了硬件级的安全运行环境，并保护 DRM 客户端中的机密数据的存储和使用：

1. DRM 证书和私钥存储在 TEE 安全存储区。
2. 内容密钥在播放时才在 TEE 中解密出密钥明文，不缓存。
3. 视频内容在 TEE 中解密，视频内容明文不出 TEE。
1. 部分海思芯片提供了增强硬件级的安全运行环境支持，具备防侧信道攻击的能力。

8.12.2 安全视频路径

安全视频路径确保加密的视频从内容解密到视频解码到本地渲染播放/投屏输出的整个视频传输路径的安全，防止解密后的视频内容被泄露。

加密视频由 DRM 客户端在 TEE 中解密，解密后的视频内容输入到安全解码器中解码和渲染播放。解密的视频内容受 TEE 安全机制及安全芯片硬件保护，OS 层无法访问，用户无法通过录屏软件录制视频。

用户通过 HDMI 线连接手机和大屏设备（如电视），并设置投屏播放 DRM 视频内容时，视频内容在传输到大屏设备前，通过 HDCP 芯片进行加密传输保护，对大屏设备进行合法性认证、视频内容加密等。

8.12.3 安全时钟

DRM 客户端使用 TEE 的安全时钟对内容 License 中的播放有效期进行校验和控制，用户无法修改 TEE 安全时钟。

8.12.4 DRM 证书认证

DRM 客户端在申请 DRM 证书时，DRM 服务端通过华为设备证书及私钥签名对 DRM 客户端认证鉴权。华为设备证书和私钥在出厂前即预制到设备的安全存储区，每台设备预制独有的证书和密钥，只有授权的应用才能访问设备证书和私钥。

DRM 客户端向 DRM 服务器申请内容 License 时，需要通过 DRM 客户端证书和 DRM 服务端证书的双向身份认证。

8.12.5 安全传输

DRM 服务器使用 DRM 客户端证书的公钥对内容密钥加密后下发给 DRM 客户端。DRM 请求和响应消息通过 DRM 证书进行签名保护，防止中间人攻击，保护 DRM 消息在传输过程中不被篡改。

8.13 机器学习服务（ML Kit）

ML Kit 基于机器学习技术为开发者提供视觉类服务和语言类服务。视觉类服务包括文本识别、人脸检测、图像分类、对象检测和跟踪、地标识别、图像分割等 AI 视觉服务；语言类服务包括语音识别、自然语言检测、翻译。

8.13.1 数据处理

ML Kit 最小化使用个人信息。 ML Kit 对于个人信息的处理，尽量在设备本地进行，如人脸检测、卡证识别等。对于设备侧无法处理的能力，ML kit 上传云侧处理的数据不会关联个人标识符，处理完成后即删除。

8.14 近距离通信服务（Nearby Service）

Nearby Service 指通过蓝牙、Wi-Fi 等技术，发现附近的设备并与它们通信，包括近距离设备间数据传输（Nearby Connection）、近距离消息订阅（Nearby Message）以及华为接触卫士（HMS Core Contact Shield）3 个主要功能。

近距离设备间的数据传输能够在无需 Internet 连接的情况下发现并建立与其它设备的直接通信通道。建立连接时，需要用户确认，所有传输的数据使用协商的密钥进行加密，保护数据的机密性、完整性，整个过程不涉及和服务器的交互，不会把数据发送到任何服务器。

近距离消息订阅基于 Internet 连接，订阅者（App）接收发布者（Beacon 或者 App）广播的共享码，根据共享码从云服务器获取对应的消息内容。客户端和云服务器使用 HTTPS 协议进行通信，使用 API Key 进行身份认证，保护消息的机密性、完整性。用户通过 App 直接发布近距离消息时，会把消息保存到华为云服务器，华为不会将消息与任何个人身份标识和设备标识进行关联，对于用户而言是完全匿名的。用户通过 Beacon 发布消息时，也会把消息保存到华为云服务器，消息和 Beacon 的共享码（即 BeaconID）进行关联，以便其他用户能够通过 Beacon 广播的共享码订阅消息。

我们倡导开发者在后台发布消息或订阅服务时获取用户的同意。在用户授权后启动 Message 服务，同时为用户提供便捷的订阅开关。

华为接触卫士是 HMS Core 提供的基于低功耗蓝牙（Bluetooth Low Energy，简称 BLE）的接触跟踪基础服务。只有经过各国公共卫生机构授权，并通过过华为严格审核后的应用才可以使用接触卫士 API 以开发新冠肺炎 (COVID-19)接触跟踪的应用。用户在启动华为接触卫士后，会生成动态共享码，为防止跟踪，动态共享码每 10 分钟生成一次，用于通过蓝牙向同样开启华为接触卫士的手机分享共享码，公共卫生机构发布有确诊新冠肺炎 (COVID-19) 则会通知用户接下如何处理。接触卫士不会使用用户的位置信息，也不会采集、分享用户的身份信息，用户可以通过开关控制是否使用接触卫士，也可以手动直接删除全部历史数据。

8.15 定位服务（Location Kit）

Location Kit 采用 GPS、Wi-Fi、基站等多种混合定位模式进行定位，赋予开发者应用快速、精准地获取用户位置信息的能力。Location Kit 为开发者提供融合定位、基于位置的提醒、识别用户的活动状态、地理编码查询等能力。

Location Kit 采用 HTTPS 协议对定位请求数据进行加密传输保护，并对定位服务器证书进行绑定校验，防止定位请求发送到仿冒的服务器。定位服务要求开发者应用获得用户的位置定位授权后才能提供服务。

Location Kit 不会保存用户的位置信息，处理后即删除，位置数据不与任何用户标识或设备标识关联，无法通过位置信息来跟踪用户，保护用户隐私。为开发者提供地理围栏功能，用户设置的围栏数据仅保存在设备本地，不会上传到服务器。此外，定位服务不会将数据披露给第三方。

