HUAWEI

HarmonyOS 6.0

安全技术白皮书

发布日期

2026-4

目录 CONTENTS

前言

01

HarmonyOS 是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。其典型的技术特征是：

- 提供分布式软总线，将所有构成超级终端的设备可信安全的连接起来；
- 通过将所有设备的资源进行虚拟池化管理，使得分布式超级终端上任意设备、任意应用能够像使用本地资源一样访问跨设备的资源；
- 通过分布式数据管理，将不同设备上的数据资源进行统一管理，使得分布式超级终端上的任意设备、任意应用能够像访问本地文件 / 数据一样访问跨设备的文件 / 数据；
- 通过分布式任务调度，将传统移动应用的单体（Monolithic）结构进行服务化改造，使得应用程序的运行可以不局限于单个设备，而是可以远程启动、远程调用、远程连接以及迁移等操作，能够根据不同设备的能力、位置、业务运行状态、资源使用情况，以及用户的习惯和意图，选择合适的设备运行分布式任务。

HarmonyOS 为整个生态体系带来的全新体验和价值体现在：

- 对消费者而言，HarmonyOS 能够将生活场景中的各类终端进行能力整合，可以实现不同的终端设备之间的快速连接、能力互助、资源共享，匹配合适的设备、提供流畅的全场景体验。
- 对应用开发者而言，HarmonyOS 采用了多种分布式技术，使得应用程序的开发实现与不同终端设备的形态差异无关。这能够让开发者聚焦上层业务逻辑，更加便捷、高效地开发应用。
- 对设备开发者而言，HarmonyOS 采用了组件化的设计方案，可以根据设备的资源能力和业务特征进行灵活裁剪，满足不同形态的终端设备对于操作系统的要求。

HarmonyOS 为整个生态提供了一套便捷高效的系统，然而对于用户隐私与网络安全保护来说，却提出了更高的要求，主要体现在：

- **分布式软总线：**将所有设备组合形成 HarmonyOS 分布式超级终端，设备间形成了一种“默认信任”的安全模型，带来互相“污染”，攻击者只需要突破一台设备，就有机会作为跳板去攻击其他设备。
- **分布式数据管理:** 文件和数据的无缝流转，数据安全防护机制要从单设备转移到对整个分布式系统的防护，难度增大。
- **智慧原子化服务 / 分布式任务调度：**应用程序从单体 APP，变成分布式智慧原子化服务，且原子化服务可以在不同设备间互相调用和跨设备运行，使应用程序的权限控制、沙箱隔离等机制变得更加复杂。

为了应对这些全新的安全要求，HarmonyOS 提出了一套基于分级安全理论体系的安全架构，围绕“正确的人，通过正确的设备，正确的访问数据”，来构建一套新的纯净应用和有序透明的生态秩序，为消费者和开发者带来安全分布式协同、严格隐私保护与数据安全的全新体验。

本文详细介绍了 HarmonyOS 系统中的安全性技术和功能。在本文的帮助下， 一方面安全从业人员可以理解 HarmonyOS 安全的具体实现，另一方面 HarmonyOS 开发者能够将 HarmonyOS 平台提供的安全能力与开发者的程序良好结合，实现保障消费者数据的隐私和安全的目的。

本文主要从以下几个章节进行阐述：

- 第一章：前言，简明扼要的说明了 HarmonyOS 的定位、显著的技术特征、为生态带来的全新价值和面临的安全风险与应对措施。
- 第二章：HarmonyOS 概述，介绍了 HarmonyOS 显著的典型体系架构，对 HarmonyOS 有别于传统移动操作系统和桌面操作系统的典型技术方案做了简单的阐述，同时对 HarmonyOS 面临的主要安全风险做了简要介绍。
- 第三章：HarmonyOS 安全理论模型，介绍了 HarmonyOS 核心的安全架构模型：基于分级安全理论的安全访问控制模型，对数据隐私机密性保护的 BLP 模型和对系统完整性保护的 Biba 模型
- 第四章：HarmonyOS“正确的人”身份管理与认证，介绍了在应用生命周期治理中，对开发者、消费者自然人、应用程序、设备等主体（Subject）的身份管理、身份认证机制进行了介绍，围绕“零信任网络架构”为 HarmonyOS 分布式系统构建一套具有韧性（Resilience）的安全能力。
- 第五章：HarmonyOS“正确的设备”系统安全架构，HarmonyOS 系统安全采用了芯 – 端 – 云垂直整合的架构，根植于信任根（芯片信任根、云服务等），以基础安全工程能力为依托，重点围绕系统完整性保护、隔离和访问控制、漏洞防利构建相关的安全技术和能力。
- 第六章：HarmonyOS“正确的访问数据”分级访问控制架构，在“零信任网络架构”“分级系统安全架构”基础上，结合消费者个人隐私敏感数据访问、GDPR 等安全隐私保护要求，形成了一套基于用户分级、应用分级、设备分级、数据分级的访问控制模型，基于场景目标设计的“一应用一密钥”的通断架构，基于芯片与硬件级的防监听与防跟踪能力，以极致保护消费者隐私数据为目标，最终实现分级安全理论提出的机密性 BLP 模型和完整性 Biba 模型。
- 第七章：HarmonyOS 个人智能计算隐私安全架构，介绍了云助端算场景下，围绕非结构化数据推理计算场景，将终端芯片级的安全能力延伸至云端，为用户数据构建从生成、传输、计算到销毁的全生命周期保护方案，旨在为 AI 时代的个人用户，构建一个安全、私密、透明的智能计算环境。
- 第八章：HarmonyOS 生态治理架构，以保证 HarmonyOS 软件生命周期可信为目标，围绕全栈代码签名、基于 AT Token 的应用权限最小化设计、基于 SEHarmony 的内核权限最小化设计、以 System Picker 为特征的“基于场景授权，不打断用户体验”的全新隐私保护框架，阐述了 HarmonyOS 面向应用和设备的

纯净生态治理架构，最大限度的保护消费者的隐私，最大程度的保护开发者的利益，最终实现“生而纯净，一生纯净”。

- 第九章：HarmonyOS 安全标准遵从与认证，介绍了 HarmonyOS 针对全球各国隐私安全法律合规遵从、标准遵从，并系统性介绍 HarmonyOS 获得全球主流安全认证的测评认可情况。

- 第十章：HarmonyOS 高安全业务能力介绍，通过对诸如 HUAWEI Pay、手机盾、电子身份证、车钥匙等高级安全特性的介绍，以场景化、实例化的形式，系统性介绍应用和业务如何基于 HarmonyOS 提供的安全能力，来构建高安全的业务系统，最大限度的保护消费者的隐私、财产和数据。

- 第十一章：构建具备韧性的 HarmonyOS 安全体系架构，参考了零信任网络架构、Cyber Resilience 网络韧性架构等前沿的安全架构，介绍了 HarmonyOS 的安全可信工程能力、安全研究奇点实验室、安全漏洞奖励计划和安全应急响应流程和机制，确保 HarmonyOS“尽可能保证没有安全漏洞，存在漏洞时通过纵深防御确保漏洞难以被利用，在漏洞发生后最快速度恢复业务和修复漏洞”

- 第十二章：HarmonyOS 安全能力开放使能生态，介绍了 HarmonyOS 提供的安全基础服务，并通过 API、Kit、SDK 的形式使能开发者。

缩略语表

HarmonyOS 概述

02

2.1 HarmonyOS 简介

HarmonyOS 是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 是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，为用户带来简捷，流畅，连续，安全可靠的全场景交互体验。HarmonyOS 三大技术理念：一次开发，多端部署；可分可合，自由流转；统一生态，原生智能。

HarmonyOS 通过应用开发、应用发布、应用安装运行三个阶段，构建关键安全能力，从始至终贯彻应用安全核心理念，帮助开发者快速理解 HarmonyOS 生态应用安全设计，提升应用开发的安全质量。

2.2 HarmonyOS 技术特征

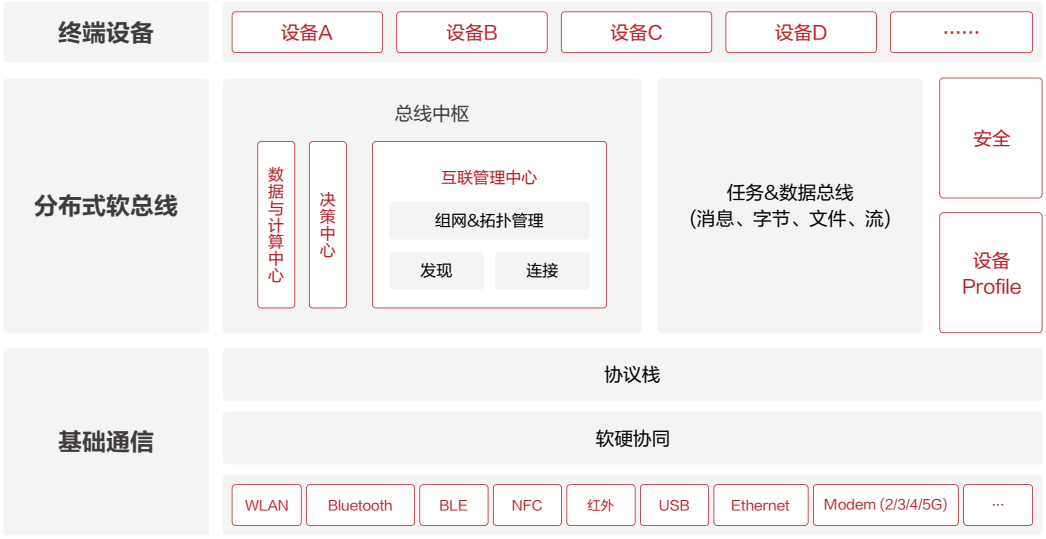
HarmonyOS 是一款面向多设备智能协同的分布式操作系统，将消费者多个设备安全的连接起来，搭建统一的分布式跨设备开发平台，使得消费者在分布式智能全场景中接触到的多种智能终端能够有机融合，呈现为一个完整统一的整体，为消费者提供好像是在使用一部“超级大终端（One Super Device）”的体验，系统性地解决了多终端环境下消费者体验不佳和开发者效率低下的问题。

HarmonyOS 系统是一款“面向未来”、面向全场景（移动办公、运动健康、社交通信、媒体娱乐等）的分布式操作系统。在传统的单设备系统能力的基础上，HarmonyOS 提出了基于同一套系统能力、适配多种终端形态的分布式理念，能够支持多种终端设备。

分布式软总线

分布式软总线是手机、智能穿戴、平板、智慧屏、车机等多种终端设备的统一基座，为设备之间的互联互通提供了统一的分布式通信能力，能够快速发现并连接设备，高效地分发任务和传输数据。分布式软总线示意图 2-1 分布式软总线示意图。

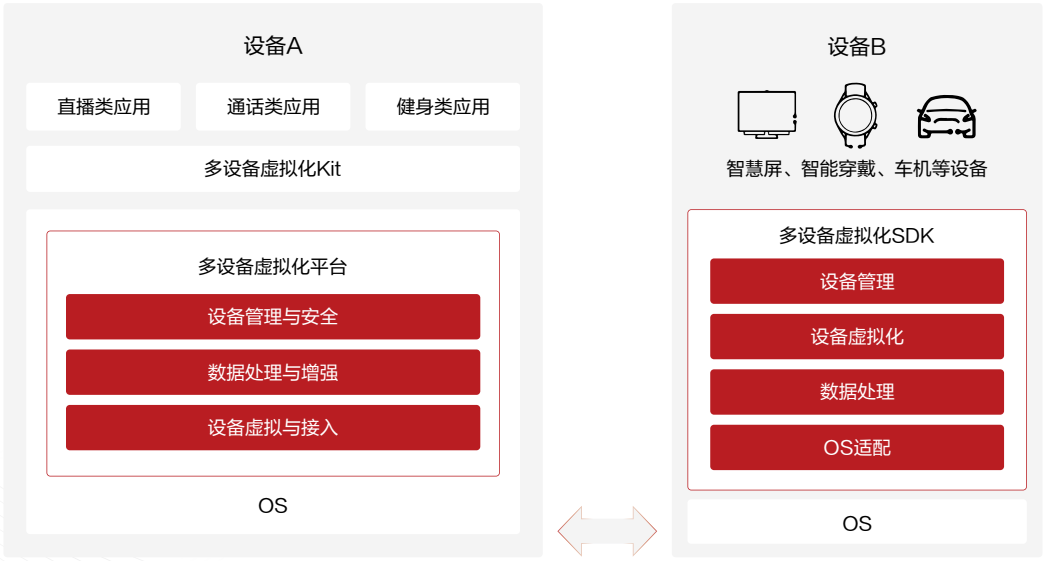
图 2-1 分布式软总线示意图



分布式设备虚拟化

分布式设备虚拟化平台可以实现不同设备的资源融合、设备管理、数据处理，多种设备共同形成一个超级虚拟终端。针对不同类型的任务，为用户匹配并选择能力合适的执行硬件，让业务连续地在不同设备间流转，充分发挥不同设备的资源优势。分布式设备虚拟化示意图见图 2-2 分布式设备虚拟化示意图。

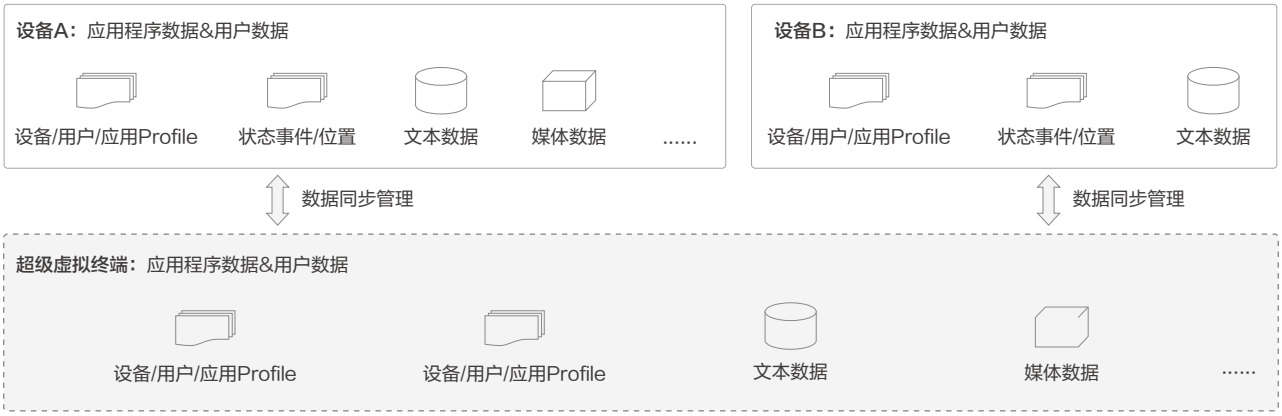
图 2-2 分布式设备虚拟化示意图



分布式数据管理

分布式数据管理基于分布式软总线的能力，实现应用程序数据和用户数据的分布式管理。用户数据不再与单一物理设备绑定，业务逻辑与数据存储分离，应用跨设备运行时数据无缝衔接，为打造一致、流畅的用户体验创造了基础条件。分布式数据管理示意图见 图 2-3 分布式数据管理示意图

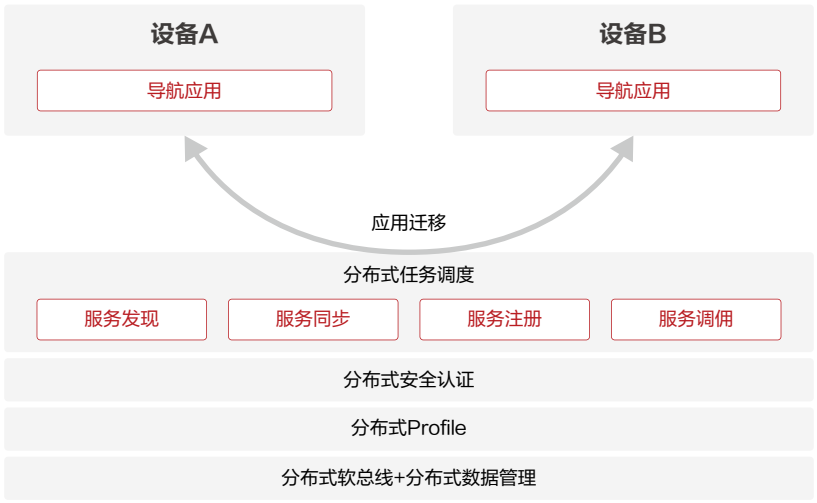
图 2-3 分布式数据管理示意图



分布式任务调度

分布式任务调度基于分布式软总线、分布式数据管理等技术特性，构建统一的分布式服务管理（发现、同步、注册、调用）机制，支持对跨设备的应用进行远程启动、远程调用、远程连接以及迁移等操作，能够根据不同设备的能力、位置、业务运行状态、资源使用情况，以及用户的习惯和意图，选择合适的设备运行分布式任务。

图 2-4 分布式任务调度示意图



2.3 HarmonyOS 安全风险评估

基于安全风险评估模型：风险 = 资产 * 威胁，结合 HarmonyOS 的分布式架构特征，我们对 HarmonyOS 的安全风险进行简要介绍。

1.HarmonyOS 关键资产

- 设备资源池化后的各种硬件、传感器资源
- 消费者隐私敏感的数据资源
- 应用程序独占的数据资源
- 设备 OS、Firmware 等关键数据

2.HarmonyOS 关键威胁

- 设备资源滥用：如摄像头、麦克风、位置信息等，被滥用带来的个人隐私跟踪、窃听等
- 消费者数据的泄露，造成个人数据泄露、隐私泄露
- 应用程序数据泄露，导致开发者利益受损
- 针对 OS、Firmware 等的篡改程序逻辑和数据、植入木马、劫持控制等的攻击

3.HarmonyOS 关键安全风险

- **分布式超级终端安全能力强弱不均带来的风险**：所有设备组合形成 HarmonyOS 分布式超级终端，设备间形成了一种“默认信任”的安全模型，一个设备和另一个设备一旦建立了安全可信连接，就可能带来互相“污染”，攻击者只需要突破一台设备，就有机会作为跳板去攻击其他设备。

- **分布式数据管理的数据安全与隐私泄露风险**：基于分布式数据管理平台，能够方便文件和数据的无缝流转，但是也使得传统在单机终端上的用户隐私保护和数据安全机制面临严重挑战，数据安全防护机制要从单设备转移到对整个分布式系统的防护，任何一个环节如果发现安全防护能力不足，都可能成为攻击的切入口。

- **智慧原子化服务 / 分布式任务调度**：应用程序从单体 APP，变成分布式智慧原子化服务，且原子化服务可以在不同设备间互相调用和跨设备运行，使应用程序的权限控制、沙箱隔离等机制变得更加复杂。

HarmonyOS 安全理论模型

03

1985 年美国国防部发布的计算机安全橘皮书（TCSEC）将系统安全划分成了如下七个等级：D、C1、C2、B1、B2、B3 及 A1。橘皮书也成为计算机安全分级标准流传最广泛、被多个国家吸纳成为安全标准、被广泛认可的划分方法。

随着安全测评技术的发展，CC（Common Criteria）建立起了一套系统性的安全测评标准和技术方法，通常认为，CC 的分级方法与橘皮书的安全等级间也建立起了相当的映射关系。CC 将安全测评认证等级划分成 EAL1~EAL7 一共七级，和橘皮书的 D~A1 一一对应。

HarmonyOS 在 IoT 时代将所有分布式设备连接起来，由于涉及到大量的用户数据安全和隐私保护，同时甚至涉及到个人生命财产安全（如智能门锁），其安全等级要求必然很高。

在充分评估了系统安全性和产品易用性、用户体验后，我们选择了以橘皮书 B2 级、CC EAL5 级为目标的安全架构，HarmonyOS 的核心安全理论模型是分级安全理论，通过结构化的保护机制，主体在访问客体的时候，需要遵循的安全模型主要是两个：

- **机密性模型：Bell-Lapadula 模型**
- **完整性模型：Biba 模型**

下面详细阐述 HarmonyOS 的安全架构模型：

3.1 计算机安全等级模型

根据 TCSEC 计算机安全橘皮书，计算机安全被分成了以下七级：

等级	描述
A1	可验证的设计，必须采用严格的形式化方法来证明该系统的安全性
B3	B3 级要求用户工作站或终端通过可信任途径连接网络系统，这一级必须采用硬件来保护安全系统的存储区
B2	结构化保护，B2 级安全要求计算机系统中所有对象加标签，而且给设备（如家庭中枢、控制设备和 IoT 设备）分配安全级别
B1	B1 级系统支持多级安全（MLS）模型

等级	描述
C2	C2 级引进了受控访问环境（用户权限级别）的增强特性，如 RBAC 基于角色访问控制
C1	C1 级系统要求硬件有一定的安全机制，具有完全访问控制的能力，不足之处是没有权限等级划分
D1	D1 级计算机系统标准规定对用户没有验证，也就是任何人都可以使用该计算机系统

同时，为了与 TCSEC 的等级模型匹配，CC 组织定义了 EAL1~EAL7 的七级认证测评模型，来和 D~A1 等级映射：

EAL	Name	TCSEC
EAL1	Functionally Tested	
EAL2	Structurally Tested	C1
EAL3	Methodically Tested and Checked	C2
EAL4	Methodically Designed, Tested, and Reviewed	B1
EAL5	Semiformally Designed and Tested	B2
EAL6	Semiformally Verified Design and Tested	B3
EAL7	Formally Verified Design and Tested	A1

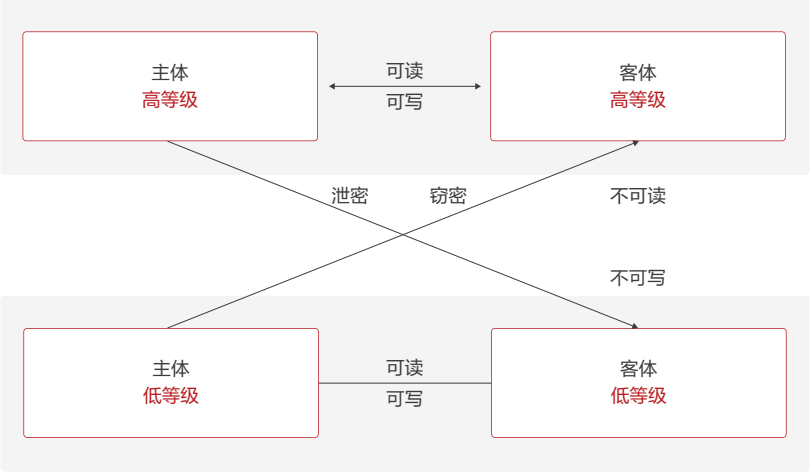
在主流的操作系统中，MS-DOS 大体在 D 级，Windows NT/UNIX 大体在 C1~C2 级水平，B1 级采用多级安全模型，它对敏感信息提供更高级的保护，例如安全级别可以分为秘密、机密和绝密级别。B2 级安全要求计算机系统中所有对象加标签，包括主体、环境、客体进行严格的标记，在严格的标签等级基础上，来实施机密性和完整性保护。

HarmonyOS 立志成为最严格保护用户数据和隐私的操作系统，严格保护消费者智能终端安全，确保关键数据在系统攻陷后仍然不会泄露。因此，HarmonyOS 选择了在整体达到 B2 级水平，在关键数据如消费者生物认证特征数据、支付、电子身份证、银行卡盾等数据，通过 B3 级专用安全芯片和处理器来存储和处理，对关键的 TEE OS 采用达到 A1 级的形式化验证技术来证明安全性。

3.2 机密性保护 BLP 模型

1973 年，D. E. Bell 和 L. J. LaPadula 将军事领域的访问控制规则形式化为 Bell&LaPadula 模型，简称 BLP 模型。

其访问控制模型如下所示：



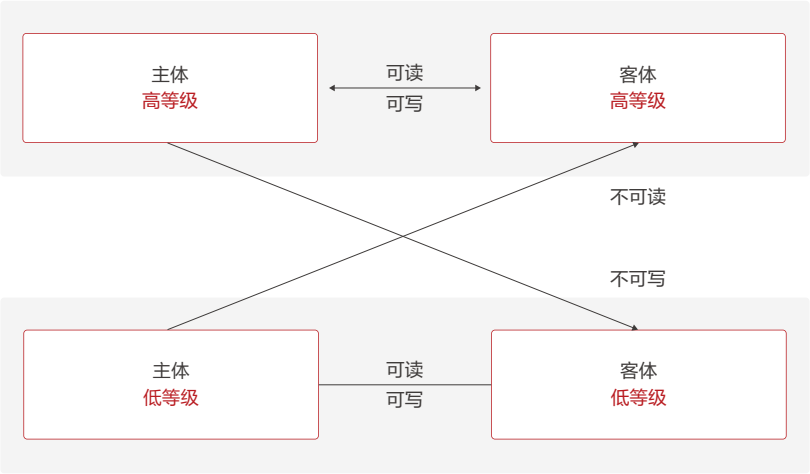
BLP 模型核心规则

- **不上读 – 主体不可读安全级别高于它的客体（数据）**
- **不下写 – 主体不可写安全级别低于它的客体（数据）**

HarmonyOS 将会严格实施 BLP 机密性访问控制原则，来确保用户数据和隐私不泄露，确保高安全数据不会在用户无感的场景下从高安全等级设备泄漏到低安全等级的设备，也确保低安全能力设备不能获取高安全等级的数据。

