HarmonyOS NEXT 安全技术白皮书

文档版本 V1.0

发布日期 2024-08-13

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址: 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址: https://www.Huawei.com

PSIRT 邮箱: PSIRT@Huawei.com

客户服务电话: 8008308300 4008308300

目 录

1 前言

摘要

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**：应用程序从单体应用，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 2 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 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”。
- 第八章：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。
- 第九章：HarmonyOS 典型高安全业务能力介绍，通过对诸如华为账号、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”
- 第十一章：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。
- 第十二章：缩略语表

2 HarmonyOS 概述

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，为消费者带来简捷，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

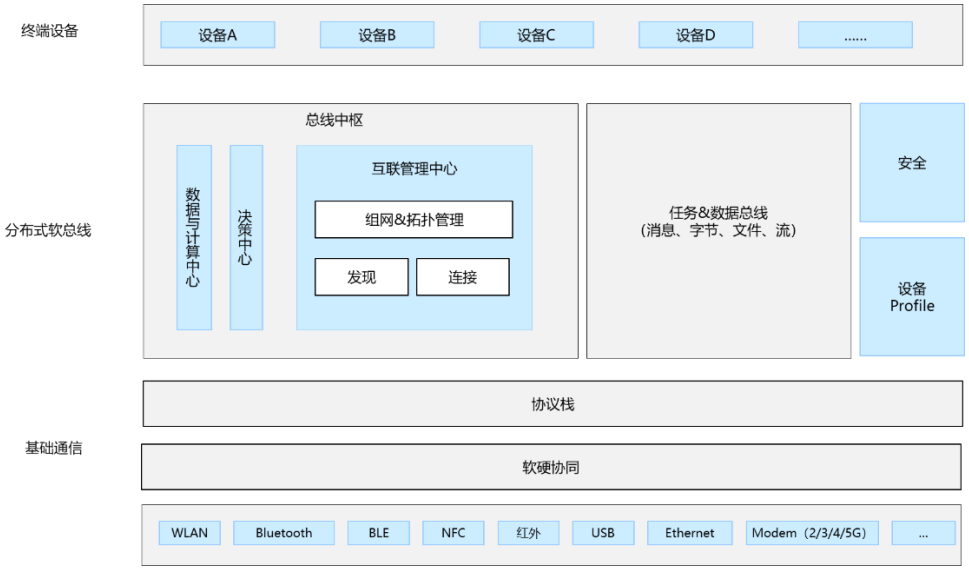
HarmonyOS 是一款面向 IoT 时代的分布式操作系统，将消费者多个设备安全的连接起来，搭建统一的分布式跨设备开发平台，使得消费者在分布式智能全场景中接触到的多种智能终端能够有机融合，呈现为一个完整统一的整体，为消费者提供好像是在使用一部“超级终端（One Device）”的体验，系统性地解决了多终端环境下消费者体验不佳和开发者效率低下的问题。