8.15.1 用户授权

Location Kit 使用安卓系统的权限控制机制判断是否允许开发者应用获取对应的位置信息。Location Kit 校验开发者应用是否获得了用户的授权，包括高精度、低精度及后台的位置权限等。

8.15.2 数据存储

Location Kit 对开发者应用提交的地理围栏信息（包括围栏 ID、经纬度等）进行了隔离和保护：

1. 地理围栏信息不上传到 Location Kit 服务器。
2. 地理围栏信息的访问通过开发者的应用包名进行隔离，开发者应用只能访问自身的地理围栏信息。

8.16 位置服务（Site Kit）

Site Kit 为开发者提供了地图搜索功能，搜索结果可以直接应用于地图展示。

Site Kit 通过 ClientID 和 APK 证书指纹、API Key 等手段对开发者进行接入认证和调用配额限制，防止仿冒应用调用。采用 HTTPS 协议对位置请求数据进行加密传输保护，并对位置服务器证书进行绑定校验，防止位置请求发送到仿冒的服务器。

Site Kit 仅在用户同意下，对搜索数据匿名化存储，用以改进位置服务，其他场景不收集和处理个人信息。华为终端无法获取用户的位置搜索和访问记录，无法跟踪或识别用户的行踪。华为终端不会披露个人信息给第三方。

8.17 地图服务（Map Kit）

Map Kit 为开发者提供一套供地图开发调用的 SDK，地图数据覆盖超过 200 个国家和地区，支持数十种语言，开发者可以轻松地在应用中集成地图相关的功能，提升用户体验。

Map Kit 通过 ClientID 和 APK 证书指纹、API Key 等手段对开发者进行接入认证和调用配额限制，防止仿冒应用调用。采用 HTTPS 协议对地图请求数据进行加密传输保护，并对地图服务器证书进行绑定校验，防止地图请求发送到仿冒的服务器。

地图服务不会收集和存储用户个人信息，因此无法跟踪用户的行为轨迹。用户请求地图数据时，地图服务先在设备中将用户的经纬度转化为地图数据坐标，再发起服务请求，无需上报用户位置信息。此外，地图在引入第三方供应商时均以华为终端同等要求约束其数据处理，确保用户的个人信息始终得到充分的保护。

8.18 情景感知服务（Awareness Kit）

Awareness Kit 为开发者提供基于用户当前时间、位置、活动状态、环境光、天气等方面的情景感知能力，为用户提供更加智慧和贴心的服务体验。

根据使用的功能， Awareness Kit 可能需要获取位置、蓝牙、网络等权限和环境光、耳机状态、活动状态、地理围栏等感知功能，所有数据均在设备中完成处理，数据不会发送到服务器。对于天气、当地节假日感知功能，需要把粗略位置（千米级别）发送到服务器以便获取信息，发送过程使用 HTTPS 协议进行加密传输，位置信息不会关联到设备或用户，也不会在云端保存。

8.19 分析服务(Analytics Kit)

Analytics Kit 是面向应用开发者的一站式数据分析平台，在用户授权的前提下基于应用上报的用户行为事件和用户属性数据，结合平台预置的大量分析模型，为开发者提供产品优化、运营决策的参考。

Analytics Kit 通过端云多层加密安全传输和云侧逻辑隔离存储，保障开发者分析数据的经营统计指标安全，保障应用业务商业分析安全。

Analytics Kit 为每个设备分配不同 AAID 作为唯一的设备标识，除此之外不收集 IMEI、SN 等持久化标识符。未经开发者的同意，开发者的数据不会用于任何其他目的，不会共享给第三方。通过自动化接口为开发者实现数据主体权利义务，包括访问权、反对权、删除权等。

8.19.1 服务端防仿冒

Analytics Kit 通过对服务器证书验证，确保数据传输到可信的服务器。通过对证书的签发者、有效期、域名等进行验证，防止开发者应用数据上报到仿冒的恶意服务器，导致数据泄露。

8.19.2 数据安全传输

Analytics Kit 上报数据至服务器时采用 HTTPS 安全协议传输方案，确保传输安全，防止应用数据被恶意攻击者通过本地/网络的中间人代理监听窃取，造成应用的商业秘密泄露。

Analytics Kit 使用随机生成的密钥对上报的数据进行加密。同时采用 RSA 公钥对随机密钥加密，将上报数据密文和随机密钥密文一同上传服务器，防止恶意攻击者获取开发者应用的数据。

8.19.3 服务器数据隔离

Analytics Kit 在服务器的数据基于不同的开发者应用设置了隔离，保证不同开发者不同应用之间的数据不可相互访问。

8.20 动态标签管理器服务(Dynamic Tag Manager)

Dynamic Tag Manager（以下简称“DTM”）是一个动态代码标签管理系统（Tag Manager System），可帮助开发者快速配置和更新测量代码及相关代码片段，可以通过 Web 页面动态更新跟踪代码，轻松完成特定事件跟踪并将数据传送给第三方分析平台，实现营销数据随需监测。

DTM Kit 将对标签代码的来源进行校验，同时开放 API 限制代码的执行权限。DTM 云侧也将对不同开发者角色进行访问控制，不同开发者团队、不同应用之间代码隔离。同时 DTM 云侧对开发者提交的自定义模板配置进行校验。同时 DTM 还提供了标签代码预览调试、版本管理等机制，确保开发者及时发现异常的标签代码，并通过覆盖版本处理。