3.3 完整性保护 Biba 模型

BLP 模型从数学角度证明了可以保证信息隐私性，但是没有解决数据完整性的问题。就此，Ken Biba 在 1977 年推出了 Biba 模型。



Biba 模型核心规则

- **不下读 – 主体不能读取安全级别低于它的客体（数据）**
- **不上写 – 主体不能写入安全级别高于它的客体（数据）**

HarmonyOS 将会严格履行 Biba 模型定义的访问控制逻辑，确保高安全设备不会安装来自不可信来源的应用程序、软件、升级、补丁，只有通过 HarmonyOS 官方认可并签名的软件才能被引入到 HarmonyOS 中。同时，也禁止低级别安全设备向高级别安全设备发起控制指令，例如：通过运动手表控制手机进行大额支付。

HarmonyOS 的安全架构模型选择了以 TCSEC B2 为目标的结构化保护安全，对 HarmonyOS 中的主体（开发者、应用程序、自然人、设备）、环境（运行 HarmonyOS 的 IoT 设备、网络环境）、客体（数据、文件、外设等）都进行严格的安全等级标记。

在 HarmonyOS 安全架构中，确保结构化安全模型有效的前提是，所有主体、环境、客体必须可信。在严格安全标记的基础上，需要保证这些主体身份、应用程序环境和客体标签的真实、完整、不可篡改，也就是 HarmonyOS 能够实现“正确的人通过正确的设备正确的使用数据”，下面我们将对三个“正确”模型进行分别阐述：

3.4 正确的人：主体正确模型

HarmonyOS 中的主体形态有如下典型的四种类型，每一种主体的“正确性”保证措施如下：

- **开发者的“正确”**：HarmonyOS 开发者网站会对开发者进行实名认证，以确保开发者承担相应的责任和义务，享受相应的权利和收益。
- **消费者的“正确”**：HarmonyOS 通过多种认证手段（PIN Code 密码、指纹、人脸、声纹、证书、实名认证等等多种手段）确保对消费者自然人的认证，保证终端不会在丢失或者仿冒的攻击者欺骗下完成认证。
- **应用程序的“正确”**：HarmonyOS 上运行的所有应用程序，无论是 APP 的包，还是执行时内存中的代码，都经过 HarmonyOS 的应用市场签名，确保仿冒、伪造的应用无法运行，也确保任何非法的病毒、恶意代码无法运行。
- **智慧原子化服务的“正确”**：HarmonyOS 的每个智慧原子化服务都有严格的身份权限定义。

3.5 正确的设备：访问环境正确模型

在保证了 HarmonyOS 主体身份的正确的基础上，需要保证 HarmonyOS 运行在一个可信的、与业务需求匹配的硬件设备上。HarmonyOS 针对 IoT 设备的安全，提供了以下能力：

- **设备来源可信**：HarmonyOS 生态的所有设备，均应该遵循统一的安全能力定义，经过检测认证后，由 HarmonyOS 运营平台颁发设备安全能力和等级证书，证书由 HarmonyOS 官方签名，确保设备来源可信。
- **设备安全等级匹配数据隐私要求**：确保 IoT 设备的安全能力，和它上面承载和处理的业务和数据的安全隐私要求匹配。低安全级别的设备，不能处理高敏感度的数据，需要遵循严格的分级规范。
- **设备的认证**：在进行分布式可信互联时，超级终端上的所有设备都被预先分配签名的身份证书，基于证书来实现对设备的认证、鉴权、签名，保证在 HarmonyOS 上流转的数据、程序、指令的机密性、完整性、不可抵赖性。
- **设备系统可信**：HarmonyOS 要求全系列产品具备可信启动可信运行的能力，在生命周期实施完整性保护，确保设备不被篡改。

3.6 正确的使用数据：访问控制模型

HarmonyOS 通过对数据进行严格的分级标签管理，在业务进行数据处理的时候，严格遵从 BLP 与 Biba 模型的机密性完整性保护，来达到整体的结构化防护水平。

HarmonyOS 严格遵从 GDPR、GAPP 和中国个人数据保护法等法律法规，对数据进行了严格的定义和分级，并将其级别进行标签化管理。

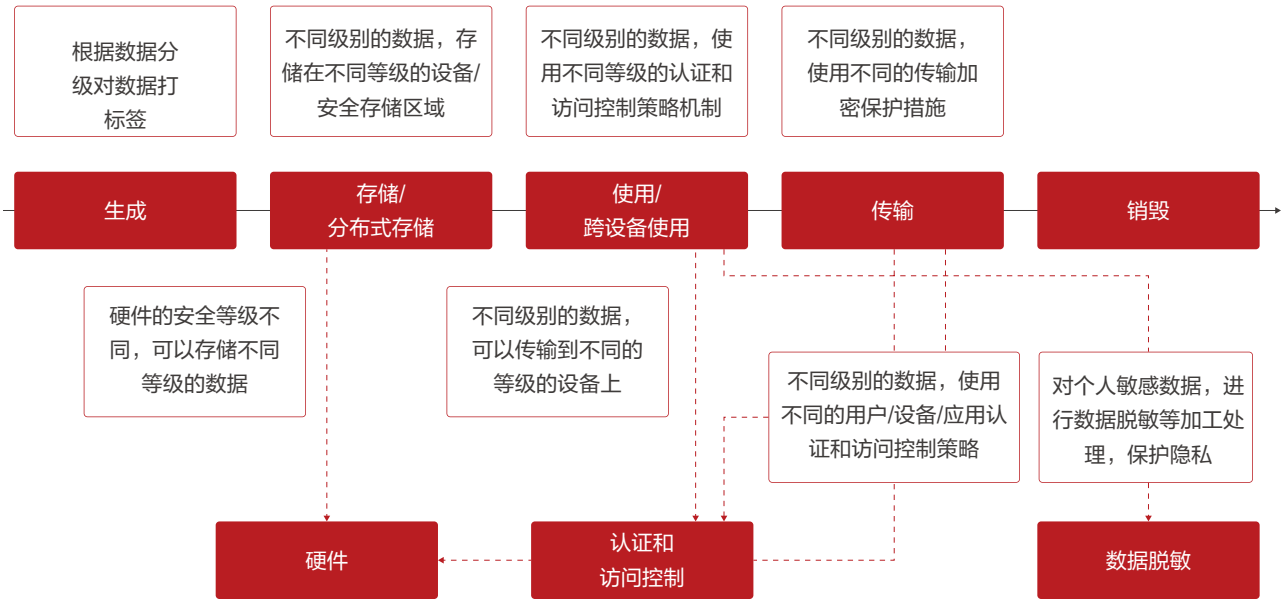
数据分级的国际标准理论依据：FIPS 199、NIST 800-122；隐私分类参考了华为公司的企业标准，同时参考了业界的最佳实践。

HarmonyOS 的数据分级标准：

- 严重：业界法律法规中定义的特殊数据类型，涉及个人的最私密领域的信息或者一旦泄露可能会给个人或组织造成重大的不利影响的数据
- 高：数据的泄露可能会给个人或组织导致严峻的不利影响
- 中：数据的泄露可能会给个人或组织导致严重的不利影响
- 低：数据的泄露可能会给个人或组织导致有限的不利影响
- 公开（无风险）：对个人或组织无不利影响的可公开数据

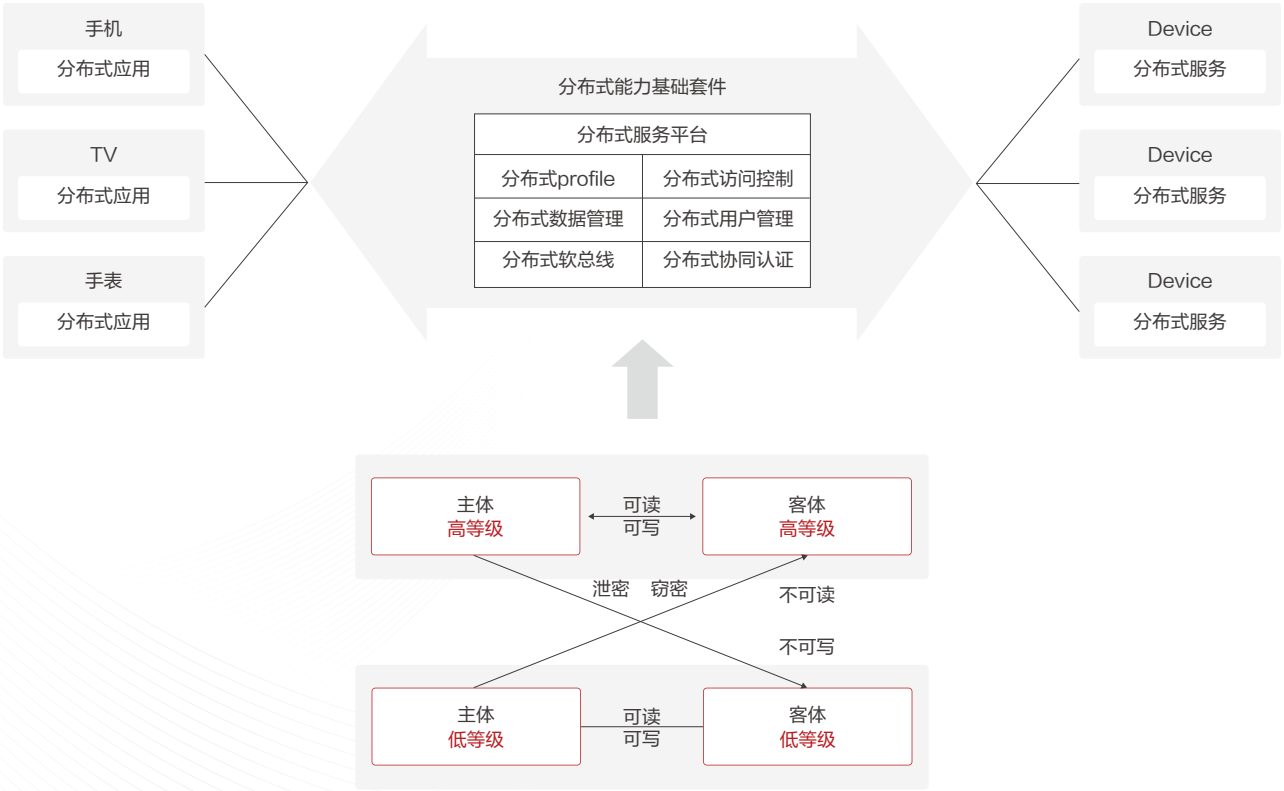
在数据分级基础上，对数据的访问严格遵循分级的生命周期管理：

图 3-1 数据访问生命周期管理



同时，结合用户分级、设备分级、业务分级和数据分级，完成在 HarmonyOS 上的分布式访问控制：

图 3-2 分布式访问控制



HarmonyOS
“正确的人”身份管理与认证

04

HarmonyOS 除提供 PIN 码、数字密码、混合密码的传统身份认证方式，还提供指纹识别，人脸识别等生物认证手段。根据不同认证方式的安全能力和特点，可应用于相应的身份认证场景，如设备解锁、应用锁，移动支付等。

同时，针对分布式业务场景，为提升用户认证的便捷性，HarmonyOS 提供分布式协同认证能力，使用户可便捷地以近端设备为入口完成用户身份认证。

随着 HarmonyOS 承载设备的多样化和场景的复杂性，基于“零信任”网络架构的动态弹性身份认证与访问控制机制，确保了基于不同风险场景，自适应的选择合适的保护策略，更好的保障消费者个人隐私与数据安全。

华为账号是华为公司推出的用户认证体系，作为管理设备、使用数字服务的统一凭证，一次登录即可使用查找设备、家庭共享、云空间、应用市场、钱包等数十种服务。

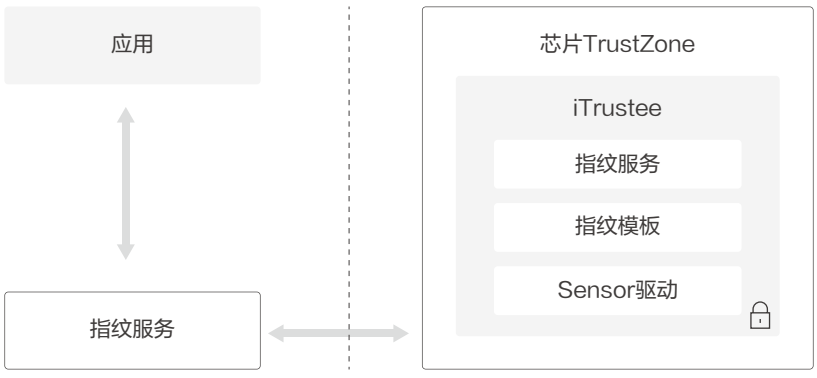
4.1 生物认证

指纹认证

HarmonyOS 目前可提供电容指纹和光学指纹识别的支持。两种技术方案的体验及安全能力基本一致。

HarmonyOS 的指纹识别安全框架图如下：

图 4-1 指纹识别安全框架



HarmonyOS 在指纹传感器和 iTrustee 之间建立安全通道，指纹图像通过安全通道传递到 iTrustee 中，特征提取、活体检测、特征比对等处理也完全在 iTrustee 中进行，基于 TrustZone 进行安全隔离。REE 的指纹框架只负责指纹的认证发起和认证结果等数据，不接触指纹原始数据。

指纹模板录入时，特征数据通过 iTrustee 的安全存储进行存储，并采用高强度的密码算法进行数据加密和完整性保护。外部无法获取到加密指纹数据的密钥，保证用户的指纹数据不会泄露。外部第三方应用无法获取到指纹数据，也不能将指纹数据传出 iTrustee。HarmonyOS 不会将任何指纹数据发送或备份到包括云端在内的任何外部存储介质，当完成指纹特征的存储（模板录入）或特征比对（身份认证）后，指纹图像随之被销毁。

其他手指错误通过认证的概率，大约五万之一。为提供额外保护，HarmonyOS 的指纹识别支持防暴力破解机制，亮屏场景下指纹识别连续错误 5 次，或熄屏场景下指纹识别连续错误 10 次，将锁定 30 秒不能进行指纹识别。如果指纹识别连续失败 20 次，则必须使用密码来解锁设备。

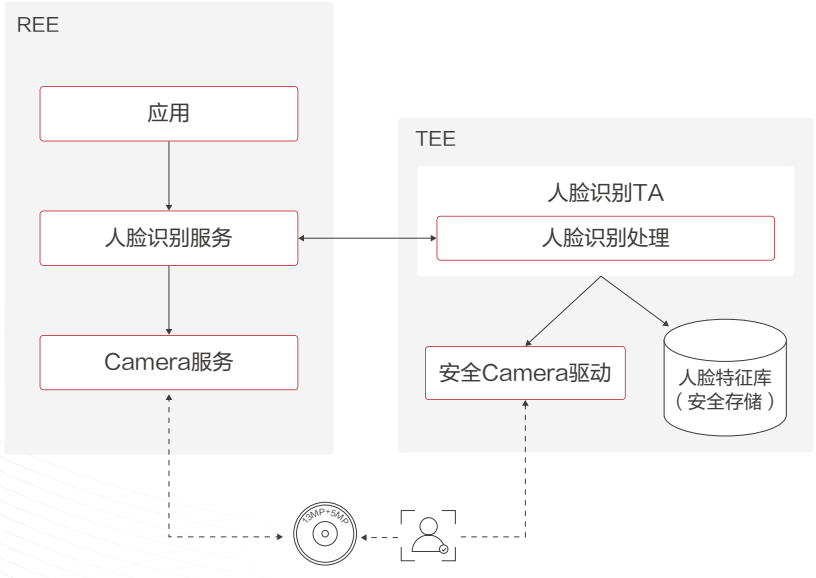
指纹识别提供便利的身份识别的同时，用户更容易忘记锁屏密码。HarmonyOS 采用 72 小时内未使用密码解锁则强制要求用户输入密码解锁，以便加强用户记忆，减少忘记密码的异常情况发生。

人脸认证

HarmonyOS 提供 2D 人脸识别及 3D 人脸识别两种人脸识别方案的支持。3D 人脸识别方案依赖特殊的深度摄像头实现，2D 人脸识别技术则基于普通的前置摄像头实现。3D 人脸识别的识别率和防伪能力均显著优于 2D 人脸识别。3D 人脸识别技术可支持支付应用，2D 人脸识别技术不能支持支付应用。不同的终端设备型号根据其产品定位选择其搭载的人脸识别类型。

HarmonyOS 的人脸识别安全框架图如下：

图 4-2 人脸识别安全框架图



HarmonyOS 在摄像头和 iTrustee 之间建立安全通道，人脸图像信息通过安全通道传递到 iTrustee 中，特征提取、活体检测、特征比对等处理也完全在 iTrustee 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，人脸特征数据通过 iTrustee 的安全存储进行存储，采用高强度的密码算法对人脸特征数据进行加解密和完整性保护。外部无法获取到加密人脸特征数据的密钥，保证用户的人脸特征数据不会泄露。外部第三方应用无法获取到人脸特征数据，也不能将人脸特征数据传出 iTrustee。HarmonyOS 不会将加密的人脸数据或者未经加密的人脸数据发送或备份到包括云端在内的任何外部存储介质。

其他人错误通过认证的概率，3D 方案大约一百万分之一，2D 方案大约五万至十万分之一。为提供额外保护，HarmonyOS 的人脸识别支持防暴力破解机制，用户使用人脸识别连续错误 5 次，则不能进行人脸识别，必须输入密码解锁设备。对于长相相似的双胞胎和亲属、以及未满 13 岁的儿童，错误匹配的概率会有所加大。

此外，由于人脸识别主要基于摄像头采集的人脸图像数据，可能无法精确分辨照片的翻拍或是制作精良的头模。

如果对以上风险感到担忧，推荐使用密码认证。同时，当 HarmonyOS 的零信任网络架构感知到系统环境风险变化时，会动态调整策略，智能启动高级安全模式，对某些高敏感数据加密密钥进行主动销毁，且要求更加严格的 PIN 码认证，来应对更严酷的安全风险。

4.2 分布式协同认证

在构成分布式系统的可信设备间，HarmonyOS 构建了分布式身份认证能力，打破设备边界，依据用户操作和业务需要，提供灵活的身份认证能力，当用户同时操作多个同一局域网下的可信设备时，用户可将手边最便捷的同等安全级别的设备作为访问入口与身份认证入口。

HarmonyOS 的协同用户身份认证（下称协同认证），基于可信设备间的安全数据传统通道，提供分布式用户身份认证框架。

基于用户秘密的分布式认证

在设备之间已建立可信关系的前提下，为实现锁屏密码作为用户秘密的分布式认证，HarmonyOS 设备上支持锁屏密码采集端与认证端的解耦。采集端提供采集用户锁屏密码及对锁屏密码的脱敏处理能力，认证端提供认证凭据的比对能力，两端通过 PAKE 协议完成分布式认证，使用户秘密可以在无需传输到对端的情况下，完成远程秘密认证。

为保证采集端与认证端的信息来自合法的安全模块，HarmonyOS 的分布式秘密认证服务会在采集端与认证端设备各自的本地 iTrustee 环境内生成执行器的身份标识，该身份标识是一个 Ed25519 公私钥对，用于在远程秘密认证过程中，在设备 A 的采集器和设备 B 的认证器之间，签名本地传出的数据，验证对方传入

的数据。

锁屏密码信息在设备 A 上完成数据采集和脱敏处理后，在 iTrustee 环境中生成 PAKE 认证协议字段，并使用采集端身份标识的私钥对协议字段数据进行签名，之后通过基于设备间可信关系的端到端加密安全通道传输到设备 B，在设备 B 的 iTrustee 环境中验证签名信息后，完成 PAKE 协议的认证过程。

在该过程中，REE 侧无法篡改签名信息。两端设备间的 PAKE 协议认证机制使得锁屏密码明文及中间计算结果不会在设备间进行传输，从所传输的协议认证字段也不会被穷举逆推出用户的锁屏密码。

HarmonyOS 的协同锁屏密码认证支持防暴力破解机制，具体防暴力破解方式和本地锁屏密码保持一致。

基于可信持有物的分布式认证

用户可以将绑定的耳机、眼镜或其他同账号手机、平板、PC 等设备添加为“可信持有物”或“伴随设备”，用于认证用户身份。对于耳机、眼镜等有佩戴检测能力的配件，配戴后通过声纹 / 指纹等本地认证方式，或者在主设备附近时通过同步主设备解锁认证结果确认了佩戴者是机主后，只要没有被取下就能够持续提供可信持有物认证通过结果，支持用户无感便捷的身份认证体验；对于手机、平板、PC 等没有跟踪用户能力的设备，需要通过一次实时的人脸、指纹等本地认证通过后，才能返回可信持有物认证通过结果，一般用于多屏协同等场景下的跨设备用户身份认证，避免用户在超级终端之间的频繁切换。

4.3 零信任网络架构

当使用该蓝牙配件对用户发起认证时，协同认证将判断蓝牙配件的连接状态、蓝牙配件与手机的距离、并基于持续佩戴 TOKEN 发起手机与配件间的持续佩戴检测，当三个因子同时满足要求时，才会认为认证成功。

随着搭载 HarmonyOS 的设备越来越丰富，场景的复杂和承载数据的敏感性都大幅提升，HarmonyOS 构建了以“零信任网络”架构为核心的身份认证与访问控制架构。HarmonyOS 构筑了以“电子围栏”为中心的可信环境识别感知能力，当感知到设备面临恶意攻击、所处环境安全性下降等风险时，会主动对数据安全进行降级处置，限制部分数据的高敏感权限（如编辑、打印、转发等能力），限制以概率统计为基础的生物特征认证手段，强制使用以密码技术为基础的 PIN 码认证，主动销毁部分高敏感数据的加密密钥。

HarmonyOS 构筑了以“用户锁屏”为中心的用户隐私数据保护能力，即在用户锁屏后，应用数据的加 / 解密密钥非必要、不存在。系统在感知到用户锁屏后，会触发对应用数据加 / 解密密钥的擦除判断，对于在本次锁屏后未预约使用的应用密钥，系统会默认执行密钥擦除动作；对于在本次锁屏后存在预约使用的密钥，系统会在业务使用完成后擦除密钥。

基于“零信任网络”架构，HarmonyOS 既保证了消费者使用终端设备的便捷，又保护了个人隐私与数据安全，实现了以人为本的人文关怀和科技美学的完美集合。

4.4 华为账号

华为账号在登录、重置密码、修改账号、申诉等环节均设置了主动风险监测机制，主动识别风险，防范账号盗用。

登录：针对钓鱼、木马、撞库等操作引起的账号被盗问题，华为账号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，保障账号安全。

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，占有用户的华为账号，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，获取账号使用权。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账号。

申诉：同重置密码环节相似，申诉环节也可以决定一个账号的归属权。攻击者可以利用申诉环节占有用户的华为账号，获取非法利益；正常用户也需要公共申诉便捷的获取账号访问权。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，华为账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、机器学习识别虚假账号，打击虚假注册，保护用户合法权益。

HarmonyOS
“正确的设备”系统安全

05

HarmonyOS 参考了可信计算机系统准则（橘皮书）、CC 安全认证、FIPS 密码模块安全分级、IOTSF 计算设备的安全分级模型等，并结合移动操作系统的攻防对抗，定义了 HarmonyOS 的系统安全架构。本章尝试对 HarmonyOS 面向分布式连接的安全分级模型和系统安全架构及其关键技术进行阐述。

5.1 HarmonyOS 系统安全概述

HarmonyOS 系统安全采用了芯－端－云垂直整合的架构，根植于信任根（芯片信任根、云服务等），以基础安全工程能力为依托，重点围绕系统完整性保护、隔离和访问控制、漏洞防利构建相关的安全技术和能力。