HarmonyOS 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。

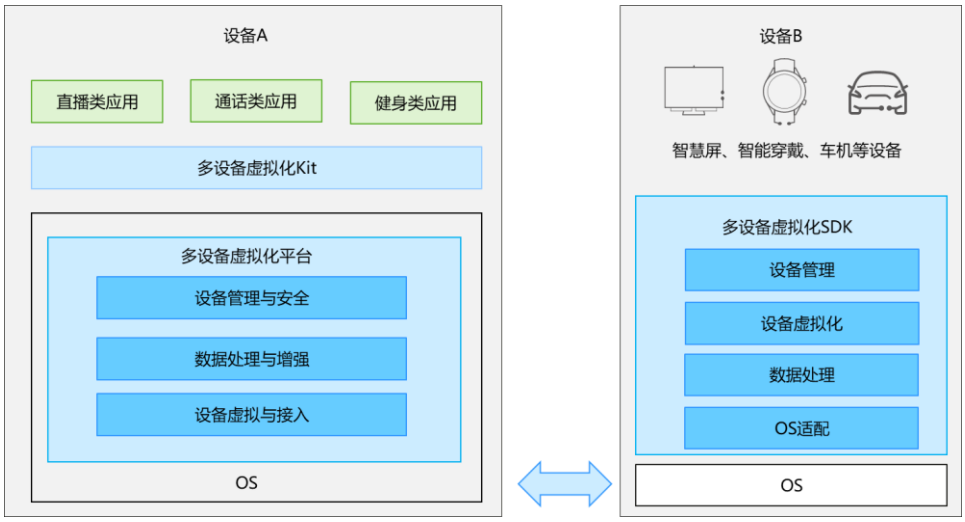
图2-1 分布式软总线示意图



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。

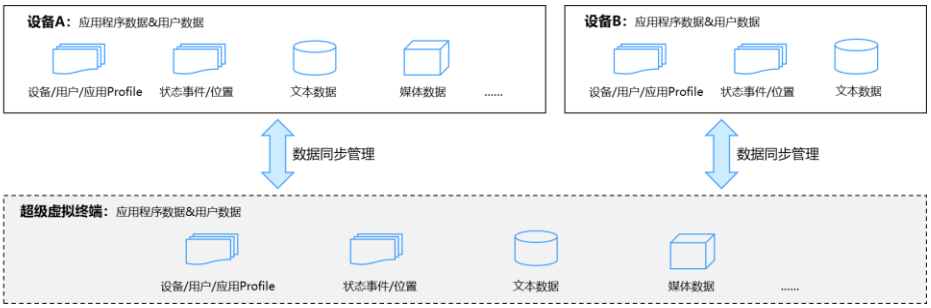
图2-2 分布式设备虚拟化示意图



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。

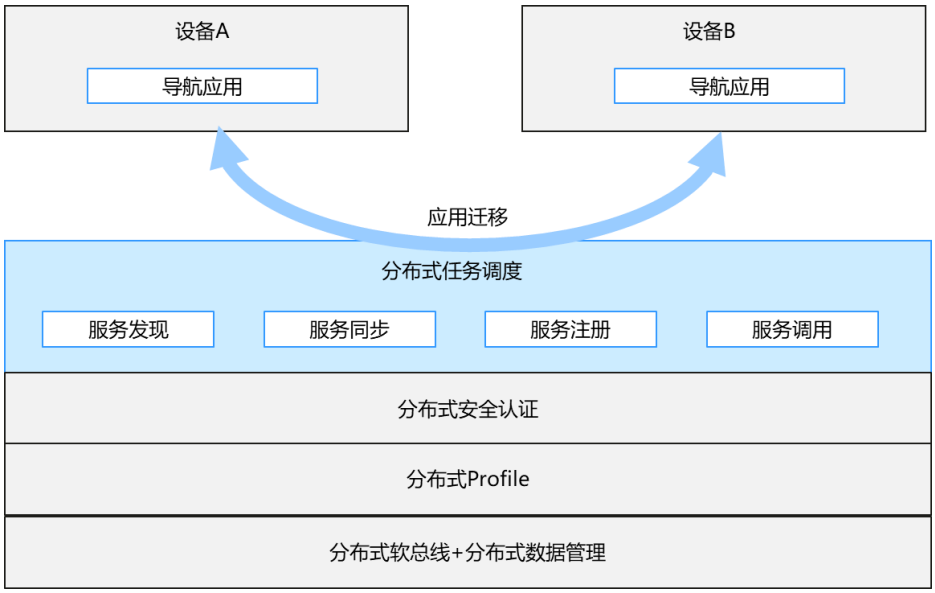
图2-3 分布式数据管理示意图



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
- 黑客攻击，篡改 OS、Firmware 等程序逻辑和数据、植入木马、劫持控制等

3. HarmonyOS 关键安全风险

HarmonyOS 面临的主要安全风险包括：

- **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：**应用程序从单体应用，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。

3 HarmonyOS 安全理论模型

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
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

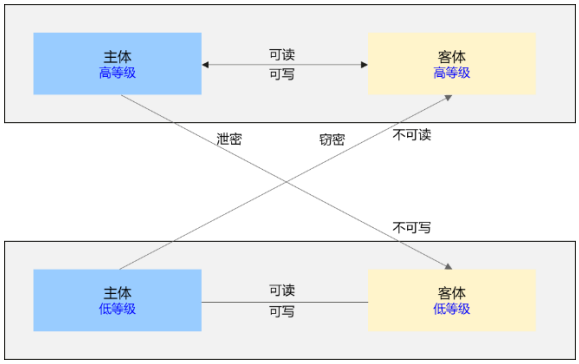
在主流的操作系统中，MS-DOS 大体在 D 级，Windows NT/UNIX 大体在 C1~C2 级水平，B1 级采用多级安全模型，它对敏感信息提供更高级的保护，例如安全级别可以分为秘密、机密和绝密级别。B2 级安全要求计算机系统中所有对象加标签，包括主体、环境、客体进行严格的标记，在严格的标签等级基础上，来实施机密性和完整性保护。