DTM 开发者需要在使用华为终端 DTM 以及处理与华为终端 DTM 相关的用户个人信息时遵循所有适用法律法规以及与华为终端达成的协议。开发者必须准确识别因使用 DTM 产品而可能收集、接收或使用最终用户个人信息的平台。开发者必须将平台告知最终用户并告知用户收集的最终用户个人信息以及收集数据的用途。此外，开发者须获取并保存最终用户对于例如 cookie 的使用或者类似的技术的合法同意，还需向最终用户提供撤销同意的能力。如果不遵守声明，华为终端可能会限制或暂停开发者使用 DTM 产品。开发者也不允许将可以识别个人身份的信息（如姓名、电子邮件地址、设备标识符或发票）上传到 DTM 服务器。另外，为了改进和维护 DTM 产品，我们可能会收集和处理用户如何使用 DTM 以及使用频率相关的信息。未经您的同意，我们不会与签约并代表我们的第三方以外的其他平台共享这些数据。

8.20.1 防仿冒

DTM Kit 通过 DTM 服务器证书验证，确保更新/下载的动态标签代码来自可信的 DTM 服务器。它将根据证书的签发者、有效期、域名等进行验证，防止服务器被仿冒。

8.20.2 有限的 API 代码执行权限

DTM Kit 开放的 API 执行权限有限，仅能通过 API 执行测量代码，完成特定事件的跟踪。DTM 对实现的 API 接口进行了严格的评审，不会获取设备的敏感权限和敏感信息。

8.20.3 动态标签代码安全管理

DTM 将对开发者提交的动态标签代码模板配置参数实行输入校验，防止恶意/异常标签代码模板入库。DTM 若发现存在违规或恶意动态标签代码的应用，可及时暂停该应用调用 DTM 的能力。

8.21 安全检测服务（Safety Detect）

Safety Detect 是华为终端推出的多维度安全检测开放服务，包括系统完整性检测、应用安全检测、恶意 URL 检测、虚假用户检测和恶意 Wi-Fi 检测能力，发挥华为手机独特优势，助力开发者快速构建应用安全。

系统完整性功能在设备本地检测，设备原始数据不会上报到服务器，仅检测结果会上报到服务器进行验证和数字签名。

应用安全仅在设备本地检测，用户已安装应用列表和应用不会上报到服务器。

恶意 URL 检测功能会上报 URL 到服务器进行检测。

虚假用户检测需要收集用户的华为帐号 ID 及设备 ID、IP 地址信息，这些信息在必要的时间内加密存储，不会分享给任何第三方。

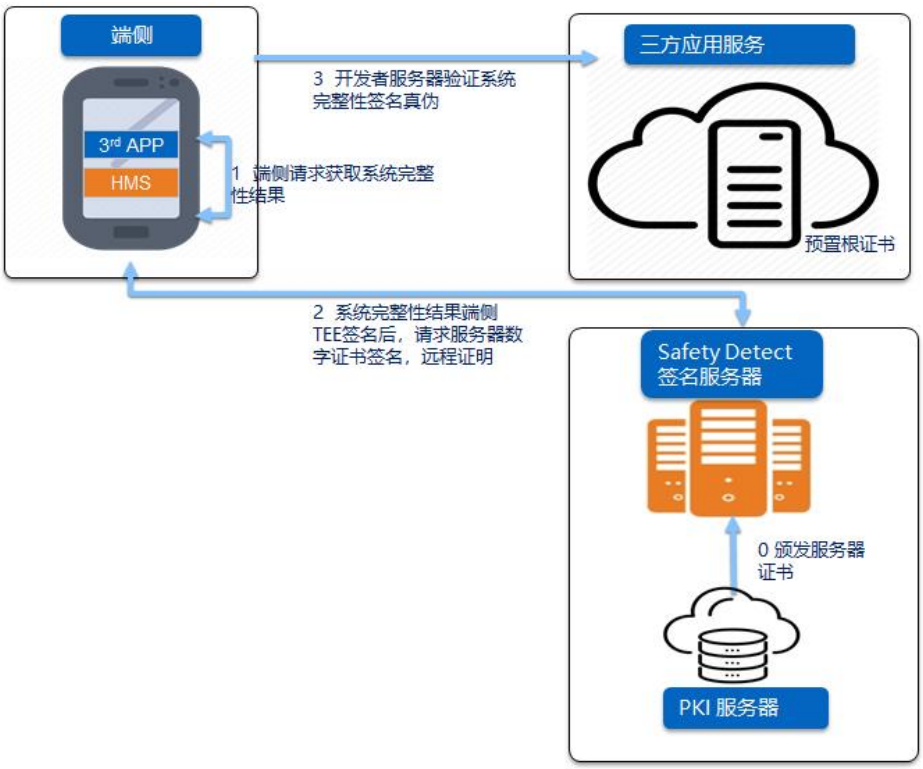
- SysIntegrity API：系统完整性检测 API，开发者可以通过该 API 评估应用运行的设备环境是否安全（如设备是否被 root）。
- AppsCheck API：恶意应用检测 API，开发者可以通过该 API 获取恶意应用列表。
- URLCheck API：恶意网址检测 API，开发者可以通过该 API 确定特定 URL 的威胁类型。
- UserDetect API：虚假用户检测 API，开发者可通过该 API 判断当前 App 的交互对象是否为虚假用户。
- WifiDetect API：恶意 Wi-Fi 检测 API，开发者可通过该 API 判断已连接的 Wi-Fi 对应用是否存在威胁。

8.21.1 系统完整性检测(SysIntegrity)

开发者在使用 Safety Detect SysIntegrity API 之前，必须确保在设备上安装了正确版本的 HMS Core 服务。如果您的应用检测到安装了错误的版本，则需要要求用户在其设备上更新 HMS Core 服务。

在调用 Safety Detect SysIntegrity API 时，开发者需传入一个 nonce 值。在检测结果中会包含这个 nonce 值，开发者可以通过校验 nonce 值确定返回结果与请求对应，避免重放攻击。Safety Detect SysIntegrity 接口包含 nonce 值和 AppID，该 AppID 在配置签名证书指纹步骤中获取。