HarmonyOS 系统安全架构如下图所示：

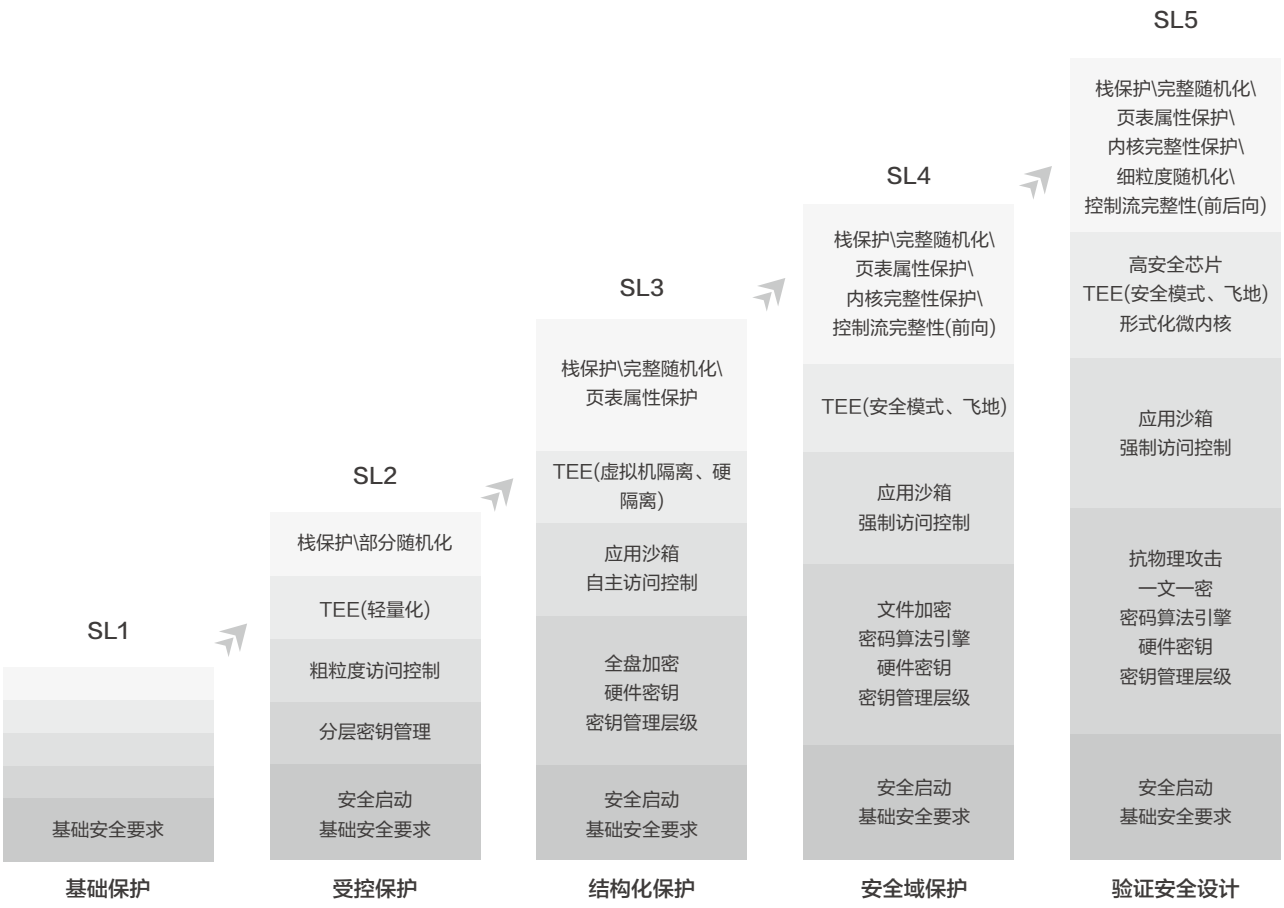
图 5-1HarmonyOS 系统安全架构

遵循可信计算理论，HarmonyOS 的安全设计整体根植于信任根，根据不同的保护对象和资产选择合适的信任根，如芯片、服务器等。完整性保护：是系统安全的根基，确保系统软件和应用程序全生命周期的完整合法，未被非法篡改，是支撑安全策略正确实施的前提。隔离及访问控制则：对系统公共资源提供多层级安全隔离（APP/ 内核 /TEE OS/ 安全芯片），主体对客体资源的访问确保独立、有序、可控；提供了系统的机密性和可用性。漏洞防利用：全生命周期的漏洞治理，围绕开发阶段消除、编译阶段加固、运行阶段阻隔、漏洞利用后风险降级的策略实施全生命周期的漏洞安全治理，有效降低漏洞对系统的威胁，也是确保上述完整性、机密性、可用性等安全目标达成的支柱。

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 5-2HarmonyOS 设备安全分级



SL1 为 HarmonyOS 设备中最低的安全等级，这类设备通常运行轻量级 OS 和低端微处理器，业务形态较为单一，不涉及敏感数据的处理；该安全等级要求消除常见的错误，支持软件的完整性保护。若无法满足 SL1 等级的要求，则只能作为配件受 HarmonyOS 设备操控，无法反向操控 HarmonyOS 设备并进行更复杂的业务协同。

SL2 安全等级的 HarmonyOS 设备，可对其数据进行标记并定义访问控制规则，实现自主的访问控制；要求具备基础的抗渗透能力；设备可支持轻量化的可安全隔离环境，用于部署少量必需的安全业务。

SL3 安全等级的 HarmonyOS 设备，具备较为完善的安全保护能力。其操作系统具有较为完善的安全语义，可支持强制访问控制；系统可结构化为关键保护元素和非关键保护元素，其关键保护元素被明确定义的安全策略模型保护；SL3 的设备应具备一定的抗渗透能力，可对抗常见的漏洞利用方法。

SL4 安全等级的 HarmonyOS 设备，可信基应保持足够的精简，具备防篡改的能力，其实现应足够精简和安全，可对关键保护元素的访问控制进行充分的鉴定和仲裁；设备具备相当的抗渗透能力，可抑制绝大多数软件攻击。

SL5 安全等级的 HarmonyOS 设备，为 HarmonyOS 设备中具备最高等级安全防护能力的设备。系统核心软件模块应进行形式化验证；关键硬件模块如可信根、密码计算引擎等应具备防物理攻击能力，可应对实验室级别的攻击。SL5 级别设备应具备高安全单元，如专用的安全芯片，用于强化设备的启动可信根、存储可信根、运行可信根。

不同的产品，需根据其产品业务形态和场景所需，定义适合的安全等级，并遵循安全等级的要求部署和构建响应的安全机制。上述设备安全分级模型，结合 HarmonyOS 的其他安全模型如数据分级，构成了分布式场景的访问控制基础架构和安全管控逻辑。

以下章节按照不同的技术维度介绍 HarmonyOS 系统安全的关键技术点。

5.2 完整性保护

安全启动

HarmonyOS 设备启动流程中的每一步，都包含对启动对象的数字签名校验，以确保设备在启动过程中加载并运行合法授权的软件。只有正确通过签名校验的镜像文件才可被加载并运行，包括启动引导程序、内核、基带、短距固件等镜像文件。在启动过程的任何阶段，如果签名校验失败，则启动流程会被终止。

设备启动时最初执行的是固化在芯片当中的一段引导程序，称作片内引导程序。这段代码在芯片制造时被写入芯片内部只读 ROM 中，出厂后无法修改，是设备启动的信任根。片内引导程序执行基本的系统初始化，从 Flash 存储芯片中加载二级引导程序。使用芯片内部 Fuse 空间（熔丝工艺， 一旦熔断不可更改）的公钥哈希值对公钥进行合法性验证后，片内引导程序再利用公钥对二级引导程序镜像的数字签名进行校验，成功

后运行二级引导程序。二级引导程序加载、验证和执行下一个镜像文件。以此类推，直到整个系统启动完 成，从而保证启动过程的信任链传递，防止未授权程序被恶意加载运行。

部分启动过程中所使用到的镜像采用了加密保护。

安全升级

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

设备刷机管控

通过刷入特权软件版本从而额外获得更多特权并危害设备安全是攻击者及黑灰产常用的手段。HarmonyOS 设计了一系列防止设备非法刷机的管控机制。通过将商用和研发版本软件签名的分离，并在出厂后通过熔丝控制切换到商用签名，实现了 HarmonyOS 商用设备上仅运行商用版本软件，各种泄露的特权版本软件均无法启动。在维修等需运行特权版本软件的场景，则需得到 OEM 签发的授权证书，校验通过后方可运行特权版本软件。在涉及改变设备的国家 / 地区、运营商、商用机 / 演示机，或临时 / 永久解锁等场景，均需在在线的加密狗机制鉴权通过后才许可。

可信启动

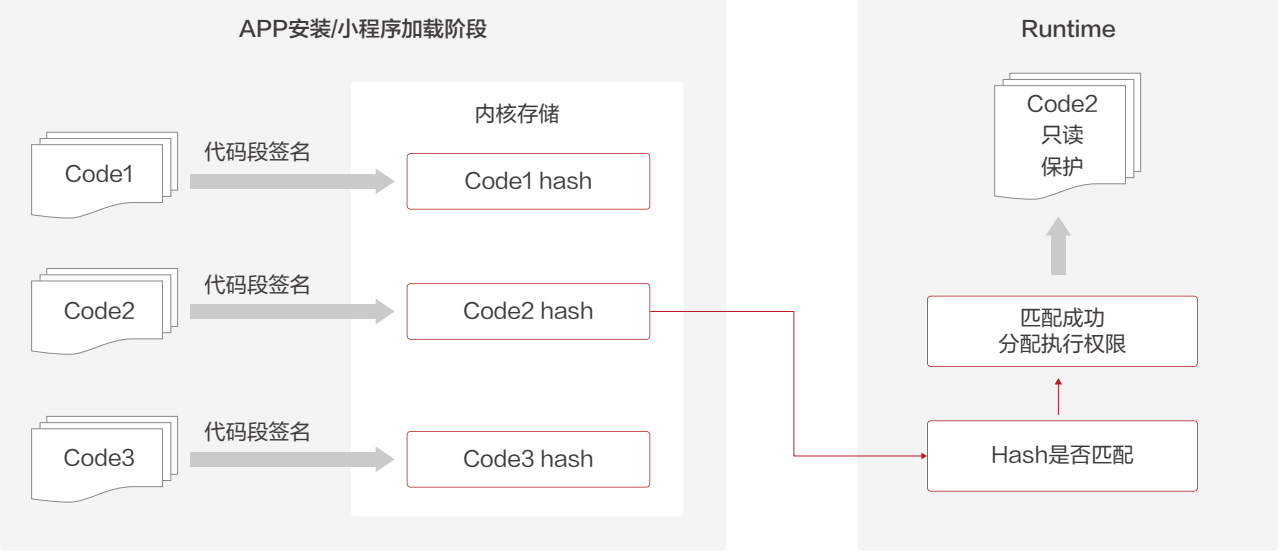
部分较新平台的设备，除了支持安全启动链之外，同时也支持可信启动。即启动过程中，设备基于芯片信任根会逐级度量系统镜像并生成度量日志，该日志既被存储于设备端，同时也可上报到远程服务器。远程服务器可基于预先存储的度量基线，检测设备加载软件的合法性。

代码强制签名

基于芯片可信根和服务器签名系统构建的安全启动，可确保系统软件的完整、合法，未被篡改；对于设备上运行的大量应用代码，则需要另外一种安全机制来确保其完整性和合法性：代码强制签名。

HarmonyOS 采用了代码强制签名技术，即系统仅加载合法签名的软件并对其授予内存的可执行权限。在应用安装时候校验签名合法性，并在系统中生成签名树信息；在代码加载及获取执行权限阶段，则由操作系统校验签名的合法性，校验通过授予内存对象执行权限；对于非法的代码加载行为，如利用匿名可执行内存植入代码等行为，由于缺乏合理的签名，会被系统拒绝。

图 5-3 代码强制签名

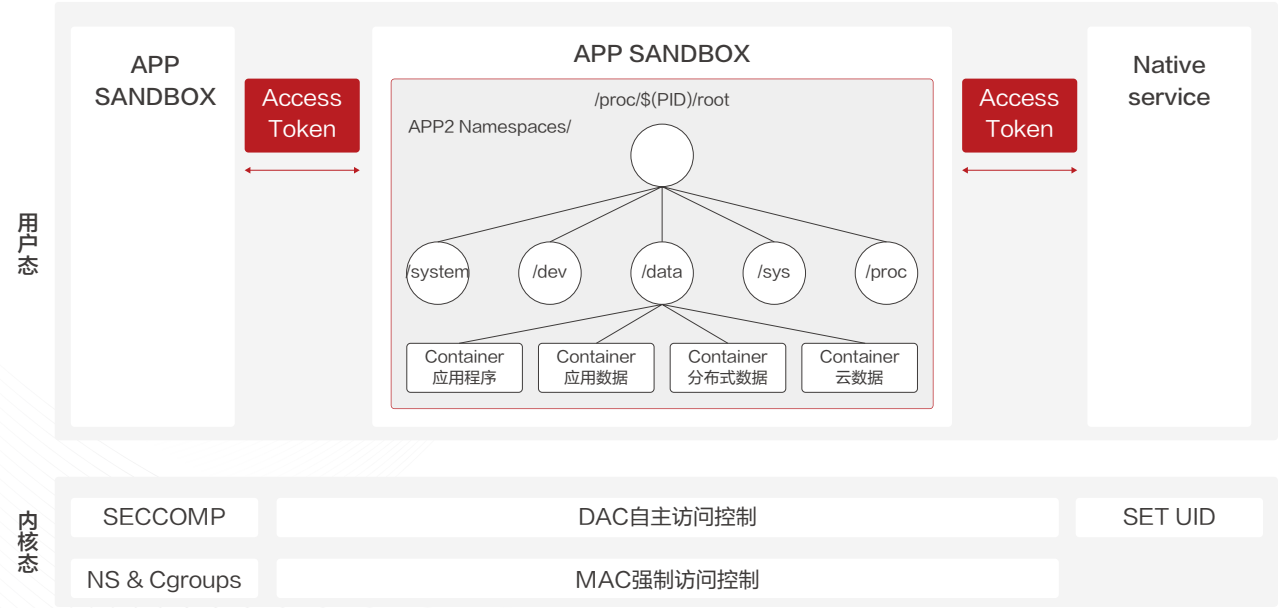


5.3 隔离和访问控制

隔离和访问控制整体架构

下图为 HarmonyOS 的隔离和访问控制整体架构，下文概要介绍所涉及的关键技术点。

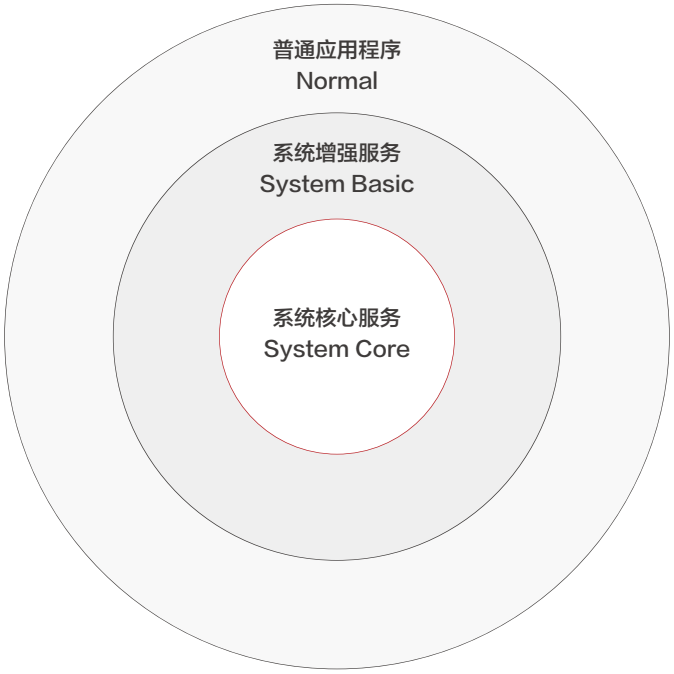
图 5-4HarmonyOS 隔离访问控制架构



Access Token

HarmonyOS 构建基于洋葱模型的分级安全机制，是构建运行生命周期安全的基础。HarmonyOS 应用层的权限框架为 Access Token，HarmonyOS 将应用分为三个 APL（Ability Privilege Level）：normal，system basic 和 system core。应用各自运行在独立的沙盒化环境中，默认仅允许访问自身的文件，如需访问其他应用或者系统的信息，则需要通过权限来实现。

图 5-5 HarmonyOS 洋葱圈模型权限管理框架

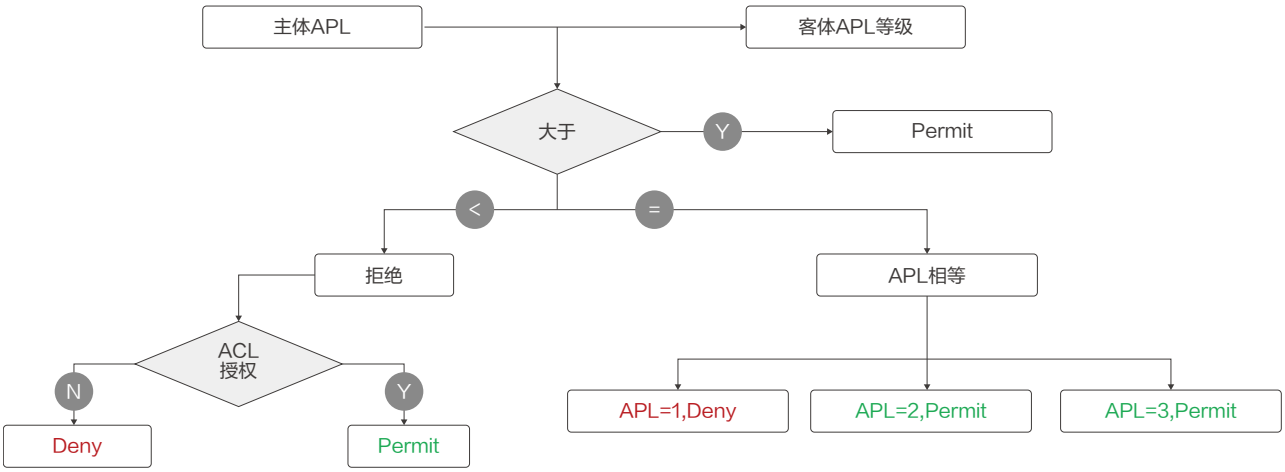


不同 APL 等级可申请的权限范围也不一样，对应规则可以总结为如下表格：

APL 等级	说明
system_core (APL 3)	该等级的应用提供操作系统核心能力。这类应用可申请的权限涉及到开放操作系统核心资源的访问操作，鉴于该类型权限对系统的影响程度非常大，目前只向系统服务开放。
system_basic (APL 2)	该等级的应用提供系统基础服务。这类应用可申请的权限，涉及允许访问操作系统基础服务相关的资源。
normal (APL 1)	普通系统应用和所有三方应用。这类应用可申请的权限，对用户隐私以及其他应用带来的风险很小。

Access Token 的访问控制规则如下图所示：

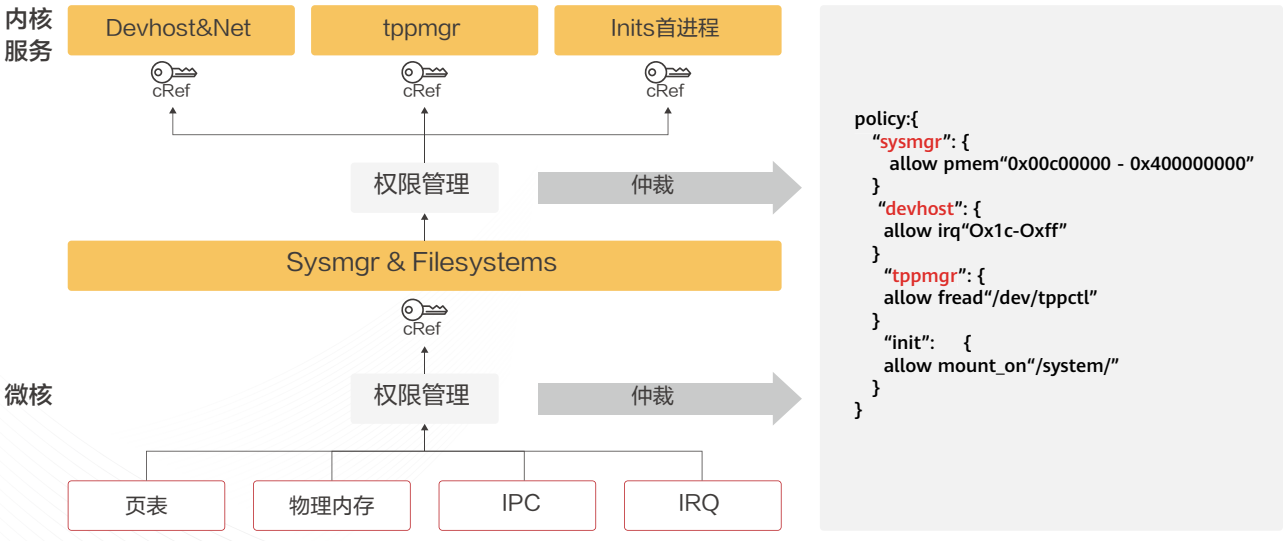
图 5-6 Access Token 访问控制规则



强制访问控制

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

图 5-7Harmony 强制访问控制



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

可信执行环境

华为自研的可信执行环境技术 iTrustee 基于 TrustZone 技术实现，TrustZone 是硬件级别的安全，兼顾了性能、安全和成本的平衡。TrustZone 技术将处理器 的工作状态分为安全世界（Trusted Execution Environment，TEE，也叫可信 执行环境）和非安全世界（Rich Execution Environment，REE，也叫普通执行 环境）。通过特殊指令 SMC 在 CPU 的安全世界和普通世界之间切换来提供硬件隔离。在安全世界，提供了对硬件资源的保护和隔离，包括内存、外设等，通过执行过程保护、密钥保密性、数据完整性和访问权限实现了端到端的安全，可防止来自非安全世界中的恶意软件攻击。

HarmonyOS 可信执行环境，支持多核多线程能力，可创建多个安全任务，并可运行在多个 CPU，极大提高可信执行环境的算力；此外，HarmonyOS 可信执行环境支持基础功能库与数学库（C 库、POSIX API）、支持动态库，可极大地方便可信应用的开发和部署。

HarmonyOS 可信执行环境技术支持如下能力：

基础安全加固

可信执行环境全生命周期确保合法性及完整性，包含：启动、升级；

对镜像文件进行逆向分析是攻击者对目标发起攻击的重要手段，HarmonyOS 的可信执行环境支持镜像防逆向保护。防逆向保护技术主要为镜像加密和符号表混淆；

HarmonyOS 可信执行环境支持防渗透，包括安全编译（如：RELRO)、地址随机化、栈保护、数据不可执行、代码段及函数指针只读；

安全管理

支持可信应用程序的生命周期管理，包括：可信应用证书签名及吊销、可信应用在安装阶段校验完整性、可信应用生命周期会话管理；

可信执行环境可能运行多个可信应用程序，为确保可信应用间的有效隔离，避免可信应用程序漏洞被攻击者利用后对可信执行环境进行持续的渗透和破坏，HarmonyOS 可信执行环境支持细粒度的资源访问及权限控制；

可信执行环境存在多个安全应用服务于 REE 的不同任务，HarmonyOS 支持细粒度的可信应用访问控制，某可信应用可只服务于特定的应用；HarmonyOS 采用白名单机制，白名单内的进程可访问某可信应用，在白名单基础上进一步支持进程代码段的合法性鉴权，防止仿冒；

可信执行环境负责敏感数据处理，需占用系统一定的资源；为提升系统资源（如内存）的利用率，HarmonyOS 可信执行环境支持资源的动态管理能力，降低静态占用资源的比例，如普通内存可动态转换为安全内存。

安全服务

HarmonyOS 可信存储服务，提供关键信息的存储能力，保证数据的机密性、完整性。可信存储支持设备绑定，支持不同安全应用之间的隔离，可信应用仅能访问自己的存储内容，无法打开、删除或篡改其它应用的存储内容。HarmonyOS 可信存储分为两种：安全文件系统存储与 RPMB 存储，前者将密文存储到特定的安全存储分区，后者存储到 eMMC 特定的存储区域，RPMB 支持防删除、防回滚。

HarmonyOS 可信执行环境加解密服务支持多种对称、非对称加解密算法以及密钥派生算法 , 支持同一芯片平台相同密钥的派生，支持设备唯一密钥 , 支持标准的加密算法，为第三方开发存储和使用密钥的业务可信应用提供支持，并遵从 Global platform TEE 标准。为提高安全性，HarmonyOS 可信执行环境内部的密钥生成和计算，均由独立的硬件芯片完成。

HarmonyOS 可信时间服务，提供可信的基准时间，该时间不能被恶意 TA 或 REE 应用修改。

HarmonyOS 可信执行环境面向开发者提供可信执行环境平台能力，提供丰富的 API，完 善的 SDK，以及相关参考手册、参考设计，同时提供安全证书管理、应用签名、 安全应用生命周期管理，应用上线服务，通过 HUAWEI DevEco Studio 开发环境 提供统一的开发者开发界面。 第三方应用，可以基于上述能力进行可信用的开发和调试。

安全元件 *

安全元件（Secure Element）是一个提供芯片级的安全执行、存储环境的子系统。HarmonyOS 支持安全元件的部署，安全元件被用于解决移动支付、身份 ID 等核心业务及数据的安全。相对于可信执行环境方案，安全单元解决方案通过芯片级的安全设计和软件算法，提供软硬结合的双重防护，不仅具备软件安全防护能力，更能防护来自物理层面的攻击，具有更高的安全性，从根本上保证了 HarmonyOS 设备核心安全业务的安全。

独立安全芯片

安全元件主要用于特定安全业务的部署，而独立安全芯片则可增强 HarmonyOS 设备的系统安全能力。

HarmonyOS 利用独立安全芯片的高安全环境（物理安全级），实现锁屏密码保护、文件加密、生物特征保护与识别、密钥管理、可信根、防回退等安全服务。从而在硬件层面为 HarmonyOS 设备的基础安全能力提供保障。