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：



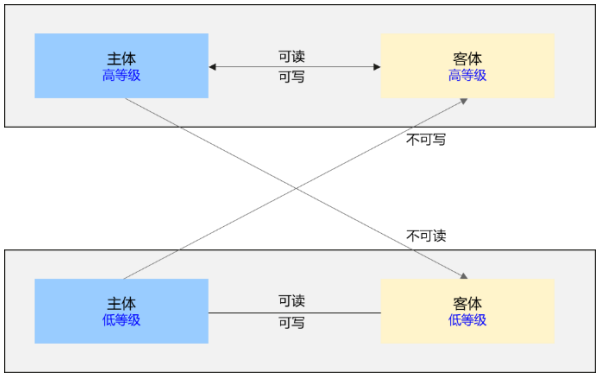
BLP 模型核心规则

- ✓ 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，无论是应用的包，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、G 应用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：

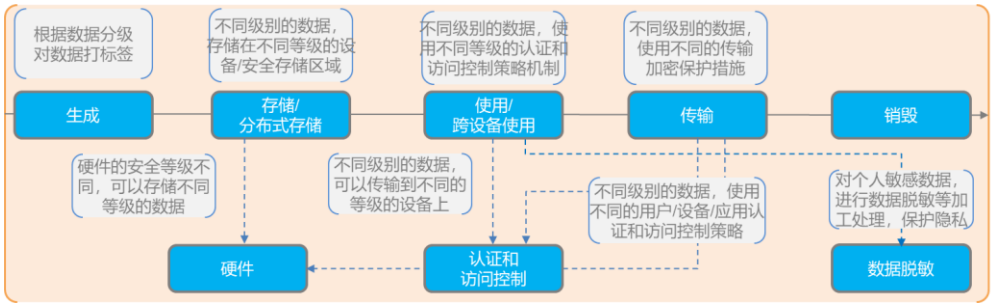
- ✓ 严重：业界法律法规中定义的特殊数据类型，涉及个人的最私密领域的信息或者一旦泄露可能会给个人或组织造成重大不利影响的数据
- ✓ 高：数据的泄露可能会给个人或组织导致严峻的不利影响
- ✓ 中：数据的泄露可能会给个人或组织导致严重的不利影响
- ✓ 低：数据的泄露可能会给个人或组织导致有限的不利影响
- ✓ 公开（无风险）：对个人或组织无不利影响的可公开数据

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、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

数据隐私分类	数据类型	数据分级	举例
	基本个人信息	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