SysIntegrity 为开发者提供安全可信的系统完整性检测。SysIntegrity 在手机的可信执行环境 TEE 中检测系统完整性，将检测结果在 TEE 中签名后，上传至 SysIntegrity 服务器请求签名并将签名后的系统检测结果返回开发者应用。开发者可以在自己的应用服务器上预置华为根证书，验证检测结果中的数字签名。



8.21.2 应用安全检测(AppsCheck)

AppsCheck 为开发者提供恶意应用列表，基于风险（风险应用/病毒应用）评估是否限制 App 行为，支持多达 14 种类型的恶意 App 检测和未知威胁检测能力。

8.21.3 恶意 URL 检测(URLCheck)

URLCheck 为开发者提供恶意 URL 检测能力，检测方式兼顾性能与时效性，支持钓鱼欺诈，网页挂马等恶意 URL 检测，为开发者提供集成简单、免运营、可信赖的安全服务，降低安全浏览服务的实现成本。

8.21.4 虚假用户检测(UserDetect)

UserDetect 为开发者提供虚假用户检测的能力。基于设备签名识别伪造设备；识别环节风险如 Root、模拟器、虚拟机、改机工具、匿名 IP；基于触屏行为、传感器行为分析识别虚假用户；基于图片和语义的验证码避免批量注册、撞库攻击、“薅羊毛”、内容爬虫等行为。

8.21.5 恶意 Wi-Fi 检测(WifiDetect)

WifiDetect 为开发者提供检测尝试连接的 Wi-Fi 及路由器特征，分析当前尝试访问的网络情况，通过聚类分析，实时反馈 Wi-Fi 检测结果，帮助应用防范来自恶意 Wi-Fi 的恶意行为攻击。

8.22 搜索服务（Search Kit）

Search Kit 通过端侧 SDK 和云侧 API 方式，全面开放 Petal Search 搜索能力，使能生态合作伙伴快速构建更好的移动应用搜索体验。

Search Kit 通过应用级客户端 ID 对访问进行接入认证，开发者可以对客户端 ID 设置 API 限制和 Access Token 的有效期设置，防止仿冒应用调用。

Search Kit 在应用打包时会被加载在您的应用当中，Search Kit 会随着应用的启动而启动。当用户关闭应用时，Search Kit 会随着应用的关闭而关闭，不会在后台做任何额外动作。

Search Kit 仅保存匿名化后的数据，该数据无法识别到最终用户，而且将在最多 6 个月内自动删除该数据数据。

采集数据本地加密，使用 HTTPS 安全协议，并在上报数据时加密传输。

8.23 DCI 版权服务（DCI Kit）

DCI 版权服务（Digital Copyright Identifier Kit，以下简称“DCI Kit”）是由华为和中国版权保护中心（即数字版权唯一标识符管理机构）合作，按照《中华人民共和国著作权法》、“数字版权唯一标识符”标准及相关规定，利用区块链和大数据、人工智能等技术，对数字作品版权进行保护，提供 DCI 版权服务用户注册、DCI 登记服务、DCI 维权服务等能力。DCI 登记成功的作品信息和版权权属确认信息将会保存在区块链中，保证所有的版权信息可信、可回溯。

8.23.1 服务端 API 接入控制

三方 CP 访问 DCI 版权服务服务端 API 时，需要向华为侧申请服务端接入证书，并将对应的应用 APPID 提供给华为添加到服务端的白名单中。访问对应的 API 时，需要按照接口入参要求，传入 nonce 值与时间戳来防止重放攻击，还需要对报文内容与报文头进行签名，DCI Kit 服务端对于签名进行验签，验签通过后才允许访问对应的 API 接口。

8.23.2 端侧 SDK 接入控制

DCI 版权服务提供 SDK 给三方开发者，便于开发者更方便的接入 DCI 版权服务。SDK 引入了华为帐号，用户需要申请对应的帐号接入 DCI 版权服务。在访问对应 API 接口时，服务端验证华为帐号的 Access Token，验证通过后才进行业务处理。

8.23.3 数字作品合法性校验

当用户上传数字作品进行 DCI 登记时，为了保证数字作品的合法性，DCI 版权服务利用人工智能与大数据技术对数字作品进行黄暴政检测，验证数字作品是否涉敏。通过提取数字作品的指纹信息在对应的图片向量特性库中检索相似的数字作品是否已经在域内库中已经登记，有效的解决图片被重复登记，版权被冒用的问题，保证了用户注册的数字作品合法、有效。

8.23.4 版权数据存储安全

DCI 版权服务将用户登记的版权信息存储在与中国版权保护中心共同创建的联盟链中（华为自研链）。利用区块链本身所采用的哈希、签名机制可以在开放的网络环境中保障账本数据的防篡改、可追溯。华为区块链服务还提供了范围可验证的同态加密解决方案，保障了用户交易过程中不泄露隐私信息。

8.24 钥匙环服务（Keyring）

钥匙环服务提供一组凭据管理接口，为用户认证凭据本地存储、跨应用、跨形态共享的能力，帮助开发者实现无缝登录的用户体验。

8.24.1 凭据安全存储

用户登录成功后，应用程序可以调用凭据管理接口，把用户的认证凭据保存 Keyring Kit 中。凭据在 Keyring Kit 中会被加密后存储在设备本地的存储中。保存凭据时，开发者可以设置读取凭据的内容时是否需要通过锁屏密码或生物特征认证用户的身份。

用户下次打开应用时，应用程序可以在 Keyring Kit 中查找可用的凭据，实现自动登录功能。

8.24.2 凭据共享

如果开发者的多个应用使用同一帐号体系，可以把某个应用的凭据授权给其他应用使用，只要用户登录了其中的一个应用，所有应用都可以无缝登录，不需要用户重复输入用户名和口令。开发者也可以在同一个应用的不同形态之间共享凭据，包括安卓应用、快应用、Web 应用形态。