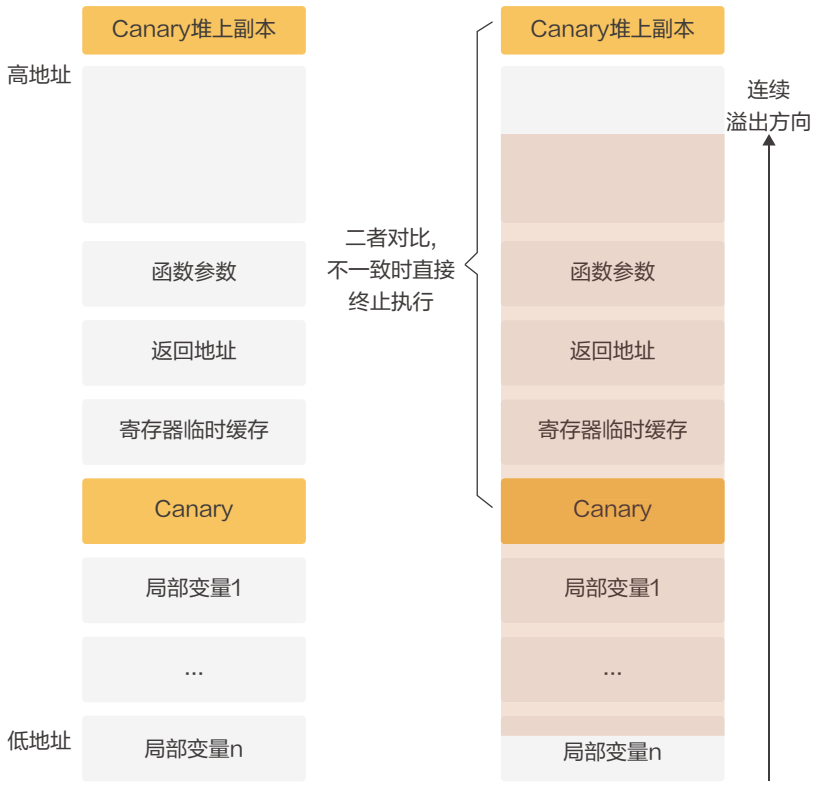
** 注：设备厂商采用的安全元件需通过相关的行业和机构认证，以支持移动支付和金融相关业务。*

5.4 漏洞防利用

栈保护

栈保护是对抗栈溢出漏洞的性价比最高的方案。大多数栈溢出攻击都具有一个典型的特征：连续覆盖。连续覆盖意味着在破坏函数返回地址之前，栈溢出同样会破坏栈上其他的数据。通过在编译阶段，在局部变量和函数返回地址中间，插入一个 Canary 变量；函数返回前，通过比对栈上 Canary 和堆上的副本就可以判断返回地址是否被破坏。栈保护性能影响较小，安全防护效果较好，HarmonyOS 的 SL2 安全等级及以上的设备均要求支持。

图 5-8 栈保护原理



地址空间随机化

在栈溢出漏洞利用中，攻击者触发漏洞后，可以将返回地址指向栈自身进而导致 shellcode 的执行。缓解的思路之一就是改变栈的起始位置，使得地址空间布局难以预测，进而提升攻击难度，提升安全性。而通过 ROP(Return Oriented Programming) 技术，可利用系统中已存在的代码片段组合实现类似 shellcode 的攻击效果。因此除了栈随机化，还需支持全地址空间随机化，保护对象包括栈、共享库、mmap、VDSO、代码、堆等。地址控制保护同时部署于用户态程序和内核中。

数据不可执行

阻止缓冲区溢出漏洞利用的另一方法是阻断注入代码的执行。由于注入的 shellcode 位于数据区域，缓解策略就是禁止 CPU 把数据区域当作代码执行。

数据不可执行叠加地址随机化，方可发挥出较好的安全保护效果，也是 HarmonyOS 的默认推荐做法。

特权模式访问禁止 / 特权模式执行禁止

HarmonyOS 使用 PAN（Privileged Access Never）和 PXN (Privileged execute never) 技术保护内核，禁止内核访问用户空间的数据和执行用户空间的代码。

在某些针对内核的攻击方法中，攻击者通过篡改某些内核使用的数据结构内的 数据指针，使其指向攻击者在用户态准备好的数据结构，影响内核的行为达到 攻击目的。PAN 技术阻止了内核访问用户态数据，这种攻击行为会被阻止。在某些针对内核的攻击方法中，攻击者通过篡改某些内核使用的数据结构内的代码指针，使其指向用户态的攻击程序，并通过系统调用触发攻击程序执行。PXN 技术阻止了内核直接执行用户态代码，这种攻击行为会被阻止。

控制流完整性 CFI

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

由于实现 ROP/JOP 攻击的常用方法是利用程序漏洞来覆盖内存中的函数指针，因此可针对性进行检查。CFI 技术通过添加额外的检查来确认控制流停留在预先设定的范围中，以缓解 ROP/JOP 攻击，如果检测到程序发生未定义的行为，则丢弃程序执行。CFI 使得攻击者在实践中利用漏洞变 得更加困难。

HarmonyOS 采用 ARM 的指针完整性保护技术 PAC 实现了 CFI 保护，保护特定对象如内核、TEE 等组件的控制流完整性；针对部分系统应用和库，则采用 Clang CFI 和 return guard 技术以缓解 ROP/JOP 攻击威胁内核。

数据指针完整性

值得注意的是，在 HarmonyOS 中，PAC 不仅用来保护控制流指针，也用于保护部分数据指针，从而缓解 DOP 类攻击带来的威胁。这类技术当前主要部署于内核中，用于保护权限、进程身份、通信端口等敏感数据。

内核完整性保护

系统运行过程中，攻击者在获得内核任意读写权限后，往往会通过破坏内核的关键数据对象从而达成任意代码执行、权限提升等攻击目标。因此在运行过程中保护内核的关键数据对象，对提升系统防护强度而言至关重要。

HarmonyOS 内核完整性保护技术通过 ARMv8 处理器提供的虚拟化扩展模式对内核保护，防止系统关键寄存器、页表、代码等被篡改。从而达到系统运行时的完整性保护和防提权的目的。

内核完整性保护技术不但实现了对于代码及只读数据段等静态数据的保护，而且实现了稀有写（Write-Rare）保护机制对于部分动态数据提供保护。利用稀有写机制保护了内核里大部分时间是被读取而极少被更改的数据。攻击者即使通过漏洞获取了内核级别的内存写能力，也无法修改这部分数据。

目前 HarmonyOS 内核完整性保护技术支持如下安全保护机制：

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

注：此功能当前仅在中国区部分海思芯片型号的产品上提供。

HarmonyOS

“正确的访问数据”数据分级访问控制

06

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数据敏感程度、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，其核心的策略参考了 BLP 模型的机密性防护和 Biba 模型的完整性保护策略。简言之，在数据创建时就应该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，要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。

围绕数据全生命周期，“正确的访问数据”将会基于 BLP 和 Biba 模型贯穿整个数据的使用。

除数据访问控制以外，HarmonyOS 还对不同分级数据采用合适的加密、数字签名方案进行保护。比如，对设备中不同分级数据采用相匹配的存储加密方案；当敏感个人数据和凭据类数据进行云同步时，采用端端加密方案，确保数据只在用户设备上可以解密，在云服务器中无法解密，华为无法获得这些数据。

6.1 数据分级原则

数据分级的原则是根据数据遭到泄露或者遭到破坏带来的风险对个人、组织或公众的影响进行分级。进而针对不同等级的数据提出不同的防护要求。

根据《FIPS-199》标准，基于数据的机密性、完整性、可用性三大安全目标进行风险评估，主要需要考虑对个人 / 组织 / 公众的影响，从而确定数据的风险等级。数据对于公众、组织或个人的影响越高，则其风险等级越高，如下表。

风险评估公式：风险等级 = F{ 机密性，完整性，可用性 }

安全目标、潜在影响	低	中	高
机密性 对于信息的访问和披露通过加密和访问控制等手段进行保护，包括个人隐私和专利信息。	未授权的信息披露可能会对组织运行 / 组织资产 / 个人产生有限的不利影响。	未授权的信息披露可能会对组织运行 / 组织资产 / 个人产生严重的不利影响。比如造成罚款，形象遭到负面影响等。	未授权的信息披露可能会对组织运行 / 组织资产 / 个人产生严重或灾难性的不利影响。比如造成公司重大商业损失，声誉损失，退出特定行业等
完整性 防止信息被非法修改和销毁，确保信息的完整性和真实性	未授权的信息修改和信息销毁可能对于组织运行 / 组织资产 / 个人产生有限的不利影响	未授权的信息修改和信息销毁可能会对组织运行 / 组织资产 / 个人产生严重的不利影响。	未授权的信息修改和信息销毁可能会对组织运行 / 组织资产 / 个人产生严重或灾难性的不利影响。
可用性 确保信息能够及时可靠的被访问和使用	对信息或信息系统的使用或访问能力的破坏可能对于组织运行 / 组织资产 / 个人产生有限的不利影响	对信息或信息系统的使用或访问能力的破坏可能对于组织运行 / 组织资产 / 个人产生严重的不利影响。	对信息或信息系统的使用或访问能力的破坏可能对于组织运行 / 组织资产 / 个人产生严重或灾难性的不利影响。

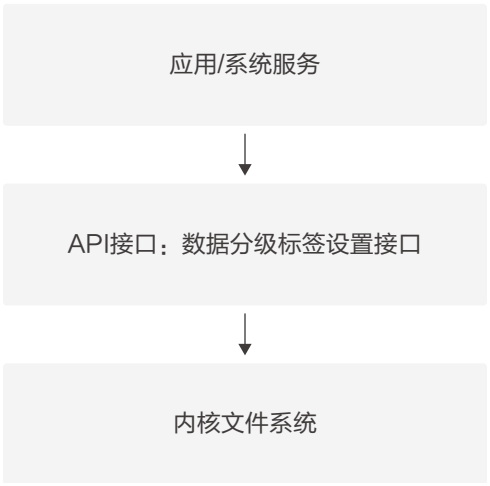
HarmonyOS 按照数据泄露造成的影响程度和业界优秀实践，对数据进行分级（参考：ISO/IEC27005、FIPS-199、NIST SP800-122）。个人数据风险等级可分为高、中、低。针对非个人数据，增加公开风险等级；针对敏感个人数据（如欧盟 GDPR 要求的特殊类型个人数据和 GB/T 35273-2020 信息安全技术个人信息安全规范定义的敏感个人信息）和业界优秀实践，增加严重风险级。并为每个级别的数据赋予数据风险标签，见下表。

数据隐私分类	数据类型	数据分级	举例
敏感个人数据	身份认证凭据	严重（S4）	用于身份认证的口令、密码等
	个人种族信息		种族血统
	负向名誉数据		犯罪记录、纪律处分等负向记录
	健康信息		体脂数据、血压数据、血糖数据、心率数据、血氧数据、ECG、医疗记录、性生活、睡眠数据
	生物特征		DNA、指纹、面部特征、虹膜、声纹、掌纹、耳廓、行为特征
一般个人数据	运动数据	高（S3）	步数、运动距离、运动时长、消耗热量、爬高、摄氧量、跑步姿态、运动心率
	个人多媒体数据		用户设备中的图片、文字、音频、视频等信息
	年龄生辰数据	中（S2）	年龄、出生日期
	社会用户标识		具有社会识别性的用户标识符，可以丢弃、置换、重新注册，如华为账号、社交账号等
	姓名昵称		姓名、昵称
	地址信息		邮政编码、工作地址、家庭地址
	一般个人信息	低（S1）	性别、国籍、出生地、教育程度、专业背景等
	正向名誉数据		专业成就
非个人数据	系统密钥	高（S3）	系统的根秘钥、根秘钥派生用于加密系统服务和应用的的各层工作秘钥、应用自身产生的用于加密系统服务和应用的的各层工作秘钥
	其他非个人数据	低 / 公开（S0）	系统、设备信息中公开发布的数据，如：软件版本号、引擎版本号、客户端版本号、驱动程序版本号、SDK 版本号、应用分类信息

数据风险等级标签设定机制

HarmonyOS 提供了设置数据风险等级标签的能力，业务在生成文件 / 生成数据的阶段，使用 HarmonyOS 提供的能力设置对应数据的风险等级；

如下图所示，业务 APP 可以通过调用风险等级标签的设置 API，设置 APP 落盘数据的风险等级，风险等级信息最终存储在应用落盘文件的元数据之中；



业务 APP 需要根据 HarmonyOS 提供的业务风险等级定义，设置对应文件 / 数据的风险等级；同时业务 APP 需要评估对应设备的安全等级，业务 APP 需要存储的数据对应的风险等级需要与设备安全等级匹配，这样才能够确保设置了风险等级的数据 / 文件在数据全生命周期受到与对应风险等级匹配的系统保护；

设备的安全等级	SL5	SL4	SL3	SL2	SL1
各安全等级设备可支持存储的数据风险等级	S0~S4	S0~S4	S0~S3	S0~S2	S0~S1

6.2 HarmonyOS 数据分级加密安全机制

HarmonyOS 提供了文件级加密功能，利用内核的加密文件系统模块和硬件加解密引擎，采用 AES256 算法的 XTS 模式实现加密。

文件系统分级加密

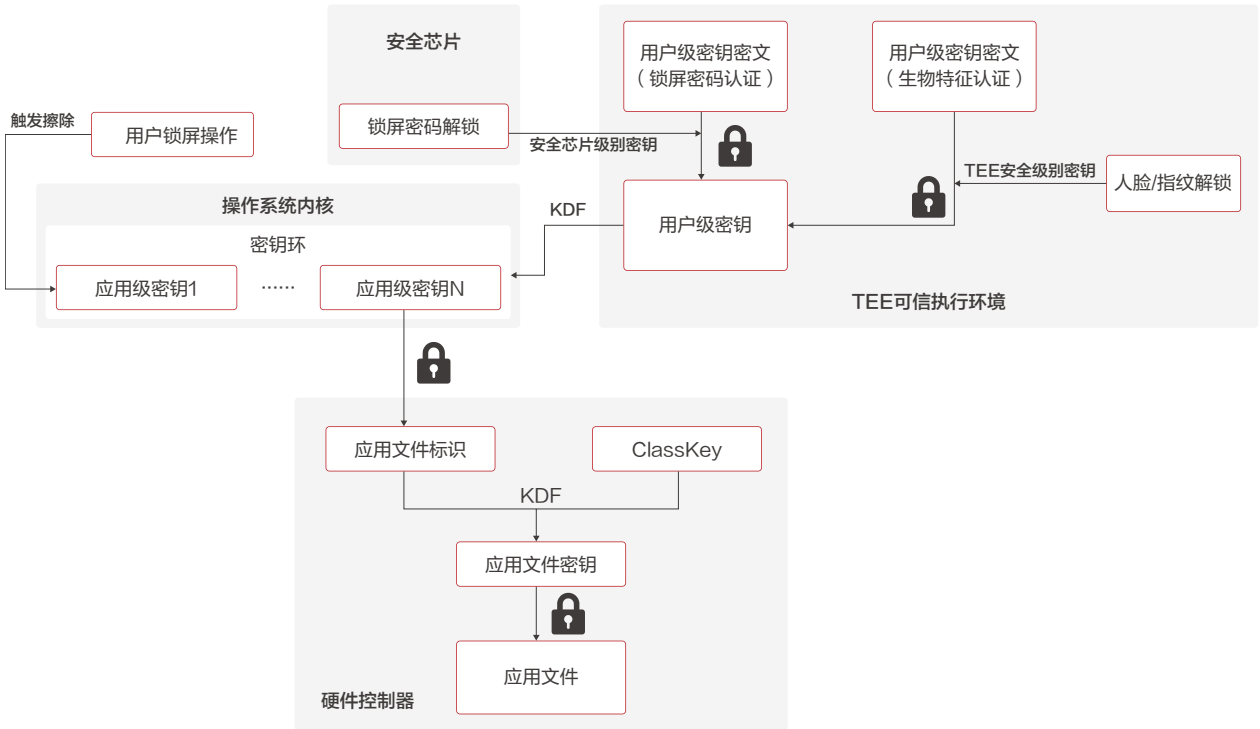
HarmonyOS 支持文件级加密功能，利用内核的加密文件系统模块和硬件加解密引擎，采用 AES-256 算法的 XTS 模式实现加密。

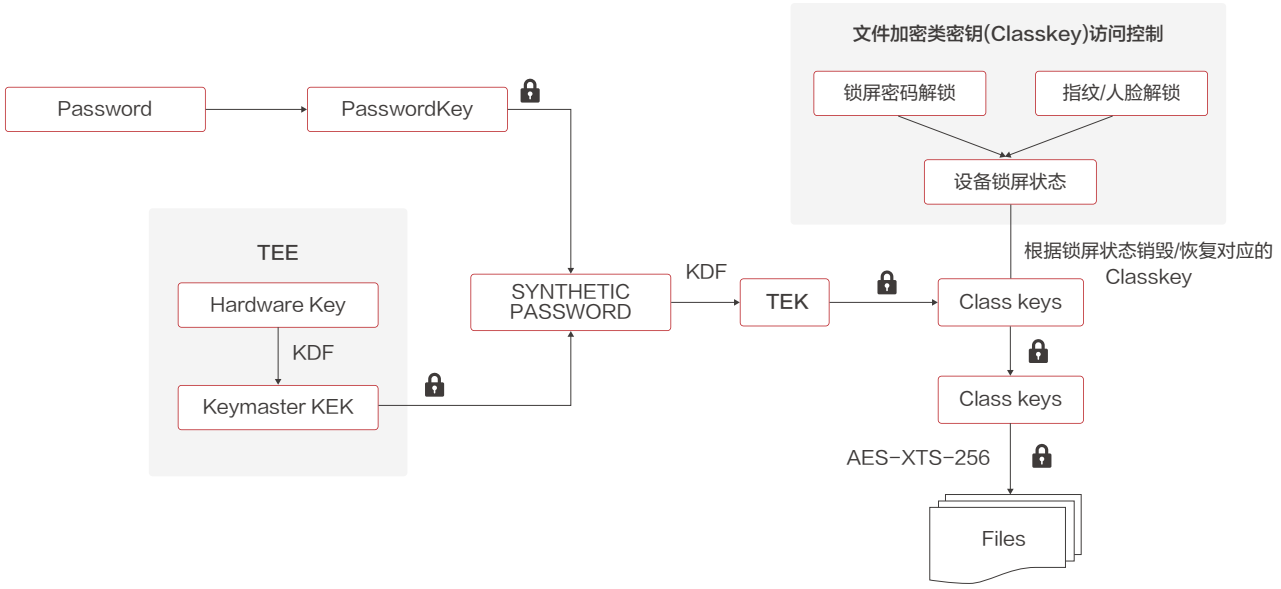
为兼顾用户数据安全和应用体验，基于不同的数据风险等级，HarmonyOS 提供了以下几种方案（以手机系统为例）：

▸ 与硬件密钥、设备锁屏密码配合的数据加密方案（EL1/EL2/EL3/EL4/EL5）：此类方案中加密数据的类密钥（Class Keys）被用户的锁屏密码和设备唯一密钥 HUK 共同保护。具体细分如下：

加密等级	说明
EL1	与设备锁屏密码无关的加密方案：EL1 类保护方案中数据是否可访问与设备锁定状态无关，受 EL1 方案保护的数据在手机一上电后即可访问，如壁纸、闹钟、铃声等。该类密钥被设备唯一密钥 HUK 保护，与锁屏密码无关。
EL2	此类数据在开机后用户首次输入锁屏密码解锁之前不能访问，重新锁定屏幕后数据仍然可以被访问。 设备开机，同时用户输入正确的锁屏密码解锁了设备之后，对应的 ClassKey 才可使用。
EL3	在 EL2 方案基础上增强。在设备锁定时，受 EL3 方案保护的文件不能打开，但可以新建和写入文件，比如支持在后台下载写入邮件附件。 设备锁屏之后，对应的 Classkey 从系统中临时清除，应用打开已有文件场景下，此时对应的 ClassKey 不可用；应用新建文件场景下，系统临时恢复此文件对应的 Classkey；设备被用户再次解锁之后，对应的 Classkey 在系统中恢复；
EL4	在 EL3 方案上进一步增强。在设备锁定时，受 EL4 方案保护的文件不能打开或者新建，直至用户解锁设备。 设备锁屏之后，对应的 ClassKey 从系统中临时清除； 设备被用户再次解锁之后，对应的 Classkey 在系统中恢复；
EL5	APP 可被独立调度且不允许后台驻留，因此，当 APP 被调度时，它的数据沙箱的加密密钥被激活；当 APP 被终止或者挂起时，它的数据沙箱的加密密钥被销毁。基于此，最大限度的减少了数据暴露的风险敞口，消减了攻击面。 不同于 EL2/3/4 的用户粒度的密钥体系，EL5 方案依照更为精细化的应用粒度构建密钥体系，以支撑操作系统在用户锁屏后按需擦除应用密钥。特别地，对于只设置了锁屏密码的设备，在用户每次锁屏后，受 EL5 类方案保护的应用数据，都有机会享受和开机后用户首次输入锁屏密码解锁之前的 EL2/3/4 数据同等的安全性。 从使用规格上看，在设备锁定后，操作系统擦除某个应用的密钥之前，此应用的数据可以继续被访问（同 EL2）；但在设备锁定后，某个应用的密钥被操作系统擦除之后，此应用的已有数据无法被访问（同 EL4），但可以新建和写入文件（同 EL3）。

图 6-1 终端设备文件级加密的密钥层级



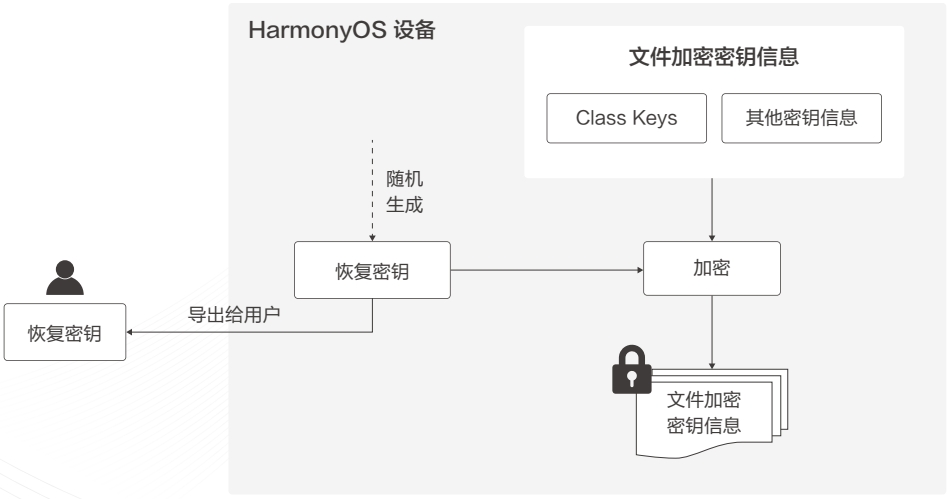


上图为 HarmonyOS 移动终端设备文件级加密的密钥层级；

对于芯片平台提供了硬件级加密能力的设备，上图的文件加密相关的 Class keys 以及 File Keys 的明文全部在 TEE 侧生成 / 存储 / 使用以及销毁，确保文件加密的密钥明文不在 REE 侧存在，增强了文件级加密的安全性；

恢复密钥

HarmonyOS 提供了文件系统解密恢复功能，用户可利用事先授权创建的恢复密钥来解密恢复磁盘中已加密的文件数据，从而在主板器件故障、用户遗忘锁屏密码等场景下提升用户数据的可用性。



上图是恢复密钥机制的密钥关系示意。用户触发导出恢复密钥时，系统将生成安全随机数作为恢复密钥，并使用该恢复密钥加密保护系统中的 Class keys 等文件加密密钥信息，其中恢复密钥导出给用户进行保存管

理、HarmonyOS 系统中不做持久化存储；恢复密钥加密保护的文件加密密钥信息将落盘、持久化存储在磁盘数据区域。

说明：恢复密钥机制仅在部分 HarmonyOS 产品上提供。

6.3 HarmonyOS 数据传输安全机制

HarmonyOS 分布式连接安全

为保证 HarmonyOS 分布式系统的连接安全，实现用户数据在各设备之间的安全流转，系统需要连接的设备之间相互正确可信：即设备和设备之间建立过可信关系，并能够在验证可信关系后搭建安全的连接通道，实现用户数据的安全传输。设备之间的信任关系包括同一华为账号设备之间的可信关系，以及点对点绑定的设备可信关系。

同一华为账号的设备连接安全

为保护登录同一账号设备之间的连接安全，HarmonyOS 设备认证服务提供基于华为账号身份的设备认证能力。设备在登录账号后，将会在端侧生成椭圆曲线公私钥对，作为本机在该账号下的身份认证凭据，并向华为云服务器申请对其公钥凭据进行证明。私钥凭据则仅在端侧存储，不会被服务器获取。

当同账号的设备在近场被软总线发现并进行同账号组网时，设备认证服务将基于双方设备的公私钥对进行认证与会话秘钥协商。认证成功后，软总线安全通道将使用设备认证服务提供的会话秘钥对传输的数据进行 AES-GCM 加密，使得即使蓝牙与 WIFI 发生漏洞时，通道上传输的数据也是被端端加密保护的，确保只有同账号的设备能解密。该会话秘钥仅本次会话有效。

基于点对点绑定关系的设备连接安全

对于两个设备是非同账号的场景，如果用户期望在这两个设备间发起分布式业务，则需要先将这两个设备建立点对点的可信关系，以确保连接的不是攻击者的设备。HarmonyOS 的设备认证服务提供基于点对点绑定关系的设备认证能力。

为保证这种可信关系真实可信，建立时用户需要强感知地手动参与，例如扫描另一设备上的二维码、输入另一设备上显示的随机 PIN 码等。

HarmonyOS 的设备认证服务将基于用户手动在设备间共享的秘密信息（如 PIN 码等），执行 PAKE 安全协议，在协议认证完毕后，建立安全通信信道。同时，设备端侧将分别生成各自的椭圆曲线公私钥对认证凭据，在已建立的安全通信信道上交换并存储对端设备的公钥身份认证凭据。由于该安全通信信道被用户参与的共享秘密信息保护，因此即使在蓝牙与 WIFI 发生漏洞时，所交换的公钥身份认证凭据也无法被有效劫持替换，防止攻击者植入仿冒的身份。

数据分级传输管控安全机制

数据跨设备传输场景下，为了确保用户数据和隐私不泄露，高风险等级数据要求不能在用户无感的场景下从高安全等级设备泄漏到低安全等级的设备，同时低安全等级的设备也不能获取高安全等级设备的高风险等级数据。

基于此原则，HarmonyOS 分布式系统提供了与数据风险等级相应的跨设备访问控制机制，保证跨设备数据传输的目的设备应具备与数据风险等级相匹配的设备安全等级：

数据接收方的设备安全级别	SL5	SL4	SL3	SL2	SL1
允许传递的数据风险等级	S0~S4	S0~S4	S0~S3	S0~S2	S0~S1

如果数据接收方设备不具备与数据风险等级相匹配的设备安全等级，那么必须在数据发送端设备上经过用户明确的授权允许之后，对应的数据才能够传输；

上述访问控制机制在 HarmonyOS 分布式数据库、分布式文件系统中实施，业务可以通过使用此分布式能力在 HarmonyOS 分布式系统建立了信任关系的设备之间安全的传输数据。

HarmonyOS 数据端端加密同步机制

HarmonyOS 提供数据端端加密同步机制，保护用户的敏感数据（如应用账号密码、WIFI 密码、登录 token 等），只有用户的设备可解密，即使是华为也无法访问云同步敏感数据。

当用户在设备侧开启敏感数据端端加密同步能力时，存储在关键资产服务中的敏感数据将被仅用户可访问的密钥加密，以密文形态上传到云，在用户的设备间同步。

HarmonyOS 以信任链传递的方式确保仅用户的设备可获取端端加密敏感数据，即使用户的账号失窃，或攻击者突破传输通道，以端端加密方式同步的敏感数据也无法被解密：当用户使用新设备登录账号时，如需获取已端端加密同步的敏感数据，用户需要验证已开启该能力设备的锁屏密码，或在这些设备上进行动态随机验证码验证。该验证流程将基于 PAKE 的安全协议进行交互，验证成功后生成仅本次会话可用的会话密钥，用于加密在设备间传递的数据端端加密同步凭据。同时，由于会话被验证通过后的每会话一密的密钥保护，即使攻击者突破了传输通道，也无法实施穷举攻击。

HarmonyOS 数据加密分享机制

数据的生命周期延伸控制一直是个人数据保护的关键诉求场景。当用户将数据分享给其他人后，如何保证数据接收者按照发送者的预期去使用数据（如：不可打印、禁止转发、禁止截屏、禁止编辑等），是非常关键的数据保护诉求。

HarmonyOS 数据加密分享服务，构建了系统级的身份认证和权限管控机制，为用户提供了数据跨设备传输后（不限定传输途径的）访问管控能力，保证了数据所有者对于数据设置的访问控制策略在接收端能够忠实执行。

账号级数据保护凭据

设备登陆账号后，数据加密分享服务会基于账号身份生成两对椭圆曲线公私钥对，分别用于消息签名和数据加解密，并在系统密钥管理服务内进行管理。

当用户需要为数据设定访问控制权限时，可以指定数据具体执行权限（如是否可打印、是否可截屏、是否可编辑）和授权访问用户信息（指定可访问该数据的接收方账号）。数据加密分享服务会使用签名私钥对上述信息进行签名，证明权限来源的合法性。同时，数据加密分享服务会对数据进行 AES-GCM 加密生成数据密文；并将数据加密密钥（AES-GCM 密钥）和访问控制权限信息打包为数据权限文件，基于接收方数据加密公钥进行加密。

绑定访问控制策略的加密数据格式

当用户指定了数据访问控制权限后，系统数据加密分享服务会使用账号级数据保护凭据计算生成加密数据。该加密数据主要包含两部分：数据密文与数据权限文件密文。

数据的接收方如果想要访问数据明文，必须先获取数据加密密钥（AES-GCM 密钥）。根据当前的加密数据格式，数据加密密钥作为数据权限文件的一部分，被数据所有者指定的接收方数据保护凭据公钥加密。授权用户设备上的系统数据加密分享服务，会使用本地管理的数据保护凭据私钥进行解密，并验证数据权限文件的完整性（使用数据所有者的数据保护凭据公钥验签）；解密后会获得数据执行权限和数据加密密钥，后者会进一步用于解密数据密文获得明文数据。

系统数据加密分享服务定义了绑定访问控制策略的加密数据格式，保证了用户对数据设置的访问控制权限不可剥离、不可篡改；任意非授权的用户都无法解密数据权限文件。

基于动态沙箱的数据权限管控

为实现数据在接收方的延伸控制，用户选定应用访问数据时，系统数据加密分享服务会将发送方指定的数据执行权限，映射为读取该数据的应用权限，并安装对应权限的应用沙箱；该沙箱对于底层系统服务（包括文件系统、以及屏幕控制、打印服务等）的访问控制权限，全部由系统数据加密分享服务定义。当该应用沙箱访问数据时，对底层系统服务的访问行为均受到系统控制，从而保证发送方设置的数据执行权限在接收方得到管控。

6.4 HarmonyOS 数据销毁安全机制

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。

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

6.5 HarmonyOS 数据分析隐私保护体验

防窥保护

HarmonyOS 提供创新性的主动隐私保护能力，主动智能感知用户在使用设备的过程中可能遇到的隐私泄露风险，并结合多种保护手段帮助用户及时规避风险，从而确保用户敏感信息的安全。

用户使用设备中，隐私信息被他人偷窥是日常隐私泄露的典型场景。HarmonyOS 主动隐私保护机制为用户提供主动隐私防窥体验。当用户启用防窥保护功能后，可以将任意应用添加到保护列表中。当这些受保护的应用处于设备前台运行或者在任务切换窗中部分显示时，防窥保护功能会在风险场景下自动生效。在识别到潜在的隐私泄露风险时，系统会通过实况窗提醒用户窥屏风险，或使用窗口蒙层主动遮盖敏感内容，帮助用户保护其敏感隐私信息免遭他人窥视。在这种主动隐私保护机制下，用户可以更加安心地浏览和处理隐私信息，并在隐私泄露风险发生时更及时做出应对，从而降低隐私泄露的可能性。

防窥功能如何保护用户隐私

防窥保护功能通过使用智能算法来主动感知用户在当前的使用环境下，其设备屏幕中所显示的隐私内容是否面临潜在的窥视风险。系统会首先判断当前是否为用户本人在使用设备，确认是用户本人后，会持续感知用户周围是否存在他人正在持续窥视用户屏幕。

当检测到处于风险场景时，系统会在设备上方显示实况窗，提醒用户“留意屏幕隐私”。用户可根据实况窗的提示，及时采取措施，例如调整设备角度或主动遮盖屏幕，以防止敏感信息继续被他人窥视。如果用户正在浏览隐私相册，系统会自动为整个隐藏相册添加蒙层，只有当用户手动解除蒙层后，隐藏相册的内容才会继续显示。

智能穿戴设备的防窥体验

除了在被窥屏设备上发起提示，HarmonyOS 同样支持在用户的可信设备上发起窥屏提示，使用户可以更及时感知设备被他人访问风险，减少隐私信息泄露的担忧。

用户可在手机已绑定的智能手表上启用防窥提醒功能。当手机中的受保护应用处于设备前台时，如果用户本人并未在手机感知范围内，且系统感知到他人正在持续注视用户手机屏幕，则会在用户的智能手表上显示通知“屏幕被他人注视”，提醒用户自己的手机上的敏感信息处于被他人偷窥的风险状态。

多样化的应用防窥体验

HarmonyOS 致力于为用户提供更优质的隐私保护体验。基于系统构建的基础防窥功能，生态应用可打造多样化的防窥体验。应用可获取屏幕窥视状态，做出个性化的应对，从而更好地保护用户的隐私信息。例如，在非设备机主状态下，应用可以自动隐藏应用内的敏感社交信息，同时使用系统的窗口蒙层，让用户在使用的过程中更加安心。

HarmonyOS 个人智能计算

07

7.1 HarmonyOS 个人智能计算设计理念

AI 大模型的快速发展，模型越来越大、支持场景也越来越多，手机、平板、PC 等终端设备难以运行大规模、复杂的 AI 模型，以用户为中心、以云助端的端网云协同 AI 系统已经是大模型发展和应用趋势。用户的 AI 请求从终端通过网络延伸到云，面临来自端网云更广泛的安全威胁与个人隐私泄露风险，亟需端到端安全与隐私保护的应对策略。为此，我们基于华为端管云全栈协同优势，设计实现了 HPIC（HarmonyOS Personal Intelligent Computing）– HarmonyOS 个人智能计算平台，一款专为 AI 时代用户打造的、业界领先的端网云协同 AI 安全与隐私保护方案。

HPIC 采用 CPAT 设计理念：

1. 用户数据自主掌控（Control）；

2. 个人专属计算空间（Personal）；

3. 匿名认证网络隐踪，用户来无影、去无踪（Anonymity）；

4. 服务可信启动，计算过程透明可验证（Transparency）。

用户数据自主掌控

用户请求需经过加密处理才能发送给计算节点，数据加密密钥由安全芯片随机生成，且只用于一轮交互——一次一密。数据流经开放网络时采用多重加密机制，保障全链路端到端安全。AI 请求在 HPIC 节点进行处理时处于可信执行环境中，严格遵循用户自定义的策略进行数据处理，是用户可安心使用的私人数据保险箱。

个人专属计算空间

HPIC 为用户打造私有计算空间，AI 计算任务执行时独享内存空间，任务完成后释放内存并自动销毁上下文，严格执行数据清除策略——用后无痕。通过无特权架构设计，HPIC 确保任何人都无法触及用户数据，即使是系统管理员也无权访问 – 特权归零。

匿名认证网络隐踪

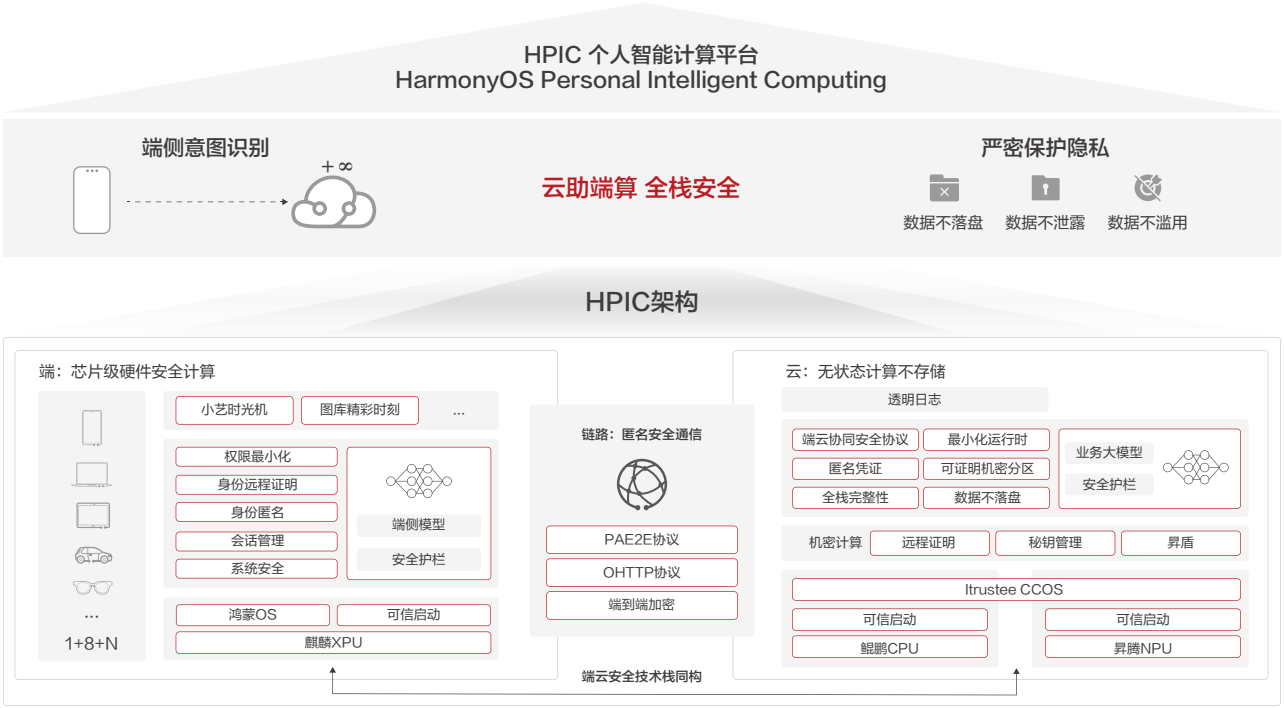
用户调用 AI 服务需提前获取匿名凭证，在云服务器对用户进行匿名校验，仅授权用户可使用 AI 服务，云服务器仅看到匿名化处理过的推理请求，无法关联真实用户身份或构建用户行为画像。网络采用隐私中继协议隐匿传输路径，无法从云服务器逆向溯源至发起请求的用户，防范对特定用户的针对性攻击。

透明可验证

HPIC 在提供服务前需证明节点处于可信状态，用户只有在验证节点可信的情况下才会发起 AI 请求；HPIC 系统设计遵循最小权限和最小攻击面原则，提供可信运行环境、可观测接口、及透明日志，实现操作的可见、可查与可证。

7.2 HarmonyOS 个人智能计算达成的目标

HarmonyOS 个人智能计算（HPIC）为华为智能服务带来了开创性的隐私和安全保护，将行业领先的设备安全模型引入云端，支持处理密集型请求。华为将尽可能在设备本地处理用户任务，但复杂的场景需要借助云端更强的 AI 模型，以便为用户提供更丰富的功能体验。HarmonyOS 个人智能计算将设备安全防护能力延伸至云服务器，保障用户数据处理的安全性和隐私性。云侧 AI 模型推理运行在可信、机密环境中，除了用户本人外，任何他人和公司都无法获取其数据。下图为 HPIC 架构示意图。



面向未来，HPIC 从芯片到云，全栈自控、全程可见，守护每一位用户的自主与安心：

芯片级信任起点：可信计算，从根而始

HPIC 安全会话通过手机、平板、PC、云服务器等终端的硬件安全芯片进行可信认证与密钥协商来建立，由（SE/TPM 等）硬件安全模块生成唯一密钥，并确保所有安全行为均基于可测、不可篡改的硬件可信根执行。

鸿蒙内核安全底座：系统即安全，内生可信

端云统一基于鸿蒙技术栈同构安全内核构建，确保应用运行在一致可信、安全隔离、权限可控的系统安全之上。

多重安全隔离空间：任务即世界，只算不留痕

每次任务请求在可信容器、TEE 等隔离区中执行，数据在可信环境中使用，计算完成即删除。确保不同用户 / 会话数据隔离，杜绝信息交叉风险。

数据密钥自控机制：用户唯一，有钥无忧

所有端云交互数据均通过设备本地唯一密钥加密，非 HPIC 安全环境和用户授权无法解密，云侧数据使用完全由用户自主掌控。

可信计算空间：全程透明可控，看得见，用得明

所有 AI 推理任务均运行于隔离、即时、用户可控的云侧执行空间中。支持设备对调用内容、运行模型、使用数据的全过程可视化，做到“看得见的智能”。

身份隐匿防追踪：默认匿名，来去无踪

用户身份使用可吊销、用途受限的凭证进行匿名认证，全程隐藏用户真实身份。网络采用隐私安全协议，云服务器无法获取用户真实 IP 地址、设备信息和用户身份，有效防止网络行为被追踪，最大程度降低用户信息泄露风险。

7.3 用户数据自主掌控

针对用户使用 HPIC 节点推理的隐私，HPIC 采用端云协同数据保护架构来保护用户的隐私。密钥由用户掌握在设备中，HPIC 节点无法追踪用户身份：

HPIC 节点身份可信

仅具有符合 HPIC 定义安全机制的节点会被颁发 HPIC 节点证书。端侧 HPIC 服务在收到连接请求时，将对 HPIC 节点发起可信验证，以挑战应答的方式防止重放攻击，确保 HPIC 节点的证明新鲜可信。普通的云计算节点或被撤销的 HPIC 节点设施将无法通过端侧的验证。

验证过程可信

鸿蒙 HPIC 服务将在可信安全环境与安全芯片内对 HPIC 节点发起验证。在验证 HPIC 节点可信后，基于 HPIC 节点的公钥发起会话密钥协商。基于可信安全环境与安全芯片的保护，该验证过程与会话密钥协商过程将无法被破坏，攻击者无法篡改验证的结果。

密钥掌握在用户手中，端与 HPIC 节点之间直通端端加密

在验证 HPIC 节点可信的前提下，端侧 HPIC 服务才接纳 HPIC 节点的公钥凭据，并在端侧生成临时的公私钥对，与 HPIC 节点发起会话密钥协商。该会话密钥将用于加密端侧与 HPIC 节点的通信数据，且不依赖 TLS 通道的安全性。仅当 HPIC 节点获取端侧 HPIC 服务授权的会话密钥后，通信数据才能解密。

会话密钥使用范围最小化

HPIC 采用以下机制达成不同业务与会话的隔离，确保会话密钥在最小化范围使用：在不同业务发起 HPIC 连接请求时，端侧 HPIC 服务将针对不同业务生成不同会话密钥；每当业务结束上一轮会话，开启新的会话时，端侧 HPIC 服务也将生成新的会话密钥，旧的历史会话密钥将无法解密通信密文。

身份匿名，HPIC 节点无法区分端侧用户身份

用户使用端侧设备可以与 HPIC 节点之间发起连接，但 HPIC 节点无法区分端侧用户身份。

端侧 HPIC 服务在连接 HPIC 节点时，将不携带任何固定账号标识。匿名身份服务将为端侧 HPIC 服务颁发基于盲签名技术的匿名凭据，该凭据可用于证明当前请求来自于合法的终端设备。终端设备在经过一定业务周期后，将重新申请新的匿名凭据。HPIC 节点无法将该匿名凭据关联到个人，也无法将不同时间周期的匿名凭据关联到同一用户。

7.4 个人专属计算空间

HarmonyOS 个人智能计算基于《信息安全技术 机密计算框架》要求，结合硬件层、系统软件层、服务层、应用层和跨层管理的安全功能和特性，并结合互联网业务的实践，定义了 HPIC 的系统安全框架。

云基础设施安全框架

HPIC 为用户打造私有计算空间，AI 计算任务执行时独享内存空间，任务完成后释放内存并自动销毁上下文，严格执行数据清除策略——用后无痕。通过无特权架构设计，HPIC 确保任何人都无法触及用户数据，即使是系统管理员也无权访问 – 特权归零。

云侧基础设施安全框架包括硬件层、系统软件层、安全服务层和应用层。

各层基础设施的分工：

1. **硬件层**提供硬件基于 TPM 和 TEE 的可信根，度量根来自 TPM，端云数据通信的根密钥来自 TEE，隐私计算环境涉及 AI 推理，对应硬件包括 CPU 和 XPU；

2. **系统软件层**有两条技术路线：机密计算方案和裸机安全 OS 方案，硬件层利用硬件安全特性提供高安全性的机密虚机和机密容器的隔离环境，软件层不依赖硬件利用高安全性的 OS 提供安全的运行环境，最小化系统必要的功能，减小攻击面，提升安全性，在此基础上提供软件分区隔离和权限访问控制的特性实现隐私数据的隔离保护，两条技术路线互相配合，机密虚机中部署安全 OS 是隔离外部访问和提升内部安全性的更优解决方案；

3. **安全服务层**基于系统软件和硬件安全特性为上层应用提供安全服务；

4. **应用层**管理端云会话，提供大模型推理业务，响应端侧推理请求，安全地完成推理并返回结果。

系统安全

云服务的系统安全

云侧系统安全基于 ARM TEE 和 TPM 的硬件可信根的安全能力，启动时通过安全启动和可信启动保证系统软件的完整性，运行时通过微内核架构的安全 OS 保证应用和容器镜像的完整性和隐私数据的机密性。

安全启动对系统固件和安全 OS 组件进行数字签名验证，逐级校验，确保加载并运行合法的授权固件和

OS 组件；安全 OS 初始化过程中导入数字签名的应用完整性 hash 值列表，应用启动时校验完整性，确保只有授权的应用才能在 HPIC 节点上运行；容器镜像在启动时，同样进行数字签名验证保证其完整性，安全启动链从系统固件一直延伸到应用。可信启动对系统固件和安全 OS 组件进行度量，安全 OS 度量上层应用，逐级度量并将度量值扩展到硬件 TPM 上，最终生成 TPM 签名的度量报告，向用户提供远程证明的能力，验证 HPIC 节点安全性。安全启动和可信启动确保 HPIC 节点上代码和关键配置文件没有被篡改，实现全栈软件的完整性。

远程证明

远程证明服务以 IETF 中 RFC 9394(Remote ATtestation procedureS (RATS) Architecture)为基础，用于验证云侧平台的可信度和平台中运行软件的完整性。基本理念是通过先进的可信安全硬件和密码学技术，以可信安全硬件为起点，对平台中各部件逐级度量、逐级验证、信任逐级传递，并向远程主体展现平台和软件的真实可信状态，实现信任的可度量、可验证、可传递。

远程证明服务在支持启动度量、运行态度量可信证明基础上，支持容器可信证明。

容器可信证明

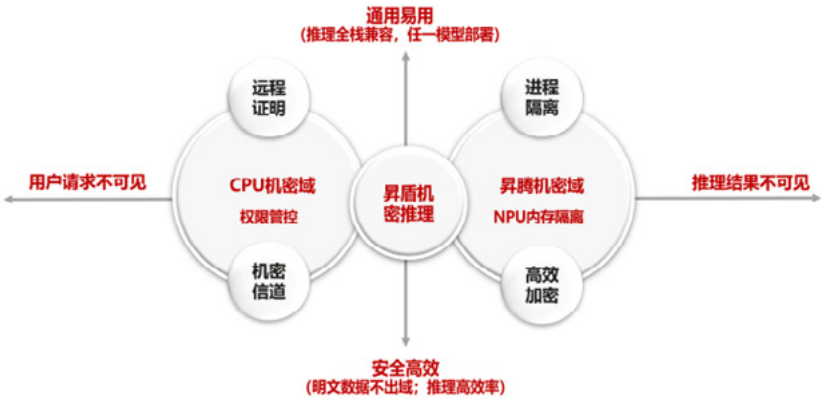
容器可信证明主要分为两步：可信度量和验证、远程证明。

可信度量和验证是在容器启动时，对容器进行可信度量和数字签名验证，并将度量值扩展到可信安全硬件中，确保度量证据不会被篡改。

远程证明是对上报来的度量证据进行可信证明，向远程主体展现平台内容器的真实可信状态。

计算节点机密推理

HPIC 在云端算力底座围绕“明文数据不出机密域“的设计原则，以华为昇腾为主要计算平台，构建异构大模型运行时数据保护能力，使能“数据可用不可见”，确保终端用户的数据在云服务器上不被恶意程序或非法用户窃取。



1. CPU 侧机密域：Harmony 智能云端业务部署在 CPU 侧利用硬件或 OS 加固而构建的机密域中，通过诸如内存隔离、权限管控等技术，实现机密域与普通域的权限隔离，使得系统恶意程序甚至管理员都无法访问机密域内的任何敏感数据；

2. NPU 侧机密域：Harmony 智能云端业务使用昇腾 NPU 加速 AI 计算，同时在昇腾侧部署了昇盾机密计算技术，实现昇腾侧的内存隔离机制，使得 CPU 侧恶意程序甚至管理员无法读取 NPU 侧受机密域保护的模型和用户推理数据；

3. 机密信道：CPU 与 NPU 之间的总线传输使用加密信道保护，利用协商后的密钥，确保数据只有 CPU 和 NPU 的机密域才能正确解密，数据离开 CPU 和 NPU 机密域时都会被加密，实现明文数据不出域。

4. 用户数据不可见：终端用户的推理请求加密传输到云端安全算力底座中，由 CPU 和 NPU 的机密域实现数据的运行时保护，推理结果加密返回给终端用户，确保云端恶意程序和管理员看不见用户的明文数据。

5. 远程证明：CPU 和 NPU 上运行的系统和软件都会经过严格的远程证明，确保运行在机密域上的软件栈没有被恶意篡改，确保云端算力底座的完整性和平台身份的真实性。

计算节点的可信启动

昇腾计算平台基于 TPM 构建了可信启动过程，在这一过程中，系统会对整个可信计算基（TCB）执行哈希链式度量（Measured Boot），并将结果扩展到受保护的 TPM 的 PCR（Platform Configuration Register）寄存器。这里的 TCB 覆盖支撑安全环境的全部系统硬件、固件和软件集合，包括 NPU 的硬件信息、固件、启动加载程序（如 Bootloader）、操作系统内核以及关键驱动程序等。

TPM 内部使用硬件密钥（Attestation Key）对 TPM 寄存器存储的度量值进行密码学签名，生成代表 NPU 身份和安全状态的硬件报告，该报告交由用户通过远程证明进行可信审计。