凭据的共享关系完全由开发者进行控制。设置凭据的共享关系时，开发者必须明确指定目标应用的标识。共享给安卓应用和快应用时，需要指定应用的包名和证书指纹；共享给 Web 应用时，需要指定 Web 应用的完整域名。

9 隐私保护

9.1 隐私合规框架

我们将隐私保护作为产品设计的基石，把隐私保护的原则融入产品设计、开发、运营和运维的各个环节，持续优化产品与服务体验。同时，为了更好地满足全球范围内的隐私合规要求，我们在业界普遍认可的隐私框架（GAPP）的基础上，融入欧盟 GDPR 的隐私保护原则，并结合各国本地法律进行适配，构建了全球隐私合规框架，守护全球用户的数据安全。

9.2 本地化部署

我们通过遍布全球的资源和服务器提供产品与服务，确保用户的数据得到遵循法律和法规要求的充分保护。在法律要求服务器本地化部署及数据不得跨境转移的情况下，用户的数据留存于当地的服务器，并由注册在当地的子公司进行运营和运维，接受当地法律的监管。例如，对于中国大陆的用户，用户的个人信息将被存储于中国大陆境内的服务器；对于欧盟的用户，用户的个人信息存储于欧盟范围内的服务器。

9.3 数据最小化

我们坚持仅收集必要的个人信息，为用户提供所需的产品和服务，不收集与达到目的无关的个人信息。同时，我们采取了合理可行的措施，确保个人信息分享的最小化，防止个人信息被滥用，降低泄露风险。

9.4 数据端侧处理

得益于华为终端设备的超强处理能力，我们能够将数据保留在终端设备上，优先在终端设备上处理数据。除非实现某些功能或服务必须要将数据传到云端处理，用户的个人信息不会离开他的个人终端设备。

例如，华为钱包中的智闪卡服务，只在终端设备上处理用户的刷卡习惯和刷卡环境等数据，就能自动识别并快速唤起用户所需的卡片。智闪卡服务使用过程中，相关必要

的数据都不会离开用户的终端设备，在带来便捷体验的同时，很好地保护了用户的隐私。

9.5 透明可控

隐私是用户的基本权利。我们始终坚持，让用户清晰知道自己的个人信息将被如何使用、以及能够根据个人意愿自主进行决策，是隐私保护最基本的要求。

不管是首次使用应用还是开始使用某项新功能，我们都会明确地告知用户，该应用将会如何收集、使用、保存、共享和转让个人信息，并在获得用户同意之后才处理用户的个人信息。同时，为了让用户能够更好地理解我们如何处理个人信息，我们在华为应用市场推出了隐私标签，以标签化、瀑布流的形式为用户清晰呈现应用是如何使用个人信息的。

我们通过隐私工具提供了一站式的隐私管理平台，帮助用户更好地管理自己的个人信息和隐私设置。用户可以在线获取个人信息的副本、更正/删除帐号信息、决策是否向第三方应用授予帐户访问权限，以及设置对营销资讯的接收偏好等，更安心地使用华为的产品和服务。

9.6 身份保护

我们的产品和服务应用了多项创新的隐私保护技术，以最大限度减少我们或第三方接触用户的个人信息，帮助用户隐藏身份，甩掉网络跟踪者。

例如，我们在跟第三方合作的过程中，采用了随机标识符而不是用户 ID 关联个人信息，即使它们被发送到远程服务器，也不会跟用户本人相关联。我们的部分产品和服务中使用了差分隐私技术，并不会直接上传用户的原始数据，而是生成原始数据的摘要，并在摘要中添加随机噪声，使这些数据无法与用户相关联。隐私保护技术的应用能够帮助我们改进相关的服务和产品，同时避免收集与用户相关的数据，保护用户的身份。

9.7 数据安全保障

用户的个人信息安全，是我们产品设计的关键目标。

依托 HarmonyOS 提供的数据保护能力，结合安全芯片和可信执行环境（SE/TEE）提供的安全加密能力，使用华为帐号作为用户安全登录的入口后，我们在业务处理和数据交换过程中，充分使用业界领先的数据保护技术，在传输、业务处理和存储中，采用端到端加密、证书链信任关系认证、签名防止数据被篡改、信任环设备间互相信任等技术。

无论是在云上存储，还是在网络中传输，我们都会为用户的数据提供保护，阻止对用户个人信息进行未经授权的访问和篡改。

9.8 数据处理受托方义务

HMS Core 为开发者提供分析、Push 等服务，在这些服务中，开发者决定了数据处理的目的和使用方式；我们代表开发者收集并处理个人信息，为数据处理受托方。

我们与开发者签署数据处理协议（DPA），明确开发者和数据处理受托方的权利和义务。我们仅根据数据处理协议（DPA）和开发者的指令处理个人信息，不出于华为目的处理个人信息。当涉及数据处理活动分包时，使用提供足够技术/组织措施保证的供应商，供应商引入也会提前获取开发者的书面授权。

作为数据处理受托方，我们协助开发者响应行使数据主体（最终用户）权利的请求，并遵从个人信息处理、数据泄露通知、数据保护影响评估和事先咨询的要求。在结束开发者合作时，我们会删除或返回涉及的个人信息。同时，我们还会向开发者提供必要的信息，以显示对数据受托方义务的遵守情况，并提供审计/检查途径。

9.9 未成年人保护

对于使用华为终端云服务的未成年人，我们采取了额外的保障措施，保护未成年人的隐私和数据安全。我们提供了专为儿童量身打造的“儿童帐号”。通过创建并登陆华为儿童帐号，我们的产品和服务将自动开启儿童保护模式，从适龄内容筛选、屏蔽评论和网页内容推荐、屏蔽直接营销等多方面，隔绝不良侵扰、引导未成年人理性消费，给予未成年人无微不“智”的保护。