远程证明服务通过验证硬件报告来判断 NPU 当前的运行环境是否可信，确保 NPU 上软件栈没有被植入恶意程序；只有在验证通过的情况下，NPU 才会接收用户数据执行大模型推理任务，确保机密数据不出 NPU 机密域。

零特权可信作业

为缓解“人因风险”的三类挑战：“人有恶意”、“人会出错”、“人有缺陷”，HPIC 环境进行了如下优化：

1. 在流程规范上，制定了作业元模型 / 作业可信元模型、人因风险模型以及作业可信管理体系要求；

2. 在管控技术上，回收远程 Shell 和 SSH 的接口，在业务运行过程中，禁止远程登录进行系统运营运维；

7.5 匿名认证网络隐踪

在数字化时代，用户隐私保护至关重要。隐私防追踪旨在通过多种手段防止用户在网络活动中的身份暴露和行为追踪。其核心目标是实现请求的匿名性，使云侧无法直接关联请求与具体用户，同时阻止对用户行为的精准画像构建。HPIC 包含 IP 层，TCP/UDP 传输层及应用层的隐私及端到端加密保护，通过 IP 盲化和身份匿名（包含用户 ID、设备 ID 等），匿名凭据认证及端到端加密等措施来防止云侧对用户的跟踪，实现了对用户的全栈的安全及隐私保护。

PAE2E	数据保护防泄露
OHTTP	隐匿 IP 防追踪
HTTPS	基础传输安全

OHTTP 协议防 IP 追踪

OHTTP（Oblivious HTTP）协议是实现隐私防追踪的关键技术之一，通过隐藏端侧 IP 地址，实现网络非目标性，有效防止针对特定用户的攻击。

①**终端与服务器的 IP 隐藏**：在 OHTTP 协议下，终端设备发起请求时，不知道目标服务器的真实 IP 地址，服务器也无法获取终端设备的 IP 地址。这种双向隐藏机制，使得攻击者难以通过 IP 地址信息对特定用户或服务器进行针对性攻击。

② **OHTTP Relay 的角色**：OHTTP Relay 作为中继节点，知晓终端和服务器的 IP 地址，但无法解密传输的数据内容。它负责在终端与服务器之间转发请求和响应，隔离终端与服务器的直接连接，进一步增强隐私保护

③ **Oblivious GW 的数据处理**：Oblivious GW（网关）在数据传输过程中，能够处理用户数据，但无法对其进行解密。它确保数据的完整性和安全性，防止用户数据在传输过程中被中间节点窃取或篡改。

Enhanced Private Pass 协议防 ID 追踪

Private Pass 标准协议采用密码学盲签名机制对授权令牌 Token 进行盲化和签发，保证了授权令牌 Token 的匿名性，同时也提供了 Token 的合法及可认证性。基于 Private pass 标准增强了令牌盗用的安全特性，利用零知识证明系统（Non-interactive Zero-Knowledge Proof）实现了令牌防盗用攻击。令牌 Token 分为长期匿名 Token 令牌和会话级别的一次性匿名 Token 令牌，其中长期 Token 用于用户身份的长期认证，而会话级别的一次匿名 Token 则用于单次会话或特定时间段内的身份验证。利用双 Token 机制，可以消减 Token 之间的可关联性，使得服务器无法通过申请服务的短期 Token 推测出用户的身份信息，从而提高用户隐私保护。此外，由于使用盲化 Token 申请机制，消除用户身份和消盲后 Token 之间的关联，

即使 Token 在传输和使用过程中被截获，攻击者也难以得到 Token 和用户真实身份信息的关联，从而达到对用户身份的隐私保护。

PAE2E 端到端加密协议防数据追踪

带隐私保护 0-RTT 端到端密钥协商加密机制 (0-RTT PAE2E): 0-Round-Trip-Time Private Authenticated E2E 是一种快速可认证会话密钥协商协议，允许在建立安全连接时实现会话密钥协商并立即发送加密数据，无需等待密钥协商握手过程完成。由于延迟减少，用户体验会得到显著提升。协议中对用户的认证基于一次（One-Time）会话匿名认证 Token 令牌，对服务端的认证基于服务端的长期可认证密钥。在双向认证基础上可以实现 0-RTT 密钥协商并构建用户到 HPIC 的端到端安全通道，实现用户数据的端到端保护。由于每次会话密钥协商使用了（One-Time）一次性会话匿名认证 Token 令牌，消减了攻击者可以重放 0-RTT 数据包的安全风险。

7.6 透明可验证

透明日志全程可验

为了提升用户对 Harmony 隐私智能计算的信任，HPIC 除了提供云侧高安全性的系统底座，并支持设备可信状态远程可证明外，还将远程证明的过程透明以供用户进行二次核验。HPIC 将远程证明过程中的度量日志和证明依赖的基线数据发布到一个仅可附加且防篡改的日志中，该日志的构建利用了透明日志技术。

透明日志是一种基于密码学的数据记录系统，广泛应用于证书管理、区块链、软件供应链等领域，其核心目标是确保日志内容的不可篡改性、可验证性和公开可审计性。它通过特定机制（如 Merkle 树）将数据条目按顺序追加存储，并提供数学证明（如一致性证明、存在性证明），使得任何人都能独立验证日志的完整性和条目有效性。

透明日志的关键特性如下：

仅追加性 (Append-Only): 新的记录只能添加到日志的末尾。一旦记录被添加并确认，就无法修改或删除之前的记录。这种特性通过数据结构（如哈希链或默克尔树的构建方式）来保证。

防篡改性 (Tamper-Evident): 对日志历史记录的任何未经授权的更改（包括插入、修改、删除、重排序）都会破坏其密码学结构，导致验证失败，从而可以被轻易检测到。日志本身不一定“防篡改”（Tamper-Proof），但任何篡改都会留下明显的证据（Tamper-Evident）。

可公开验证性 (Publicly Verifiable): 任何人都可以获取日志的（部分或全部）数据和密码学证明，并独立执行验证算法，以确认：

- 日志的当前状态是否包含了某个历史状态（一致性）。
- 某个特定的条目是否确实包含在日志的某个已知状态中（包含性）。

HPIC 节点的可信状态每个自然月会被远程证明一次，验证失败的节点会被下线，以保证用户的推理请求只会发给云侧经证明安全的可信环境。为了保证公开可验证，HPIC 对外开放 API 接口查询远程证明的度量日志和基线数据，白名单内的安全研究人员或学者可通过接口查询到的数据，对远程证明的过程进行回放，从而实现对云侧 HPIC 节点可信状态的二次核验。

7.7 典型业务能力介绍

小艺时光机：AI 点亮生活，留驻精彩时光

小艺时光机是小艺官方出品的智能体，根据用户的每日生活，如运动记录、拍过的照片、去过的地方推荐值得记录的特别时刻。用户可以编辑保存至“我的手记”，逐渐形成专属于个人的人生杂志，方便用户沉浸式浏览精彩的生活点滴。精彩时光推荐中涉及游记、日记等的 AI 文案，均通过 HPIC 个人智能计算云上的计算能力生成，在 HPIC 的安全技术保障下，华为也无法触碰到用户的私有数据，用户可以放心浏览到独属于自己的精彩内容。

小艺简报：专属小艺生成的，符合用户当下情景的 AI 简报

小艺简报是小艺建议的子特性，为用户提供当下的、与个人相关的简报。通过桌面的小艺建议卡片或者客户消息通知在恰当的时机推送给用户，包含三大类卡片内容：效率信息类（如：信息摘要简报）、情感健康类（如：睡眠简报）、学习发展类（如：每日播客）。小艺通过 HarmonyOS 智能服务提取用户备忘录、日历日程、短信中的待办信息，按重要优先级顺序，基于 HPIC 个人智能计算云上的计算能力，为用户生成全局待办简报。全方位保障用户的隐私与数据安全。

小艺通话：智慧通信新体验，安全与智能的深度融合

小艺通话是华为基于 HarmonyOS 打造的智慧通信服务，以“安全为基、智能为核”为核心理念，通过创新技术将传统通话中的“听得见”升级为“看得见、读得懂、用得上”的多维体验。小艺通话不仅是一次通信方式的简单调整，更是对用户隐私与效率双重需求的深度响应，为用户提供从拨号前的智能辅助到挂断后的信息管理的全链路通信守护。用户可在拨号盘一键启用“小艺通话”，系统会基于通话语音实时生成文本，也提供通话摘要、通话翻译服务；小艺通话摘要、翻译从本地大模型过渡到基于 HPIC 的云侧个人智能计算云中，使用云端更强大的模型计算能力的同时，也确保在设备端对等的安全计算环境中处理用户的通话数据，让用户在隐私保障的前提下，享受自然、高效、可信赖的智能服务；小艺通话，让跨语言沟通更轻松，让信息管理更可信，让通话体验更安心。

HarmonyOS 生态治理

08

HarmonyOS 对于应用生态和设备生态，都提供了相应的纯净治理机制，来确保运行在终端上的应用程序和 IOT 设备，满足 HarmonyOS 的安全标准规范，严格遵循数据安全与隐私保护要求，保护消费者的权益。

8.1 HarmonyOS 应用程序生命周期治理概述

图 8-1 HarmonyOS 应用程序生命周期的治理架构

HarmonyOS 应用程序生命周期的治理架构，从应用的开发、上架、发布、安装、运行、卸载，进行全生命周期管理。确保开发者开发出符合安全及隐私规范的应用，并且做到应用来源可信，同时使应用全生命周期内应用完整性得到保证。在运行阶段，确保应用的运行可信，消费者的隐私与数据安全得到保护，应用对消费者无骚扰，做到恶意行为可追溯可管控。

在应用上架发布阶段，我们应确保应用质量。应用程序应该满足权限最小化，数据使用公开透明，无不良内容，无恶意行为等基本要求。同时也要保证开发者的应用程序安全可用不被篡改，开发者的知识产权受到保护。

在应用运行阶段，我们首先确保应用运行环境安全，同时也要确保应用行为可知可控。对有恶意行为的应用，要建立分级管控措施，根据应用行为的严重程度，按要求对应用的权限或能力、应用安装包、应用开发者等采用不同粒度的管控方式。

如上图所示，我们在应用全生命周期的不同阶段，分别提供不同的关键技术和措施，来解决生态构建的重大挑战问题。

8.2 HarmonyOS 应用程序“纯净”开发

对于 HarmonyOS 开发者，提供开发者注册、账号管理、实名认证，并进行开发者证书管理，开发者的应用开发以及调测提供配套管理能力。

开发工具提供安全能力，帮助开发者进行代码级以及二进制相关的安全与隐私检查，确保开发者能够快速开发出高质量 HarmonyOS 程序。

同时，DevEco IDE 为开发者提供应用来源管控和完整性保护的安全能力，例如：DevEco IDE 能够自

动化帮助开发者进行秘钥的生成和管理，自动化的签名管理、自动化的调试证书管理和自动化的调测设备管理，方便开发者开发的应用或服务能够快速上架。

实名认证要求：现行有效的是 2022 年 8 月 1 日开始施行的《移动互联网应用程序信息服务管理规定 (2022 修订)》，同时为了促进生态健康有序发展，保护开发者、用户的合法权益，申请成为一个 HarmonyOS 开发者需要注册账号，注册账号时可以同步进行实名认证，实名认证包括个人开发者实名认证和企业开发者实名认证；确保应用的开发者是可以被追溯的。在应用上架发布环节仍需要实名认证，建议注册时立即实名认证。

8.3 HarmonyOS 应用程序“纯净”上架

在系统收到开发者申请发布的应用，首先会检查应用的完整性在上载的过程中没有被破坏，然后会按照 HarmonyOS 应用检测规范进行安全与隐私检测和人工审核，当应用通过相关检测符合发布标准，系统会完成检测后的重新签名过程，确保 HarmonyOS 应用是经过严格的审核。在这个过程中，确保正确的开发者发布了正确的应用。

HarmonyOS 不仅对 APP 的包（Package）进行了签名，对 APP 运行的内存页表也进行了签名，不只是保证 APP 安装时的可信，也保证 APP 运行时的可信，确保 HarmonyOS 终端没有病毒和恶意代码。

同时我们也提供了应用加密、应用签名等功能，保护开发者应用程序完整性和机密性，保护开发者知识产权。

8.4 HarmonyOS 应用程序“纯净”运行

HarmonyOS 在应用安装的时候，会基于 PKI 验证 HarmonyOS 应用的合法性和完整性。

HarmonyOS 为应用程序全新设计了安全隐私保护机制：

- 纯净来源：鸿蒙应用上架到鸿蒙应用市场分发前，应用市场会对应用进行严格地审核，确保鸿蒙应用的安全和质量。应用市场会对经过检测的上架应用进行应用市场重签名。鸿蒙应用签名是鸿蒙应用必须包含的内容，用于校验鸿蒙应用的完整性和来源可靠，只有签名校验通过，才能在应用市场发布，以及在 HarmonyOS 上安装。

- 纯净权限：取消了短信、电话、通话记录等涉及个人数据风险权限，对通信录等权限使用“权限证书”的方式进行严格管控。对图库、通讯录等强制使用 System Picker 方式防止权限滥用行为。

- 隐私访问可知可控：HarmonyOS 提供透明可控机制帮助用户对应用的访问行为可知可控，这些机制贯穿于应用整个运行期间，包括敏感数据或者能力被访问前、被访问中和被访问后各个阶段。

◎ 隐私权限授权（访问前）：开发者必须填写权限使用理由字段，在运行期间应用访问敏感数据或者能力前需要申请相应的权限，用户可结合开发者填写的理信息作出选择；

◎ 隐私指示器（访问中）：敏感数据或能力（例如，相机、麦克风、位置信息）被应用持续访问时，HarmonyOS 通过状态栏显示隐私指示器实时提醒用户，便于用户感知应用对敏感数据或能力的访问行为。隐私指示器是由 HarmonyOS 系统服务实现；在部分旗舰手机设备，隐私指示器默认支持由更高安全级别的 TUI 渲染实现，TUI 接受 TEE 保护，可防止恶意应用劫持或篡改隐私指示器，确保隐私指示器在极端场景下的可靠显示。

◎ 权限使用记录（访问后）：HarmonyOS 支持用户查看应用访问敏感数据或者能力的历史记录，便于用户完整地审视应用行为。当某个应用长时间未被用户使用或者应用存在风险行为时，HarmonyOS 将对该应用权限进行自动回收，保护用户隐私。

▸ 在鸿蒙电脑上，HarmonyOS 还允许运行来自非官方应用市场签名的外部扩展程序。为了保证鸿蒙生态的纯净安全，系统针对这些外部扩展程序进行了增强防护。

8.5 HarmonyOS 设备生态治理概述

华为通过基于 HarmonyOS 以及 HMS Kit Framework 构建了设备生态的基础框架，同时构建对应的 Kit 能力对设备厂商进行赋能，如：DV Kit 设备虚拟化能力，Cast+ Kit 设备投屏能力等。

为确保 OEM 设备合作伙伴厂商的设备能够获得更好的体验，华为提供了合作伙伴管理平台，确保只有符合资质的厂商，以及设备完成对应的安全认证测试才能批准接入 HarmonyOS 生态，华为会提供了一套完备的设备开发安全规范，帮助设备生态合作伙伴开发出符合生态体验和安全要求的设备。

图 8-2 HarmonyOS 设备生态治理平台

华为提供的设备开发安全规范包括：

▸ OEM 生态开发者认证

▸ 设备安全测评与认证

- 设备安全的授权凭据管理

8.6 HarmonyOS 设备生态合作伙伴认证

为了确保加入 HarmonyOS 设备生态的设备符合 HarmonyOS 生态的体验及安全标准，需要具备对厂商的溯源能力，包括：要求设备厂商必须实名认证，首先在华为的官方网站上先注册华为账号，并完成实名和企业的资质认证，然后在 Device Partner 生态伙伴管理平台同意并签署《华为智能硬件合作伙伴服务协议》，签署后才能正式成为华为生态的合作伙伴。

成为生态合作伙伴后，生态伙伴在华为 Device Partner 合作伙伴管理平台根据产品的认证类型选择对应的合作伙伴的类型，在管理平台的管理中心根据提供的合作计划进行创建产品并登记产品信息，在合作方管理平台上可以获取对应的开发指导和规范，指导设备的开发。

8.7 HarmonyOS 生态设备安全认证

合作伙伴完成生态设备的开发后， 需要根据设备安全分级标准规范进行安全的自检和安全整改，在完成安全整改后，可以提交华为生态认证实验室对设备进行安全认证测试，在设备满足安全等级认证要求并通过认证测试之后， 认证实验室会颁发对应的认证测试证书和徽标文件。

8.8 HarmonyOS 生态设备分级管控机制

为了保证设备的数据在对应的安全等级设备上流动，合作伙伴在选择集成对应的功能时，选择的功能会明确需要的最小安全等级，并且会给出对应的安全等级规范技术要求，设备厂商需要根据对应的安全等级技术规范要求进行开发设备， 在开发完成后，设备在安全认证测试阶段会对设备的安全等级进行认证。

只有符合最小的安全等级测试要求后，设备才能赋予对应的安全等级。华为在合作方管理平台会登记对应设备的安全等级信息，设备在使用时会获取该安全等级信息。该安全等级信息会在云端进行签名，下发对应的凭据，设备在获取安全等级信息时，会发送对应的挑战信息给云端，云端下发经过对 Challenge 和安全等级信息签名的凭据下发，设备侧会进行安全等级导入到安全可信区，并有对应的防回退机制保障无法回退。

华为提供给生态设备的不同的业务 Kit 能力在设备间互操作时，需要评估对方的安全等级，只有在确保对方安全等级符合要求的设备上流动，如业务 A 要求只能在 SL2 安全等级的设备上才能传输， 因此会确认对方设备确实符合要求，才会将数据进行传输，华为会为设备提供分级的管控机制（见 HarmonyOS“正确的访问数据”分级访问控制架构章节）。

HarmonyOS 安全标准遵从与认证

09

HarmonyOS 的设计和实现参考了网络安全、系统安全、数据安全等领域的公开标准，并遵从各国隐私保护法律法规及标准。

HarmonyOS 的鸿蒙内核获得了国际信息技术安全评估通用标准 CC EAL6+ 证书，这是业界通用操作系统内核领域首个 CC EAL6+ 等级认证，标志着华为公司成为全球首个获得该领域最高认证等级的智能终端供应商。CC（Common Criteria）认证是 IT 行业全球认可度最高、行业影响力最大的产品信息安全认证之一，认证遵循国际标准 ISO/IEC15408《Information security, cybersecurity and privacy protection — Evaluation criteria for IT security》，是产品安全评估方面的权威标准，在全球范围内具有广泛的接受度与认可度。

HarmonyOS 获得中国网络安全审查认证和市场监管大数据中心（CCRC）颁发的评估保障级 EAL5 增强级（EAL5+）认证证书，这是业界智能终端整机操作系统领域首个 EAL5+ 等级认证，也是我国操作系统目前能够通过的最高级别安全认证，标志着 HarmonyOS NEXT 的信息安全保障能力在终端操作系统中已达到行业领先水平。中国网络安全审查认证和市场监管大数据中心（CCRC）为国家市场监督管理总局直属正司局级事业单位。依据《网络安全法》《数据安全法》《个人信息保护法》《网络安全审查办法》及国家有关强制性产品认证法律法规，承担网络安全审查技术支撑，以及网络安全相关的产品、管理体系、服务、人员认证等工作。CCRC 的评估保障级 EAL（Evaluation Assurance Level）认证遵循的国家标准 GB/T 18336《信息技术 安全技术 信息技术安全评估准则》，等同采用国际 CC（Common Criteria）认证标准 ISO/IEC15408，是产品安全认证的权威标准。NEXT EAL5+ 安全认证围绕系统安全、应用安全、数据安全、全场景安全等领域开展，证明了鸿蒙生态底座的安全能力；并采用了“半形式化”评估分析方法，增强了安全性评估的准确性和严谨性，验证产品在设计安全、代码安全、实现安全、过程安全和管理安全等方面的能力，证明了 NEXT 在整个生命周期环节持续安全可信。

HarmonyOS 获得中国信息通信研究院泰尔实验室颁发的新型移动智能终端系统安全隐私保护能力测评证书，这是业界首个新型移动智能终端操作系统安全隐私保护能力测评证书，标志着 HarmonyOS 作为一款新型移动智能终端操作系统，已具备领先的安全隐私保护能力。该测评依据 T/TAF 161-2023《移动智能终端个人信息保护规范》、FT-Z09-0020-01《新型移动智能终端系统安全技术要求》等标准要求，对 HarmonyOS 操作系统框架、应用全生命周期、终端管控能力等 38 项指标进行检测，验证了 HarmonyOS 的隐私保护能力。华为终端一直致力于提升系统的安全性和隐私保护能力，HarmonyOS 采用全新的星盾安

全架构，构建端到端的应用安全能力，保护应用自身安全和运行时安全，为应用程序开发、安装、启动、运行、更新等生命周期各阶段提供安全隐私保护能力。

支持 HarmonyOS 产品的设计、开发、维护服务和互联网遵循国际权威标准 ISO/IEC 27001 信息安全管理体系，获得英国标准协会（BSI）的 ISO/IEC 27001 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。获得该认证意味着华为终端软件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。

在 HarmonyOS 版本上，我们已获得：

认证名称	认证对象	颁发机构	说明
CC EAL 6+	鸿蒙内核	荷兰 NSCIB	CC 认证是依据信息技术安全评估通用标准 ISO/IEC 15408 对 IT 产品的安全功能和安全保障能力进行全方位评估，涉及产品的设计开发、安全功能、交付管理等方面，是全球广泛认可的权威安全认证。CC 认证分为 7 个 EAL 级别，级别越高评估越严格。HarmonyOS 内核获得 CC EAL6+ 认证。
评估保障级 EAL5 增强级	HarmonyOS NEXT	中国网络安全审查认证和市场监管大数据中心中国网络安全审查技术与认证中心	该认证基于 GB/T 18336《信息技术 安全技术 信息技术安全评估准则》《移动智能终端操作系统安全技术要求（评估保障级 4 增强级）》标准进行评测，该标准等同采用国际 CC（Common Criteria）认证标准 ISO/IEC15408，EAL5+ 认证从产品的设计开发、配置管理、交付、测试、脆弱性评估等方面对产品的安全性进行全面严格的评估和测试，并采用了“半形式化”评估分析方法，增强了安全性评估的准确性和严谨性，证明了 NEXT 在整个生命周期环节持续安全可信。
新型移动智能终端系统安全隐私保护能力测评	HarmonyOS NEXT	中国信息通信研究院	中国信通院泰尔终端实验室依据 T/TAF 161-2023《移动智能终端个人信息保护规范》、FT-Z09-0020-01《新型移动智能终端系统安全技术要求》等标准要求，对 HarmonyOS NEXT 操作系统框架、应用全生命周期、终端管控能力等 38 项指标进行检测，验证了 HarmonyOS NEXT 领先的安全隐私保护能力。
ISO/IEC 27001	华为终端有限公司 华为终端软件	英国标准协会	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。获得该认证意味着华为终端软件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。

HarmonyOS 典型高安全业务能力介绍

10

HarmonyOS 典型高安全业务能力介绍，通过对诸如小艺、钱包、云空间、查找设备等高级安全特性的介绍，以场景化、实例化的形式，系统性介绍应用和业务如何基于 HarmonyOS 提供的安全能力，来构建高安全的业务系统，最大限度的保护消费者的隐私、财产和数据。

10.1 小艺

小艺是鸿蒙系统级 AI 助手，它深度融合人工智能技术与 HarmonyOS 生态系统，是鸿蒙系统的强大 AI 底座，在使能鸿蒙各应用的同时，通过使能鸿蒙基础控件的方式使能第三方应用。随着 AI 技术的演进，小艺升级为系统智能体，无处不在，随时召唤。致力于为用户提供高效、便捷、安全的智能交互体验，其功能覆盖语音、文字、图片、视频等多种输入形式，支持跨设备协同操作，在智慧出行、运动健康、鸿蒙智家、智慧办公、影音娱乐的各个场景下表现出色，它可以简单快捷的完成信息查询、日程管理、智能家居控制、个性化推荐等。

小艺践行华为隐私保护的最高纲领要求，引入成熟的安全防护技术并应用到各个数据操作阶段，运用机密计算、差分隐私、数据脱敏、去 ID 化等技术方案，在全链路上保障用户的信息安全。

小艺的隐私安全设计，遵循如下设计原则：

- 数据最小化原则
- 控制权掌握在用户手中
- 模型本地化，敏感数据不上云
- 端云同构，确保云端数据安全

小艺作为鸿蒙系统级 AI 助手，面临典型 AI 攻击类问题，为确保模型的稳定可靠输出，有效防范和应对各种攻击，如投毒和后门攻击、对抗攻击、指令攻击和模型窃取攻击等，我们构建了 AI&LLM 安全护栏，有效拦截不合理的输入 & 输出。

小艺严格落实华为公司的 AI 安全治理框架体系，打造五道安全技术护栏，严守合规底线，确保安全的为用户服务。

1）数据安全护栏：构建数据来源检查、数据内容检查能力，识别训练数据集安全隐私风险；

2）模型安全护栏：参考业界优秀实践，从安全算法、安全数据、安全测评维度体系化构建符合人类普世价值观的关键技术能力；

3）部署安全护栏：通过价值观检测系统，利用 1.5B 大模型提升云侧文本和图片价值观检测能力，满足价值观牵引要求；

4）应用安全护栏：结合不同应用场景，防护大模型应用中的新型攻击，通过构建大模型应用安全护栏，有效消减大模型应用场景中安全风险

5）运营运维安全护栏：应对不断变化的攻击模式，满足保护大模型所涉及的训练数据、模型、生成内容的全生命周期安全，持续提升 AI 安全运营能力

10.2 钱包

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 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，支持应用程序处理器和安全元件之间的通信。

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账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安全协议加密。

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。这些信息会通过安全控件传输到卡组织进行验证，华为不会保存或使用您的 CVV 等信息。

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结果、CVV 码、您的设备信息（例如设备型号等）发送到发卡机构，并执行“绑定”流程，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。

为了保证持卡人数据的安全和隐私，无论是国际上还是央行都曾出台相应标准，银行卡信息保存在终端设备上必须经过 Token 化。所谓 Token 化是指用户通过 Huawei Pay 绑定银行过程中，信息经由卡组织提供的安全控件传输到卡组织，将卡号进行虚拟转化后，才返回到华为钱包进行存储，因此手机内储存的并不是真实的银行卡号。绑定过程也需要经过华为和银行的实名验证，确保华为账号和银行卡属于同一用户所有。

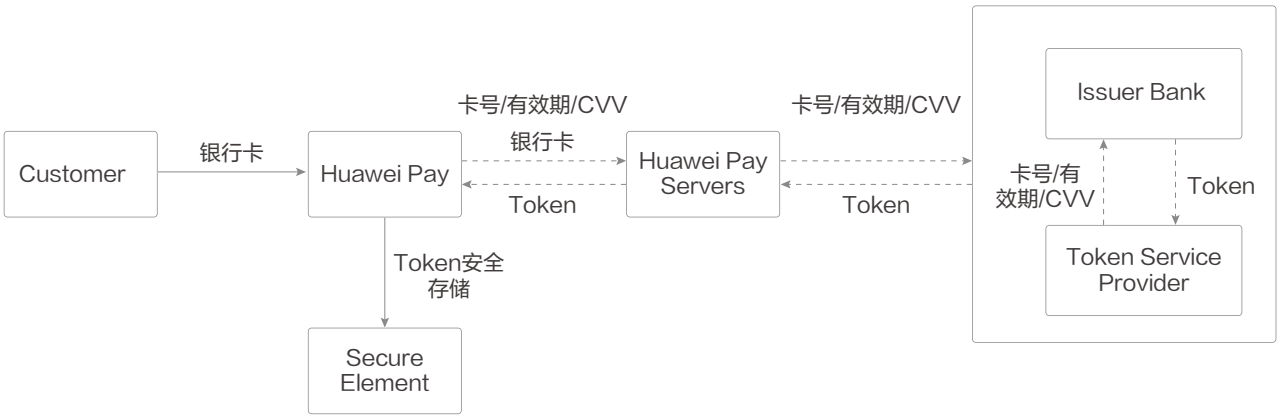


图 10-1 华为 Pay 绑定过程

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：短信验证等。

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支持 Huawei Pay 设备的授权，并且确认用户已使用生物识别或设备密码认证后，才会允许进行支付。

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，并在身份验证通过后进行碰一碰银行卡支付。

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。

生物特征支付

HuaweiPay 支持指纹支付和人脸支付；用户的指纹和人脸信息保存在手机的安全区域中，不会传到华为云端；同时用户的支付信息通过数字证书签名保护。

国际权威金融认证

HuaweiPay 通过了 PCI-DSS 等相关认证，符合支付行业权威安全标准要求。

交通卡

华为手机交通卡是交通卡公司将自己的交通卡应用和卡数据通过空中下载的方式加载到手机的安全单元（Secure Element）中。

交通卡开卡

用户在钱包中发起开卡请求，通过与安全单元建立 SCP（Secure Channel Protocol）通道，在安全单元内开辟可信、独立的交通卡安全运行空间，将交通卡卡应用和卡数据通过安全通道下载到交通卡独立安全单元空间中，确保交通卡安全。

交通卡余额充值

用户在钱包中发起交通卡余额充值，通过与安全单元建立 SCP（Secure Channel Protocol）通道，交通卡公司将余额数据安全的下载到交通卡独立安全单元空间中，确保余额不被篡改伪造。

交通卡刷卡

通过手机的 NFC 控制器，交通卡公司的闸机可以直接和安全单元中的交通卡应用进行通信。在通信过程中完成卡片和闸机之间的相互认证成功后，卡片按照闸机的要求从余额去扣减相应数额的金额。

车钥匙

手机车钥匙遵循智慧车联产业生态联盟（Intelligent Car Connectivity Industry Ecosystem Alliance，简写为 ICCE）推出的标准数字车钥匙规范。

用户开通手机车钥匙后，可以通过手机自带的 NFC 控件器与车辆进行交互，完成开启车门、启动车辆发动机等操作。也可以在和车辆配对完成后，通过蓝牙或星闪等方式和车辆进行认证，实现无感解闭锁 / 主动车控等操作。

通过汽车制造商提供的配套 app，用户可以将手机车钥匙分享给亲友使用。在得到车辆拥有者授权之后，用户可以随时下载对应车辆的数字钥匙并启动车辆。当然，车辆拥有者也可以随时取消授权。

在车辆拥有者在开通手机车钥匙时，通过与安全单元建立 SCP（Secure Channel Protocol）通道，在安全元件内开辟可信、独立的安全运行空间。随后车辆拥有者可以请求汽车制造商通过安全 SCP 通道将车钥匙数据下载到手机中，从而将自己的手机变成汽车钥匙。用户的数字车钥匙存储在手机独立安全单元 (Secure Element) 中，确保车钥匙安全性。

当用户进行恢复出厂设置后，设备会主动删除车钥匙以保证用户财产的安全。

10.3 云空间

华为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。

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。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。每个用户的密钥由密钥管理系统（KMS）生成并管理。云空间验证用户合法身份后才能获取用户密钥，防止密钥泄露。涉及 S4 级敏感个人数据（参见 3.6 章节描述）的应用，用户密钥会在端侧关键资产存储服务（Asset Store Kit）中存储，同时使用用户设备端到端加密主秘钥加密后再上传至云侧服务器，云空间服务器无法获取到用户密钥，具体端到端加密安全机制可参考 6.3 章节描述。

10.4 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。

10.5 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。在您未登录华为账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，在输入华为账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账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。

10.6 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，为用户提供纯净的浏览环境。

华为浏览器基于系统提供的密码保险箱功能，可以为用户安全的自动保存在网站上的用户名密码。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。

10.7 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。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。支付反欺诈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。

10.8 骚扰和诈骗拦截

Harmony OS 提供了全面的骚扰和诈骗防护功能，有效拦截骚扰诈骗来电、骚扰诈骗信息、诈骗网页和换脸诈骗视频通话。用户可以在系统设置的“骚扰和诈骗拦截”页面按需自定义配置拦截规则和黑白名单，HarmonyOS 根据用户配置的拦截规则对来电和信息的内容和频度、网页内容、视频通话内容进行检测和拦截，降低骚扰诈骗行为对用户的困扰。

** 注：骚扰和诈骗拦截功能仅在中国大陆地区的设备上提供。*

11 构建具备韧性的 HarmonyOS 安全运营体系

构建具备韧性的 HarmonyOS 和云服务安全运营体系，参考了零信任网络架构、Cyber Resilience 网络韧性架构等前沿的安全架构，介绍了 HarmonyOS 和云服务的安全可信工程能力、安全防护体系、安全研究实验室、安全漏洞奖励计划和安全应急响应流程和机制，确保 HarmonyOS 和云服务“尽可能保证没有安全漏洞，存在漏洞时通过纵深防御确保漏洞难以利用，在漏洞发生后最快速度恢复业务和修复漏洞”。

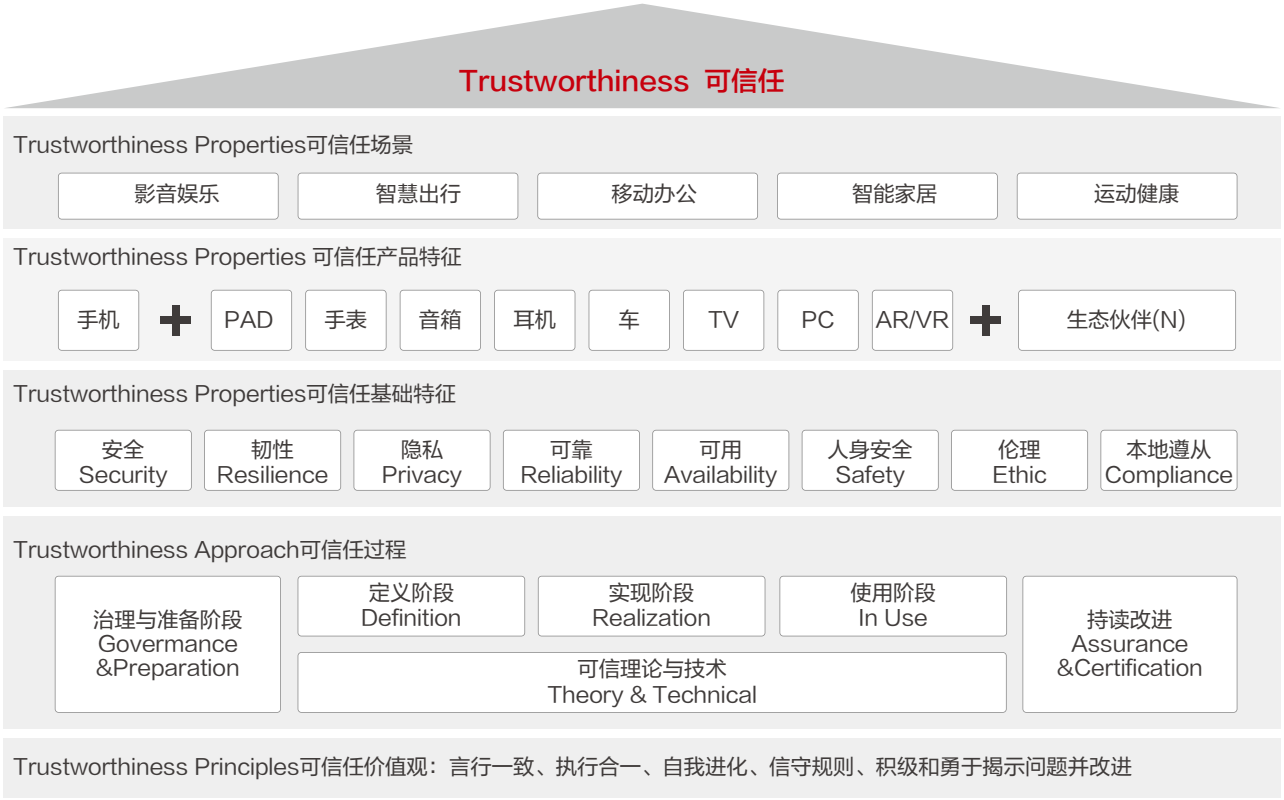
11.1 HarmonyOS 可信工程

今天，人类社会正在迈向万物互联的智能世界，全场景、全连接、智慧化等发展趋势，对消费者产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买一个产品的基本条件。可信不仅仅是产品外在表现的结果，更是产品内在实现的过程，是结果和过程双重可信的高质量。

华为公司把网络安全和隐私保护作为公司的最高纲领。华为将在遵循 ISO9000 的质量管理体系、遵循 ISO/IEC/IEEE 15288 和 12207 的系统工程和软件开发过程之上建设更加强壮的管理系统，使每一位具备可信价值观的员工，基于华为可信任过程相互协作创新，开发出具备可信特征的产品，给客户提供可信的高质量产品，并持续改进。

华为对业界主流安全标准、流程规范、指导书，以及法规指令、白皮书、学术论文等 150+ 篇文档开展研究，我们发现每一个标准不一定都是完备的，或者关注点各自有侧重。未来在数字社会里面构建消费者喜爱的终端和服务，需要什么样的可信标准？为了在设计和信任之间建立起桥梁，便于产品定义者和设计者、以及消费者和运营者对如何可以达成可信形成一致地理解，我们结合华为自身大规模的研发和运维经验，有设计复杂产品的系统知识和系统架构能力。我们从系统工程的行业共识出发，基于可解释、可落地、可验证和有相当业界共识基础的四个原则定义华为可信框架。

图 11–1 华为可信框架



我们要在每一个消费者产品和解决方案中，都融入可信特征、构建高质量，包括：

安全性（Security）：产品有良好的抗攻击能力，保护业务和数据的机密性、完整性和可用性。

韧性（Resilience）：系统受攻击时保持有定义的运行状态（包括降级），遭遇攻击后快速恢复并持续演进的能力。

隐私性（Privacy）：遵从隐私保护既是法律法规的要求，也是价值观的体现。用户应该能够适当地控制他们的数据的使用方式。信息的使用政策应该是对用户透明的。用户应该根据自己的需要来控制何时接收以及是否接收信息。用户的隐私数据要有完善的保护能力和机制。

安全性（Safety）：系统失效导致的危害不存在不可接受的风险，不会伤害自然人生命或危及自然人健康，不管是直接还是通过损害环境或财产间接造成的。

可靠性和可用性（Reliability& Availability）：产品能在生命周期内长期保障业务无故障运行，具备快速恢复和自我管理的能力，提供可预期的、一致的服务。

伦理（Ethic）：增强人类、服务于社会和环境福祉，AI 系统不能加强对弱势和边缘群体的偏见和歧视，并通过程序性要求保障 AI 数据集的多元性。

本地遵从（Compliance）：遵从各国 / 各地区关于禁忌、无障碍和未成年保护要求。

每一个产品在产品定义和完整实现环节、在创新中融入可信思考和控制，从源头就注入可信。我们还要保证产品从创新到客户现场的整个过程是完整、双向一致可追溯的，并在必要的时候提供恰当的（权限分离、信任、行为监控）机密性保护，确保产品没有被仿冒、篡改，确保部署、维护、处置作业过程和作业工具可信，敏感数据没有被泄漏。

11.2 入侵防御体系

云上网络以数据为核心，立体化布防，建立了多层次的纵深安全防御体系。

- **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-Site Scripting）、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、账号提权等攻击行为。
- **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。

11.3 安全攻防实验室

华为终端奇点安全实验室和银针安全实验室是由业界顶级安全研究员组建的安全研究和渗透测试团队，通过如下活动，持续对 HarmonyOS 产品、云服务和解决方案开展网络安全和隐私风险评估工作，提前识别和消除风险，持续保障 HarmonyOS 和云服务安全与隐私纵深防御体系：

- 持续开展安全技术研究，并跟踪学术界、产业界和安全研究员群体的技术动态，掌握最前沿安全技术
- 将安全新技术及时导入产品和解决方案开发流程，应用于产品和解决方案的安全测试

➤ 以渗透测试者视角对 HarmonyOS 产品、云服务和解决方案开展渗透测试，总结系统性改进方案并落地到产品，协助产品团队构建安全纵深防御体系

11.4 漏洞奖励计划

华为非常重视自身产品和服务的安全问题，通过和安全社区及业界同仁共同合作，来帮助我们不断提升和完善自身产品和服务的安全性，因此，我们发布了华为终端安全奖励计划。我们承诺，对每一位报告者反馈的问题都会有专人跟进、分析和处理，并及时给予答复。

此计划包括基于HarmonyOS的华为手机、平板、电脑以及相关的华为智能设备、以及HarmonyOS系统、产品间分布式交互特性等。设备清单详见如下列表：

产品形态	类别和型号
手机	Mate/Pura/P/Nova/ 畅享系列
平板	MatePad Pro/MatePad Air/MatePad/MatePad SE 系列
电脑	MateBook 系列
穿戴	智能手表 / 运动手表 / 手环等
IOT	智慧屏 / 路由 / 音箱等

服务涉及到的详细域名如下：agchosting.link；agconnect.link；agcstorage.link；dbank.com；dbankcdn.com；dbankcdn.cn；dbankcdn.ru；dbankcloud.com；dbankcloud.eu；dbankcloud.ru；dbankcloud.asia；dbankcloud.cn；dbankedge.cn；dbankedge.net；hicloud.com；petalmail.asia；petalmail.com；petalmail.com.au；petalmail.com.cn；petalmail.eu；petalmail.lat；petalmail.ru；petalmaps.com；petalmaps.com.ru；petalmaps.ru；petalsearch.cn；petalsearch.com；petalsearch.com.cn；petalsearch.ru；powerapp.io；szsharelink.com；appgallery.huawei.com；appgallery5.huawei.com；appgallery8.huawei.com；appgallery7.huawei.com；appgallery1.huawei.com；appstore.huawei.com；id.huawei.com；id5.huawei.com；id1.huawei.com；appgalleryconnect.huawei.com；developer.huawei.com/consumer/；developers.huawei.com/consumer/；developer-code.huawei.com；developer-notice.huawei.com；devecostudio.huawei.com；hts.huawei.com；ads.huawei.com；bizconnect.huawei.com；cloud.huawei.com；bugbounty.huawei.com；vmall.com

注意：我们将会随着时间更新以上列表。

详细的奖励规则请参考 https://bugbounty.huawei.com/#/home

11.5 安全应急响应

安全应急响应中心 SRC（Security Response Center）的职责是快速响应 HarmonyOS 安全风险及问题。SRC 遵循 ISO/IEC 30111 漏洞处理流程，以及 ISO/IEC 29147 漏洞披露标准，处理 HarmonyOS 中的漏洞。我们将按漏洞响应流程对上报的潜在漏洞进行处理。

漏洞响应流程介绍，

1）接受上报：主动监控和接受外部上报安全漏洞和问题，启动漏洞响应流程。

2）问题验证：协调资源，验证是否是漏洞或安全问题，评估风险等级。

3）解决方案：制定漏洞风险缓解和修复方案。

4）漏洞披露：漏洞确认修补后，与安全研究员协调安全问题的披露。

5）问题反馈：收集和总结来自内外部用户的意见，重要案例反馈给开发流程用于指导产品开发。

为避免提前披露对消费者及行业合作伙伴造成伤害，在整个漏洞处理的过程中，我们会严格控制漏洞信息的范围，要求漏洞上报者对漏洞进行保密，直到漏洞修复和披露。

HarmonyOS
安全能力开放使能生态

12

HarmonyOS 提供的安全能力，以 API、Kit、SDK 形式为生态应用向开发者提供能力。

12.1 设备证书服务 Device Certificate Kit

Device Certificate Kit（设备证书服务）面向应用开发者，提供了证书算法库、证书管理和设备真实性证明的能力。

证书算法库

证书算法库提供了用于解析和验证数字证书的能力，包括 X509 证书、X509 证书扩展域段、X509 证书吊销列表的解析及校验能力，以及证书链的校验能力。

通过调用证书算法库接口，开发者可以屏蔽三方算法库的实现差异，实现迅捷开发。

应用场景：应用对接收的服务端证书或用户输入的证书进行解析，获取证书基本字段或扩展字段用于显示或校验，并使用 CA 证书链和 CRL 校验证书的合法性。

证书管理

证书管理提供了系统级的证书管理能力，通过证书管理接口可以确保证书和私钥在存储和使用过程中的安全性，防止未经授权的访问和使用。

当前提供了应用私有证书凭据的安装、获取、签名及删除能力，用户公共证书凭据授权、获取和使用的能力，用户 CA 证书的获取能力。

应用场景：安装应用私有证书凭据，并使用应用私有证书凭据进行签名、验签。

设备真实性证明

设备真实性证明能力，提供了设备真实性和应用身份证明的能力，采用标准的 X509 证书格式，基于密码算法、证书链实现校验业务请求是否来自真实设备和合法应用，帮助开发者识别黑灰产的攻击行为。

能力特定：

1. 基于硬件级的设备证书认证

2. 支持对应用身份的证明

3. 采用标准的 X509 证书格式

应用场景：设备真实性证明能力主要可以抵御以下攻击场景

1. 模拟器、云手机等非真实设备：由于只有真实的设备才具备出厂灌装的设备证书，并且只有拥有设备证书的设备才具备此能力，所以通过本方案可以确保请求来自真实的设备。

2. 重打包应用、仿冒应用等非真实应用：由于设备真实性证明证书链包含对应应用包名和签名公钥 hash 信息，可以通过验证这些信息保证所有带签名的信息来自合法的应用。

通过抓包等方法修改或伪造应用请求：使用设备真实性证明私钥对重要的业务请求附加签名，可以确保重要的请求的完整性，并通过挑战值机制杜绝重放攻击。

12.2 设备安全服务 Device Security Kit

系统完整性检测

向开发者提供判断设备运行环境是否安全的能力，应用通过调用接口获取系统是否被越狱、被攻击、被模拟，应用基于检测结果评估如何响应。设备完整性检测为用户提供更加安全、可信的设备使用环境。系统完整检测服务具备以下技术优势：

1）基于可信执行环境 TEE 提供系统完整性检测结果：在设备安全启动时，在 TEE 中评估检测系统完整性，可信度高，并动态评估系统完整性。

2）系统完整性检测结果请求证书签名；服务端使用 X.509 数字证书对系统完整性检测结果签名，使用 JWS 格式回传给系统完整性检测 API，签名结果不可篡改。

恶意 URL 检测

向开发者提供检测应用访问网址是否为恶意网址的能力，应用通过调用接口可获取访问网址是否是钓鱼、欺诈、木马等恶意网址，应用基于检测结果实施提示和拦截。恶意 URL 检测能力向三方开发者提供了集成简单、免运营、可信赖的安全服务，降低安全浏览服务的实现成本。

应用设备状态检测（Device Verify）

应用设备状态检测向开发者提供了管理应用在某设备上使用状态的能力，该服务基于设备证书对设备身份进行认证并签发 DeviceToken，应用的服务器使用 DeviceToken 到 Device Security 服务器查询和管理

应用在该设备的使用状态。

应用场景：对应用在某台设备上的使用状态进行管理和检测，包括判断应用是否在该设备上首次安装，或在该设备上用户是否已获取了优惠券等的状态检测，以支撑业务进行新用户营销活动。

可信服务证明

位置信息的安全风险：在一些对安全性较高的场景下，应用在终端侧会获取设备的位置信息，应用服务器把位置信息当做因子一起参与业务逻辑判断或风控检测。但由于应用在 REE 侧获取的位置信息存在被篡改和仿冒的风险，带来以下风险：

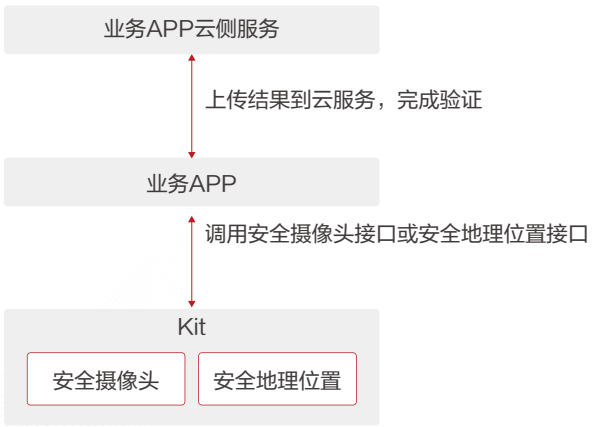
1）营销活动薅羊毛：电商、银行类应用经常会在指定城市开展营销活动。如果位置信息被篡改，可以快速切换到目标城市，获得参与营销活动资格。

2）逃避风控检测：诈骗集团通过前期的诈骗资料收集以及植入木马（盗取验证码和密码）等，交易时通过返回被篡改的地理位置逃避风险的检测。

3）游戏外挂：对一些依赖地理位置信息的应用实施攻击行为，通过篡改地理位置，可以瞬间移动到 NPC，破坏游戏平衡。

人脸图像存在与位置信息同样的安全风险：在金融类应用中，一些业务需要人脸识别通过后才能完成，当前应用的流程一般是先采集人脸数据、再上传到应用服务器完成人脸识别。但如果在设备采集的人脸被篡改，服务器人脸识别通过，带来安全风险、甚至财产损失。

图 12-1 安全摄像头和安全地理位置



在 TEE 里完成位置信息和人脸图像的采集，保证这些信息采集过程的安全性。同时，TEE 还会对这些信息做签名，应用服务器先验证签名、保证数据的安全性和完整性后，再使用数据。

说明：当前这个安全能力只能解决设备自身被攻击时，位置信息和人脸图像的安全性，不能解决外部输入的安全性。比如，位置信息的外部输入依赖 GNSS，如果 GNSS 被攻击（或其它攻击方式），设备采集的

位置信息仍然存在风险。人脸图像同样依赖于外部输入，如果外部输入是人脸模具（或其它攻击方式），设备采集的人脸图像仍然存在风险，这种情况下，推荐结合活体检测完成人脸识别。

数字盾服务

数字盾服务通过可信用户交互（TUI, Trusted User Interface）为金融应用的大额转账交易提供端到端安全防护，主要包括以下关键功能：

- 数字盾密码管理：主要包括数字盾密码的创建、修改以及关闭，其中数字盾密码输入过程中均使用 TEE 隔离的数字键盘控件，实现用户数字盾密码的防窃取输入。
- 交易信息密码认证：在转账交易场景中，通过数字盾密码对交易信息进行强认证，认证结果依托密钥管理服务提供的加密签名功能验证，确保交易完整性与不可抵赖性。
- 生物特征绑定与认证：支持人脸或指纹等生物特征的绑定与认证，增强交易安全性。
- 数字盾签名密钥备份与恢复：备份数字盾签名密钥，确保应用卸载重装后，密码认证功能仍正常运行，保障密钥持久化存储。