我们根据年龄为未成年人提供了定制化的内容分类分级，确保未成年人接触到的都是符合其年龄层次的内容。例如，华为应用市场提供 3 岁/7 岁/12 岁/16 岁/18 岁的分龄模式，孩子只能下载适龄应用，且无法查看和发表评论；华为视频分为儿童/青少年/成人模式，只呈现适龄内容以供未成年人访问。

我们仅在征得监护人同意后收集未成年人的个人信息，且只在法律允许、监护人明确同意或保护未成年人所必要的情况下使用或披露。监护人有权随时访问、修改或删除被监护人的个人信息，操作方法可参照具体产品及服务的隐私通知或补充声明。

10 安全和隐私认证及合规

10.1 ISO/IEC 27001/27018 认证

ISO/IEC 27001 信息安全管理体系是国际上针对信息安全领域，被广泛接受及应用的体系认证标准。该认证意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确的应对。HMS 于 2016 年 1 月首次通过此认证，并每年完成年度复核，其中 2019 年完成换证审核，证书通过 ANAB 和 UKAS 权威认可。

ISO/IEC 27018 专注于云中个人信息保护的国际行为准则。它基于 ISO 信息安全标准 ISO 27002，并针对适用于公有云个人可识别信息 (PII) ISO 27002 控制体系提供了实施指南，以确保个人身份信息（PII）资料在经由云个人身份信息处理者处理时得到适当保护，从而为在多国市场运营的云服务提供商提供一个共同合规框架。HMS 于 2019 年 10 月通过此认证，并每年完成年度复核。

10.2 ISO/IEC 27701 认证

ISO/IEC 27701 隐私信息管理体系从组织治理、法律合规、流程规范、信息技术、监督审计等多个维度，提供了一套完整的个人信息处理方法和隐私信息管理的框架。该认证意味着在持续优化设计、研发、运营和运维服务等环节，已经拥有完备的个人信息保护管理体系，在个人信息安全管理、透明性和隐私合规等方面都处于全球领先水平。HMS 于 2019 年 11 月作为行业首批通过此认证产品，并每年年度复核，当前证书已通过 ANAB 权威认可。

10.3 CSA STAR 认证

CSA STAR 认证是在 ISO/IEC 27001 的基础上，增加了云安全控制矩阵（CCM－Cloud Control Matrix）和其他安全要求，涵盖了风险治理、数据安全、应用安全、基础设施安全、开发和设计、身份和访问管理、数据中心安全、变更管理、配置管理、业务连续性管理、运营恢复力、人力资源、供应链管理等方面的 16 个控制领域。HMS 于 2016 年 1 月首次通过此认证，并每年完成年度复核，其中 2019 年完成换证审核，审核报告通过 GOLD 级。

10.4 CC 认证

CC(Common Criteria)认证是全球认可度高的产品信息安全认证，在全球 31 个国家受到广泛认可。CC 认证有 7 个等级（EAL1-EAL7），级别越高，审核过程越严苛细致，表明产品的安全保障越全面。

TEE(安全可信执行环境) OS 的内核于 2019 年 9 月通过 CC EAL5+认证，EAL5+是商用 OS 内核安全认证，意味着华为手机用户在应用使用过程中的指纹、人脸、锁屏密码等敏感数据得到妥善保护。

10.5 PCI DSS 认证

PCI DSS（Payment Card Industry Data Security Standards）认证是目前全球高级别的金融数据安全标准之一、权威的支付卡产业数据安全标准之一，旨在严格控制数据存储以保障支付卡用户在线交易安全。该标准得到了全球卡组织和金融机构的广泛支持和推广，成为商户和服务提供商必须遵循的一项规范。华为钱包中的应用内支付服务（IAP）于 2018 年 1 月通过此认证，并每年完成年度复核。

10.6 华为帐号 EuroPriSe 认证

2020 年 1 月，欧洲隐私保护认证组织 EuroPriSe 向 Aspiegel Limited（Huawei Technologies Cooperatief U.A (Netherlands)的全资子公司）在欧盟和欧洲经济区提供的 HUAWEI ID 服务授予了 European Privacy Seal 证书。EuroPriSe 提供由独立第三方颁发的欧洲隐私信任标志，用于证明 IT 产品和基于 IT 的服务符合欧洲隐私和数据安全法规。EuroPriSe 提供了透明的程序和可靠的标准。

10.7 ePrivacyseal 认证

ePrivacyseal 是欧洲权威隐私认证，认证涵盖了数字产品的通用数据保护法规 GDPR（General Data Protection Regulation“通用数据保护条例”）的要求，认证标准目录也不断适应 GDPR 和其他数据保护法律的解释。ePrivacyseal 从法律和技术两个维度对认证对象进行评估，意味着认证对象可更好的遵守 GDPR，保护消费者隐私安全。面向 EEA 提供的广告、Petal 搜索、应用市场、华为帐号、Huawei AppGallery Connect 都已于 2020 年 7 月获得由德国 ePrivacyseal Gmbh 认证颁发证书。

10.8 网络安全等级保护

网络安全等级保护制度是国家的基本国策、基本制度和基本方法。网络安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，消费者云服务业务通过了公安部的网络安全等级保护 3 级备案和测评，严格遵循国家在移动应用安全建设方面的技术保障要求和安全管理要求。

11 展望

11.1 关注安全技术，保护用户并对用户赋能

用户的数据安全和隐私保护是 HMS 一直以来的工作重心。为了提升业务的用户体验，华为终端云服务将走向原子化、智慧化，为用户带来直达、便捷的服务结果，构建智慧的服务分发平台。广泛的应用大数据、机器学习、AI 等技术，积极面对隐私保护和数据安全的挑战。

我们持续致力于帮助用户提高效率，同时保护他们的安全和隐私。在保持业务可用性的同时，对安全和隐私解决方案的创新非常重要。安全和隐私解决方案的实现通常依赖于基础技术的使用和研究。需要持续研究数据保护技术。这些技术通过客户端加密和端到端加密，使用多方计算、同态加密、差分隐私、函数加密，以及基于 AI 的隐私保护技术（如联合学习）确保数据安全。