防窥保护

防窥保护功能通过使用智能算法来主动感知屏幕被窥视风险。

针对应用内可能出现的敏感信息，如浏览记录、支付记录、收藏记录等，应用开发者识别需要进行防窥保护的页面，在感知防窥状态变化时，对页面信息进行隐藏。系统还提供统一的防窥保护窗口蒙层能力，业务可接入防窥保护蒙层能力，在感知到需要隐藏整个应用窗口的内容时直接使用系统蒙层进行窗口级覆盖。

12.3 用户身份认证服务 User Authentication Kit

User Authentication Kit 提供集口令、人脸、指纹于一体的系统级用户身份认证功能，以及风格统一的认证交互界面，在确保用户身份认证安全性的同时带给用户更好的身份认证体验。

归一化认证接口

屏蔽不同认证因子的差异，调用锁屏口令、人脸、指纹认证的接口归一。

同一套接口提供人脸、指纹、锁屏密码的组合认证方式。

同一套接口提供人脸认证、指纹认证和业务自定义认证的组合。

支持感知认证安全等级差异

支持调用者指定期望的认证安全等级，避免将低安认证能力应用在高风险操作的用户鉴权场景，例如将防伪能力不够的 2D 人脸认证用于支持场景。

支持业务自定义认证方式

支持带导航键的认证界面，用户点击导航键可切换业务自定义认证界面。

支持短时间内复用设备解锁认证结果

- 支持认证方式无关的解锁认证结果复用，采用该认证方式，只要在解锁后调用者指定的时间范围内（最长 5min），可不用重复认证用户直接返回认证通过结果；
- 支持认证方式匹配的解锁认证结果复用，采用该认证方式，不仅需要处于调用者指定的解锁后时间范围内，还需要解锁使用的认证方式与调用者指定的一致，才能复用解锁认证结果，直接返回认证通过。

提供系统级用户身份认证界面

- 支持调用者自定义认证界面的标题和导航键文字。
- 身份认证控件会根据设备屏幕状态自适应调整窗口显示模式。

12.4 加解密算法框架服务 Crypto Architecture Kit

加解密算法框架服务为生态应用提供安全算法能力，支持对称加解密、非对称密钥生成、非对称加解密、签名验签、消息验证码、摘要、密钥派生、密钥协商和随机数等基础算法能力。同时也支持国密 sm2、sm3 和 sm4 算法。

应用场景：

- 对称加解密：常用于保证数据的机密性，防止敏感数据泄露。
- 非对称加解密：常用于保证数据的机密性，在无法将对称密钥安全共享给对方时，可以将公钥共享给对方，对方在对公钥进行验证后，使用公钥对消息进行加密，并传递给私钥持有者，私钥持有者使用对私钥对密文数据进行解密。
- 签名验签：基于非对称密钥，常用于保证数据的完整性和数据来源的身份验证。
- 消息验证码：基于对称密钥，常用于保证数据的完整性。
- 摘要：对数据完成不可逆的加密，且输出长度固定，常用于签名等场景。
- 密钥派生：基于一个对称密钥或口令，安全地派生出多个对称密钥。
- 密钥协商：常用于在一个非安全通道中，无需共享任何秘密的情况下，协商出一个对称密钥。
- 随机数：纯软件实现的安全随机数 DRBG，生成的数据具备随机性，不可预测性，与不可重现性，常用在密码学中，如对称和非对称密钥的生成等。

12.5 通用密钥库服务 Universal Keystore Kit

通用密钥库服务（HarmonyOS Universal Keystore Service，HUKS）为应用提供密钥全生命周期管理能力，HarmonyOS 应用开发者使用密钥管理套件（Universal Keystore Kit）可进行密钥生成、密钥销毁、密钥使用（如加密、解密、签名、验签等）。在具备可信执行环境等安全隔区的高安等级 HarmonyOS 设备中，通用密钥库服务确保了其管理密钥的明文，在生命周期内不会暴露在非安全环境。

通用密钥库服务对密钥进行了严格的权限控制，密钥仅可由生成密钥的应用访问。在密钥生成时，通用密钥库服务记录了应用的进程标识等信息，供应用访问密钥时进行身份验证。HarmonyOS 应用开发者可以叠加用户身份认证功能（如生物特征认证、PIN 认证）以增强密钥的访问控制，通用密钥库服务确认身份认证结果后，才允许相应的密钥访问与操作。

此外，通用密钥库服务还提供了密钥合法性证明（Key Attestation）功能。应用可以基于证书链技术，对通用密钥库管理的密钥进行证明，包括证明密钥生成环境、密钥所属应用等属性。其中，证书链基于匿名的根证书签发，不会泄露用户设备信息，同时能保证密钥证明结果的合法性和完整性。

目前，通用密钥库不仅支持国际标准的 AES、RSA 等算法，还支持 SM2、SM3、SM4 商用密码算法，支持金融应用中的资金流转、刷卡支付等场景。

12.6 在线认证服务 Online Authentication Kit

基于账号密码的应用方式因输入复杂、难于记忆且易遭受网络钓鱼攻击等问题，在便捷性与安全性方面均存在不足。HarmonyOS 提供免密认证框架，支持 FIDO（Fast Identity Online）、IIFAA（International Internet Finance Authentication Alliance）、SOTER 标准免密认证协议，可以支撑业务通过人脸 / 指纹方式进行免密认证登录，提高登录便捷性，同时也能有效增强登录安全性。应用接入对应的服务器后，可以在端侧使用对应的相关能力，利用生物特征等来代替传统的密码，实现免密登录、免密支付等业务场景。

FIDO 认证协议

FIDO 是一种国际主流的免密认证标准，众多生态应用厂商广泛使用该能力，包括中国工商银行，中国银行，农业银行，交通银行等银行应用、以及多种证券或金融类应用。HarmonyOS 构建了基于 FIDO UAF 的免密身份认证功能，应用可以通过接入系统 FIDO 服务实现开通、使用免密身份认证等能力。FIDO 服务的开通和使用流程需要验证用户的生物特征，确保只有正确的用户可以使用凭据。FIDO 服务在开通时会为应用生成业务密钥，业务密钥的生成和使用在 TEE 环境中实现，业务私钥不会出安全环境。FIDO 的认证报文采用业务私钥签名后返回给应用，保障了认证结果的可靠性。

针对同一业务涉及应用、网页混合登录场景，HarmonyOS 提供基于 FIDO2 标准协议的通行密钥机制。借用该系统能力，用户可使用生物特征（例如指纹、人脸）登录应用或网页。应用可以通过接入通行密钥实现以下功能：

- 通行密钥注册：应用或网页需要为用户提供更便捷、安全的登录方式时，可使用通行密钥注册能力。该能力通过验证用户的生物特征，在本设备上完成应用或网页的通行密钥创建。与基于 FIDO UAF 的免密认证相似，通行密钥注册时，会在 TEE 环境中为应用生成针对该应用的通行密钥私钥，该私钥不会出安全环境，保障私钥的机密性和完整性。

- 本地免密认证：应用或网页需要在本设备上验证用户的通行密钥时，可使用本地免密认证能力。仅当用户的生物特征在 TEE 内完成认证时，相同安全环境内的通行密钥私钥才会参与对本次登录或支付的认证报文的签名，应用或网页获取被签名的认证报文后，可在服务器使用公钥验证，从而完成本次会话的免密认证。如果 TEE 内的生物认证没有给出认证通过的结果，通行密钥将不会参与认证报文的签名，从而保障该认证结果的可靠性与真实有效性。

- 跨设备扫码认证：应用或网页需要在其他设备上验证用户的通行密钥时，可使用跨设备扫码认证能力。该能力使用已注册通行密钥的设备作为辅助登录设备，通过跨设备扫码的方式，在其他设备进行应用或网页的免密认证。其中，用户需要在已注册通行密钥的设备上验证用户的生物特征，确保使用该设备上通行密钥的人是正确的用户。两端设备基于近场通信传输的共享秘密协商会话密钥，建立安全传输通道，保障认证数据在传输过程中的机密性与完整性。

IIFAA 认证协议

IIFAA（互联网可信认证联盟）是 2015 年由中国信通院、蚂蚁集团、阿里巴巴、华为、中兴、三星联合发起的可信认证生态联盟，该联盟致力于推动可信认证技术发展及行业应用，引领行业制定技术规范。HarmonyOS 提供了 IFAA 免密认证模块，使集成 IFAA 认证能力的应用可接入系统免密身份认证机制。

SOTER 认证协议

为了解决传统可见的密码验证在安全性和便捷使用上的问题，腾讯制定了 SOTER 认证协议，该协议旨在提供一套生物认证平台和标准，使得设备上的传感器（如人脸传感器 / 指纹传感器）能够安全、高效、简单地进行免密登录、免密支付等操作。HarmonyOS 提供了 SOTER 免密认证模块，使集成 SOTER 认证能力的应用、小程序可接入系统免密身份认证机制。

12.7 关键资产存储服务 Asset Store Kit

Asset Store Kit 包含了关键资产存储服务（ASSET）开放的接口能力集合，提供了用户短敏感数据的安全存储及管理能力。其中，短敏感数据可以是密码类（账号 / 密码）、Token 类（应用凭据）、其他关键明文（如银行卡号）等长度较短的用户敏感数据。

安全存储

关键资产的安全存储，依赖底层的密钥管理服务。具体来说，关键资产的加 / 解密操作以及访问控制校验，都由密钥管理服务在安全环境(如可信执行环境)中完成，即使系统被攻破，也能保证用户敏感数据不发生泄露。

访问控制

1、基于属主的访问控制： 所有的关键资产都受属主访问控制保护，业务无需设置。

- 只允许关键资产被其属主（写入该关键资产的业务）访问。
- 关键资产属主身份由 ASSET 从系统服务中获取，即使业务身份被仿冒，仿冒者也无法获取到其他业务的数据。
- 关键资产加 / 解密时，其属主身份参与了完整性保护，即使关键资产属主身份被篡改，攻击者也无法获取到其他业务的数据。

2、基于锁屏状态的访问控制： 分为以下三种保护等级（安全性依次递增），业务可根据实际情况设置任意一种，若不设置，则默认保护等级为“首次解锁后可访问”。

- 开机后可访问：关键资产在开机后被允许访问。
- 首次解锁后可访问：关键资产在首次解锁后被允许访问。
- 解锁时可访问：关键资产仅在处于解锁状态时被允许访问。

3、基于锁屏密码设置状态的访问控制： 该访问控制默认不开启，业务可根据实际情况决定是否开启。

- 在用户设置了锁屏密码后，关键资产才被允许访问。

4、基于用户认证的访问控制： 该访问控制默认不开启，业务可根据实际情况决定是否开启。

- 关键资产在用户身份认证通过后被允许访问。
- 任意一种认证方式（指纹、人脸、PIN 码）通过，均可授权本次关键资产的访问。
- 业务可通过设置认证有效期，达成一次用户认证、授权多个关键资产访问的效果。认证有效期最长可设置 10 分钟。

12.8 安全控件 &Picker

HarmonyOS 生态始终将用户隐私放在首位。隐私是用户的基本权利，安全是产品的基本属性。基于这种理念，HarmonyOS 对用户隐私数据的管理从“管权限”逐渐变为了“管数据”，通过安全控件 &Picker 等机制，让用户可以更加细粒度地管理个人数据。

安全控件

隐私权限管理需要用户手动授权，这对于一些普通用户来说可能比较困难，另外，应用程序对某些敏感信息使用可能在不同的使用场景，用户使用应用过程中，隐含着对于权限的授予意愿，安全控件是系统提供的一组系统实现的 ArkUI 基础组件。应用可以自由集成该类组件，当组件被用户点击后，应用将被授予临时授权，无需向用户弹窗授权就可访问受限资源，实现通过识别用户主动行为自动授权的设计思路。

整体方案由安全控件 UI 组件、安全控件管理服务、安全控件增强组成：

UI 组件实现了固定文字图标的样式便于用户识别，同时提供了相对丰富的定制化能力便于开发者定制。

控件管理服务提供控件注册管理能力、控件临时授权机制、管理授权生效周期，确保应用后台、锁屏下无法注册使用安全控件。

安全增强部分实现了包括地址随机化、挑战值检查、回调 UI 框架复核控件信息、调用者地址检查、组件防覆盖、真实点击事件校验等机制，防止应用开发者通过混淆、隐藏、篡改、仿冒等方式滥用授权机制，泄露用户隐私。

Picker

Picker 是系统提供的一组数据选择接口，开发者不需要在应用中集成 Picker 就可以直接调用 Picker 接口。应用通过拉起 Picker 界面，允许用户在预定义的数据集合中选择要访问的数据，用户在应用上操作选择后，应用便可以获取数据，以达到应用借助 Picker 接口，而无需申请权限就可以直接访问数据的目的。

安全控件 &Picker 列表

- 粘贴控件
- 保存控件
- 位置控件
- 文件 picker
- 照片 picker
- 联系人 picker
- 音频 picker
- 相机 picker

- 扫码 picker
- 卡证识别 picker
- 档扫描 picker

12.9 密码保险箱

随着应用数量的增多、密码复杂程度的增加，用户忘记登录密码的情况频发。HarmonyOS 密码保险箱提供密码的自动保存、自动填充、自动生成强密码、多设备同步功能，为用户打造了安全存储密码、无缝免密登录的便捷体验。

HarmonyOS 应用在注册新账号以及修改账号密码场景下，密码保险箱为应用接入生成强密码功能，自动生成符合开发者定义密码规则的强密码，帮助用户生成足够安全强度的密码，若用户将此密码进行账号注册或修改，密码保险箱可为用户保存该密码。

密码保险箱默认生成的密码长度为 16 个字符。其中包含数字、大写字符、小写字符。开发者可以通过设置 TextInput 控件的 newPassword 属性开启生成强密码功能，并通过定义 passwordRules 预制密码生成规则，指定密码的长度或长度范围，密码首位格式（首位 大写字母 or 小写字母 or 数字 三选一）以及是否需要在密码中加入特殊字符。

密码的保存 / 填充与查看

密码保险箱把应用的账户密码信息加密保存到终端设备之中，以储存在关键资产数据库的形式实现，密码保险箱提供硬件级加密存储能力，并通过应用 ID（应用安装包的唯一标识）对不同应用的“密码”数据进行隔离；密码保险箱保存的“密码” 数据通过认证加密方式进行加密保护，加密算法为 AES_256_GCM；对应的加密密钥受 ITrustee 保护，加密 / 解密处理始终在安全环境内执行。

在填充或查看“密码”数据的过程中，依托 HarmonyOS 用户身份认证服务，会进行用户身份信息认证（人脸 / 指纹或锁屏密码），用户身份通过后，才可以访问密码保险箱存储在关键资产的用户密码。

多设备同步

密码保险箱支持多设备同步功能，用户在本端设备上登录华为账号，完成可信设备的认证后，本设备密码保险箱保存的账号密码，可以在同华为账号下的设备间同步。用户可以在其他的同华为账号的设备上直接查看及使用同步的账号密码，无需重新录入。密码保险箱“密码”数据在整个同步过程中，以端到端加密的方式通过云服务器完成同账号设备间的加密传输，用于确保云服务器无法获取用户的账号密码。

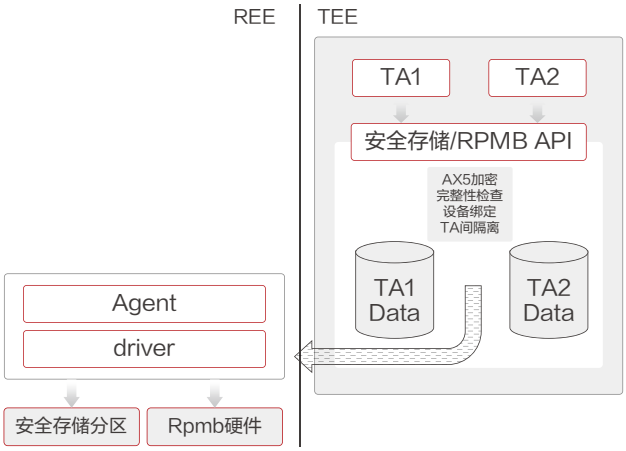
12.10 可信执行环境

HarmonyOS 系统里可信执行环境 iTrustee 提供统一的 KIT，主要涉及以下几个部分

可信存储

iTrustee 提供可信存储能力，以保证数据的机密性、完整性、设备一致性和高可靠性。不同 TA 的存储数据相互隔离，TA 仅能访问自己存储的数据，无法打开、删除或篡改其他 TA 的存储数据。基于上述安全能力，可信存储特性可用于存储 TA 的关键数据，如密钥、证书等。

可信存储分为两种：安全文件系统存储与 RPMB（Replay Protected Memory Block）存储，前者将密文存储到特定的安全存储分区；后者将密文存储到闪存特定的存储区域。安全文件系统存储同时提供了 DE 和 CE 存储区，满足不同场景下的安全存储需求。



可信显示 TUI

iTrustee 提供 TUI（Trusted User Interface，可信用户交互）能力，在 TEE 中为安全应用提供可信的显示、输入和指示。

可信显示能力：保证显示的信息不会被任何 REE 侧的软件或者其它 TA 所攻击，如截屏、篡改、掩盖等。

可信指示能力：可信界面会显示预置的图片或文字，提示用户当前的显示处于安全的环境。可信显示支持 PNG 图片、文本、按钮和输入框等基本控件，支持显示统一大小的黑体汉字、英文字母、符号和数字，用户可以信任显示屏上所显示的信息，确认是由一个 TA 所显示的。

可信输入能力：保证用户的输入不会被任何 REE 侧的软件或者其它 TA 所提取、篡改或劫持。iTrustee 将接收用户输入的器件设置为只能由 TEE 访问的安全状态，保证用户的输入不会传递到 REE 侧，同时通过使用权限控制隔离其它 TA 的访问。可信输入提供 qwert 英文全键盘控件，支持输入英文大小写字母、符号、数字，暂不支持中文。

TUI 常见的应用场景包括：PIN 码输入，支付、转账、敏感交易信息显示。当前 TUI 仅支持遵循 GP 标准的 GP TUI 开发方式，GP 标准 TUI API 为安全应用（TA）的开发者提供与用户交互的功能支持。通过在 TEE 环境中运行的 TA 来调用 GP TUI API，可以安全的向用户显示敏感数据、获取用户的敏感输入。TUI 使用过程中可以确保由 TEE 控制屏幕，并与 REE 和其它 TA 隔离。

iTrustee 支持采用 TUI 显示可信二维码功能：二维码也称为二维条码，常见的二维码为 QR Code（全称为 Quick Response Code），是指在一维条码的基础上扩展出另一维具有可读性的条码，使用黑白矩形图案表示数据，被设备扫描后可获取其中所包含的信息。一维条码的宽度记载着数据，而其长度没有记载数据。二维条码的长度、宽度均记载着数据。二维条码有一维条码没有的“定位点”和“容错机制”。容错机制在即使没有识别到全部的条码、或是说条码有污损时，也可以正确地还原条码上的信息。当前二维码经常被用作支付或身份认证等高安全场景，这种场景对二维码的保护是非常必要的。iTrustee 提供二维码接口，安全应用通过自己的算法，生成 text 字符串，调用 iTrustee 提供的接口生成二维码图片，并通过 TUI 安全显示出来，可提高应用场景的安全性。

可信时间

iTrustee 提供可信的基准时间，该时间寄存器只能由 TEE 里时间驱动访问，不能被恶意 TA 或 REE 应用修改。

该特性保证了 TA 持久时间的单向性，支持使用密钥时对有效期、使用频率等安全属性的检查。另外还提供可信的定时功能，支持开发者设置定时任务。

可信加解密

iTrustee 提供密钥生成能力，HASH、HMAC、对称算法和非对称等算法类型，包括国际算法和国密算法。算法接口实现遵从 Global platform TEE 标准，底层对接软引擎和硬件引擎，提供了不同安全等级的算法能力。

iTrustee 中的密钥管理服务为 TA 提供了硬件密钥生成的能力，TA 可以使用硬件密钥和加解密 API 进行关键数据加密，提升数据的机密性和安全性。HarmonyOS 提供的安全能力，为生态应用程序以 API、Kit、SDK 形式向开发者使能。同时，为生态设备提供专业 CBB、安全模组、独立芯片等形式开放。

12.11 业务风险检测能力

业务风险检测为开发者提供场景化（反作弊、反欺诈、违规内容检测等）的风险检测服务。当前 HarmonyOS 已开放的能力有涉诈剧本检测

特性介绍

电信网络诈骗中犯罪分子使用的诈骗手段常被设计成一套有预谋的流程，逐步诱导受害者上当受骗。

HarmonyOS 在犯罪分子常用的路径上埋点，获取涉诈行为线索，经过检测模型的综合决策，输出当前设备上用户受到诈骗威胁的风险。

应用场景

金融支付类应用在用户转账、支付前，通过调用涉诈剧本检测接口，检测用户是否受到诈骗威胁。该接口返回一个风险分，以及涉诈行为的线索，例如，接收到涉诈引导信息、设备有被操控风险等，应用可以根据风险分及线索，进行有效提示或拦截。

12.12 内容风控检测能力

内容风控服务接口用于对终端用户提交的文本或图片内容进行合规性检查的服务，如识别暴力、色情等违法的信息，有效协助用户进行风险预警和违法内容拦截。当前面向元服务开发者已开放的能力有文本、图片内容合规检测。

特性介绍

- 内容风控检测能力能够识别网络上常见的违规内容，例如：谩骂、低俗、无意义灌水以及违法违规，帮助构建健康的网络环境。
- 违法违规文本、图片内容识别
- 谩骂，隐晦低俗，色情内容识别
- 血腥、恐怖、恶心不适图片识别
- 其他如灌水等无意义内容识别

应用场景

消费者在云服务提交的评论、账号昵称、账号头像、评论区图片等。

缩略语表
Acronyms and Abbreviations

表 A-1 缩略语清单

英文缩写	英文全称	中文全称
3D	Three Dimension	三维
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用软件编程接口
APK	Android Package	Android 安装包
ARM	Advanced RISC Machines	高级精简指令集计算机器
CE	Credential Encryption	凭据加密
CFI	Control Flow Integrity	控制流完整性
DE	Device Encryption	设备加密
ECC	Elliptic Curve Cryptography	椭圆加密算法
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
eMMC	Embedded Eultimedia Card	嵌入式多媒体卡
HarmonyOS	HarmonyOS	华为 HarmonyOS 系统
GP	GlobalPlatform	全球平台组织
HMAC	Hash-based message Authentication Code	散列信息认证码
HUK	Hardware Unique Key	硬件唯一密钥
HUKS	HarmonyOS Universal Keystore Service	华为通用密钥库系统
ID	Identifier	标识符
IMEI	International Mobile Equipment Identity	国际移动设备标识
InSE	Integrated Secure Element	集成安全元素
IOT	Internet of Things	物联网
IT	Information Technology	信息技术
JOP	Jump Oriented Programming	跳转导向编程
LTO	Link Time Optimization	链接时优化
MAC	Media Access Control	媒体接入控制（MAC 地址即媒体接入控制地址）
NFC	Near Field Communication	近距离无线通信技术

英文缩写	英文全称	中文全称
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
OS	Operating System	操作系统
OTA	Over The Air	空中升级
PAN	Privileged Access Never	特权模式访问禁止
PIN	Personal Identification Number	个人身份识别码
PKI	Public Key Infrastructure	公共密钥基础设施
POS	Point of Sales	销售点
PXN	Privileged Execute Never	特权模式执行禁止
REE	Rich Execution Environment	普通执行环境
ROM	Read-Only Memory	只读存储器
ROP	Return Oriented Programming	返回导向编程
RSA	Rivest Shamir Adleman	RSA 加密算法
RPMB	Replay Protected Memory Block	重放保护存储区
SD	Secure Digital Memory Card	安全数字存储卡
SDK	Software Development Kit	软件开发工具包
SHA	Secure Hash Algorithm	安全散列算法
SN	Serial Number	序列号
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境
TLS	Transport Layer Security	传输层安全性协议
TUI	Trusted User Interface	可信用户界面
UID	User Identifier	用户身份标识符
mmap	memory-mapped	内存映射文件方法
VDSO	Virtual dynamic shared object	虚拟动态共享对象
OEM	original equipment manufacturer	贴牌生产
CE	Credential Encryption	凭据加密
SECE	Sub-Enhanced Credential Encryption	子增强凭据加密
ECE	Enhanced Credential Encryption	增强凭据加密
SCP	secure channel protocol	安全通道协议
SSD	Supplementary Security Domain	辅助安全域
SE	Secure Element	安全元件
SP	Select partner	优选合作伙伴

英文缩写	英文全称	中文全称
TSM	trusted service manager	可信服务平台
APDU	application protocol data unit	应用协议数据单元

修订记录

日期	修改描述
2024-08-2	初始版本
2025-09-24	版本更新

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
网址：https://www.huawei.com
PSIRT邮箱：PSIRT@huawei.com
客户服务电话：8008308300 4008308300
邮编：518129