此外，需要支持安全协作，用户数据在传输到云之前已经在客户端进行保护，以便用户能够对各场景中谁有权访问其数据进行完全控制。也需要在零信任环境中管理数据的方法。随着 AI 应用的日益广泛，防止 AI 的对抗性、防止因成员推理导致的隐私泄露以及确保 AI 的可解释性至关重要，从而构建用户所依赖的强健 AI 系统。

另一个重要方面是从可用性的角度来探讨如何增进用户的理解，并在使用应用之前、期间和之后对用户提供帮助。很明显，需要找到可用的解决方案，帮助用户了解服务会收集和生成哪些数据，以及这些数据在不同组织内部和组织之间被广泛使用和披露的程度，并让用户能够控制这些数据。

开发者要能够通过各种方法（例如隐私印章）证明其解决方案的安全和隐私保护能力，从而在开发的应用/服务与用户之间建立信任。

11.2 巩固防御机制，提升安全能力，共建安全生态

安全是一项长期持续的工作。新兴的攻击向量、快速的技术发展以及业务运作模式或立法的改变总会带来新的安全与隐私威胁。我们持续投入先进的检测技术，保护基础设施、系统、设备、应用和数据。我们与各安全伙伴合作，增强系统、Web、应用和设备级的异常检测。

同时，确保生态系统不包含非法、有害、不当和侵犯版权的内容，构建可信、符合伦理、安全的生态系统。

HMS 通过深入构建开放 HMS Core 安全能力，持续增强 SafetyDetect 中的系统完整性检测、应用安全检测、恶意 URL 检测、虚假用户检测等服务，助力开发者提供更加安全的开发者应用。

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 安全应急响应中心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，并发布漏洞预警和推送补丁更新。

11.3 做好准备，应对颠覆性技术带来的威胁

我们提前做好准备以应对颠覆性技术带来的不可预见的威胁。同时，这些技术可能会带来新机遇，重塑解决方案。例如，由于量子计算技术的突破，在后量子时代，公钥密码术将被打破，并影响当前基于公钥密码术的技术（例如 HTTPS、密钥管理、签名等）。

换脸技术利用机器学习和 AI 生成欺骗性的图像或视频，普通用户很难区分真假。这可能会误导用户或导致滥用，影响个人的上网安全。

我们相信，必须与学术合作伙伴携手合作，应对在实现为用户创造安全生态系统的使命中遇到的挑战。

12 缩略语表

英文缩写	英文全称	中文全称	说明
ADSS	Account Data Security Standard	帐户数据安全标准	由中国银联风险管理委员会审核通过，旨在加强银联卡收单网络账户信息安全管理，进一步明确和细化对收单业务各参与方账户信息安全管理要求，防范账户信息泄漏风险
AES	Advanced Encryption Standard	高级加密标准	密码学中的高级加密标准（Advanced Encryption Standard，AES），又称 Rijndael 加密法，是一种区块加密标准
AI	Artificial Intelligence	人工智能	研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学
AIDL	Android Interface Definition Language	安卓接口定义语言	可以跨进程访问的服务
API	Application Programming Interface	应用程序接口	API 是一些预先定义的函数，或指软件系统不同组成部分衔接的约定。 目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问原码，或理解内部工作机制的细节
App	Application	应用程序	安装在智能手机上的软件
APT	Advanced Persistent Threat	高级可持续威胁攻击	使用复杂精密的恶意软件及技术以利用系统中的漏洞

英文缩写	英文全称	中文全称	说明
ARM	Advanced RISC Machines	高级精简指令集架构	32 位精简指令集（RISC）处理器架构
CA	Certificate Authority	证书颁发机构	作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任
CBC	Cipher Block Chaining	密文分组链接	在 CBC 模式中，每个明文块先与前一个密文块进行异或后，再进行加密
CC	Challenge Collapsar Attack	CC 攻击	攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装
CCM	Counter with CBC-MAC	使用 CBC-MAC 的计数方式	一种经典的构造 MAC 的方法
CCS	Cloud Certificate Service	云证书管理服务	提供业务证书在线（离线）签发，注销，冻结，状态查询等证书管理服务
CERT	Computer Emergency Response Team	计算机安全应急响应团队	对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，来保证计算机信息系统和网络免遭破坏
CPU	Central Processing Unit	中央处理器	中央处理器作为计算机系统的运算和控制核心，是信息处理、程序运行的最终执行单元
CSRF	Cross-Site Request Forgery	跨站请求伪造	一种挟制用户在当前已登录的 Web 应用程序上执行非本意的操作的攻击方法
CVV	CardVerificationValue	信用卡验证值	印在信用卡背面的附加码
DBF	Database Firewall	数据库防火墙	一款基于数据库协议分析与控制技术的数据库安全防护系统
DDoS	Distributed denial of service attack	分布式拒绝服务攻击	处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击
DES	Data Encryption	数据加密标准	一种使用密钥加密的块算法

英文缩写	英文全称	中文全称	说明
	Standard		
DEP	Data Execution Prevention	数据执行保护	防止应用运行用于暂存指令的那部分内存中的数据，从而保护电脑
DMZ	Demilitarized Zone	隔离区	一个非安全系统与安全系统之间的缓冲区
DPA	Data Processing Agreement	数据处理协议	数据控制者与数据处理者，或数据处理者与子数据处理者之间签署的安全隐私协议，反映双方在个人信息处理过程中需要履行的责任和义务。
DRM	Digital Rights Management	数字版权管理	一种加强保护数字化的音视频节目内容，文档、电子书籍的版权的技术
DTM	Dynamic Tag Manager	动态代码标签管理系统	动态代码标签管理系统（Tag Manager System），可帮助开发者快速配置和更新测量代码及相关代码片段，可以通过 Web 页面动态更新跟踪代码，轻松完成特定事件跟踪并将数据传送给第三方分析平台，实现营销数据随需监测。
ECC	Elliptic Curves Cryptography	椭圆曲线密码编码学	一种建立公开密钥加密的演算法，基于椭圆曲线数学
EMUI	Emotion UI	华为 EMUI 系统	华为基于 Android 进行开发的操作系统
Harmony OS	HarmonyOS	HarmonyOS 系统	HarmonyOS 是新一代的智能终端操作系统
FIPS	Federal Information Processing Standards	联邦信息处理标准	用于政府机关的自动化数据处理和远程通信标准
GCM	Galois/Counter Mode	采用 Counter 模式的加密方式	对称加密算法分组密码的一种工作模式
GDPR	General Data Protection Regulation	通用数据保护条例	任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织均受该条例的约束
HDCP	high bandwidth digital content	高带宽数字内容保护技术	保护未经压缩的数字音视频内容

英文缩写	英文全称	中文全称	说明
	protection		
HDMI	High Definition Multimedia Interface	高清多媒体接口	一种全数字化视频和声音发送接口，可以发送未压缩的音频及视频信号
HIPS	Host Intrusion Prevention System	主机入侵防护系统	一套采用 C/S 结构的主机安全系统，可以及时发现服务器系统上的安全问题并解决，以保证服务器系统的安全运营。
HMS	Huawei Mobile Service	华为终端云服务	华为终端云服务提供端、云开放能力的合集，助力开发者实现应用高效开发、快速增长、灵活变现。
HMAC	Hashed message Authentication Code	哈希信息认证码	一种基于 Hash 函数和密钥进行消息认证的方法
HTML	HyperText Markup Language	超级文本标记语言	一种标识性的语言，包括一系列标签．通过这些标签可以将网络上的文档格式统一，使分散的 Internet 资源连接为一个逻辑整体
IAP	In-App Purchases	应用内支付	为应用提供便捷的应用内支付体验
IDS/IPS	Intrusion Detection System / Intrusion Prevention System	入侵检测系统/入侵防御系统	IDS：一种对网络传输进行即时监测，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备 IPS：一部能够监测网络或网络设备的网络资料传输行为的计算机网络安全设备，能够及时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。
IM	Instant Messaging	即时通讯	一种基于互联网的即时交流消息的业务
IMEI	International Mobile Equipment Identity	国际移动设备识别码	用于在移动电话网络中识别每一部独立的手机等移动通信设备，相当于移动电话的身份证
KMS	Key Message Service	密钥管理服务	KMS 给用户/业务提供密钥管理的能力。KMS 给每个业务分配一对由加密机加密保护的

英文缩写	英文全称	中文全称	说明
			Master Key，最终通过 HKDF 算法提取出最终的用户和业务密钥。
NFC	Near Field Communication	近距离无线通信	一种短距高频的无线电技术，可以在设备彼此靠近的情况下进行数据交换
OOBE	Out-Of-Box Experience	系统初始化阶段	在安装完 Windows 后就会进行的一个步骤，对 Windows 进行一些基本设置。
PCI-DSS	Payment Card Industry Data Security Standard	支付卡行业数据安全标准	对于所有涉及信用卡信息机构的安全方面作出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。
PBKDF2	Password-Based Key Derivation Function 2	基于密码的密钥派生功能 2	应用一个伪随机函数以导出密钥
PKI	Public Key Infrastructure	公钥基础设施	一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能
POS	Point Of Sale	销售终端	一种多功能终端，把它安装在信用卡的特约商户和受理网点中与计算机联成网络，就能实现电子资金自动转账
PSIRT	Product Security Incident Response Team	产品安全应急响应团队	负责接受、处理和公开披露华为产品和解决方案相关的安全漏洞
RASP	Runtime Application self-protection	应用程序运行时自我保护	RSAP 将自身注入到应用程序中，与应用程序融为一体，实时监测、阻断攻击，使程序自身拥有自保护的能力。
RBAC	Role-Based Access Control	基于角色的访问控制	面向企业安全策略的一种有效的访问控制方式
RSA	Rivest Shamir Adleman	公开密钥密码体制	使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

英文缩写	英文全称	中文全称	说明
SD	Secure Digital Memory Card	安全数字存储卡	一种基于半导体快闪记忆器的新一代记忆设备
SDK	Software Development Kit	软件开发工具包	软件工程师为特定的软件包、软件框架、硬件平台、操作系统等建立应用软件时的开发工具的集合
SHA	Secure Hash Algorithm	安全哈希算法	一个密码散列函数家族，是FIPS 所认证的安全散列算法。能计算出一个数字消息所对应到的，长度固定的字符串（又称消息摘要）的算法。
SIM	Subscriber Identity Module	用户识别模块	GSM 系统的移动用户所持有的 IC 卡，称为用户识别卡
SSL	Security Socket Layer	安全套接层	广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输，利用数据加密(Encryption)技术，可确保数据在网络上的传输过程中不会被截取及窃听
TCIS	Trust Circle Index Service	信任环	TCIS 服务器是信任服务中用来管理公钥信息的服务器组件。基于 Internet 的适用性，采用 WEB 方式提供所有服务。
TEE	Trusted Execution Environment	可信执行环境	特指运行在安全世界（如TrustZone）的操作系统及可信应用程序
TLS	Transport Layer Security	安全传输层协议	用于在两个通信应用程序之间提供保密性和数据完整性
VLAN	Virtual Local Area Network	虚拟局域网	一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样
VPN	Virtual Private Network	虚拟专用网	在公用网络上建立专用网络，进行加密通讯
XMPP	Extensible Messaging and	可扩展通讯和表示协议	一种基于标准通用标记语言的子集 XML 的协议

英文缩写	英文全称	中文全称	说明
	Presence Protocol		
XSS	Cross Site Scripting	跨站脚本攻击	利用网站漏洞从用户那里恶意盗取信息