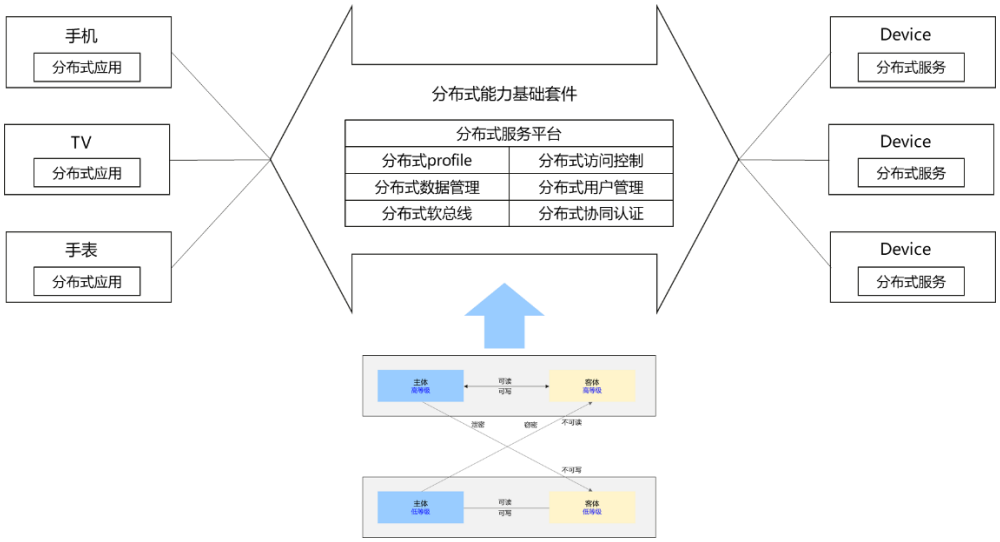
在数据分级基础上，对数据的访问严格遵循分级的生命周期管理：

图3-1 数据访问生命周期管理



根据数据访问生命周期，并结合用户分级、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



4 HarmonyOS“正确的人”身份管理与认证

HarmonyOS 除提供数字密码，图形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。

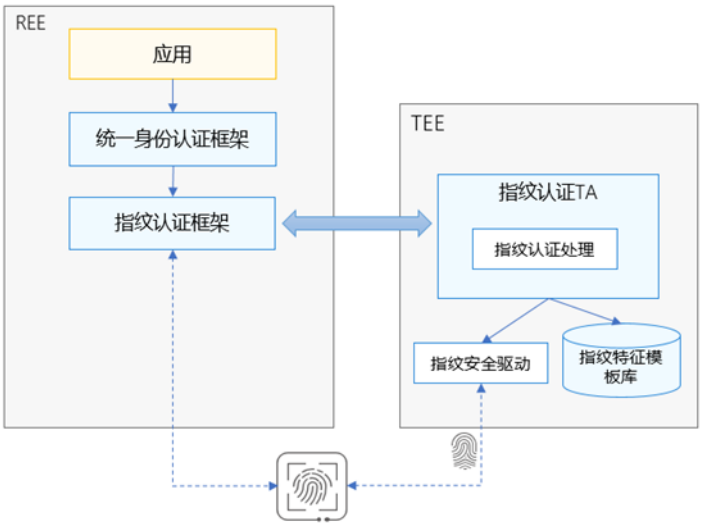
4.1 生物认证

指纹认证

HarmonyOS 目前可提供电容指纹和光学指纹的支持。两种技术方案的体验及安全能力基本一致。不同的终端设备根据其产品定位选择其搭载的指纹认证技术类型。

HarmonyOS 的指纹认证安全框架图如下：

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（Rich Execution Environment，普通执行环境 ）的指纹认证框架只负责指纹认证相关任务的调度和指纹认证结果等数据的传递，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 的指纹认证支持防暴力破解机制，指纹认证连续错误 5 次，将锁定 30 秒不能进行指纹识别。如果指纹认证连续失败 100 次左右，则指纹认证功能将被冻结，必须使用锁屏密码来解锁设备。锁屏密码认证通过后，冻结的指纹认证功能将恢复正常。

指纹认证提供便利的身份鉴别的同时，更容易导致用户忘记锁屏密码。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机制，以便加强用户记忆，减少忘记密码的异常情况发生。

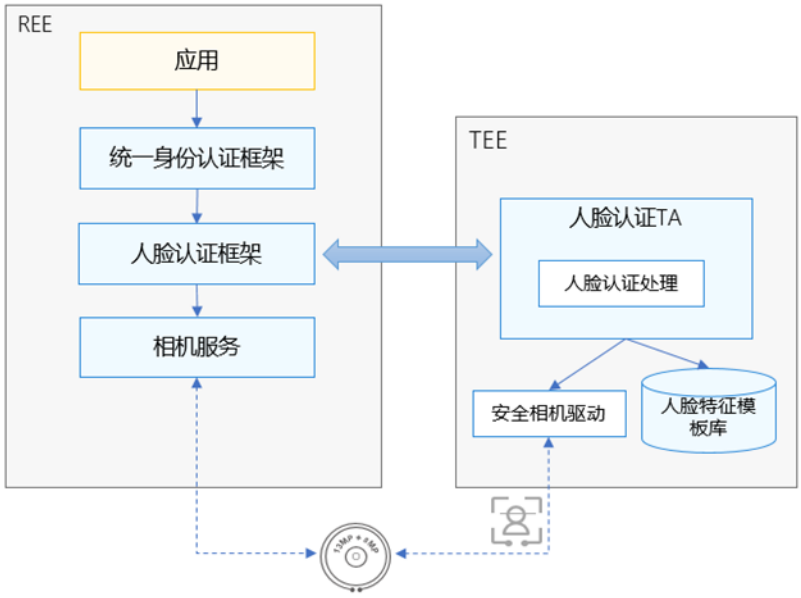
人脸认证

HarmonyOS 提供 2D 和 3D 两种人脸认证方案的支持。3D 人脸认证方案依赖特殊的深度摄像头实现，2D 人脸认证技术则基于普通的前置摄像头实现。3D 人脸认证的准

确率和防伪能力均显著优于 2D 人脸认证。3D 人脸认证技术可支持原生支付应用，2D 人脸认证技术不能支持原生支付应用。不同的终端设备型号根据其产品定位选择其搭载的人脸认证类型。

HarmonyOS 的人脸认证安全框架图如下：

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认证相关任务的调度和人脸认证结果等数据的传递，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 的人脸认证支持防暴力破解机制，用户使用人脸认证连续错误 5 次，将锁定 30 秒不能进行人脸认证，如果人脸认证连续失败 100 次左右，则人脸认证功能将被冻结，必须输入锁屏密码解锁设备。锁屏密码认证通过后，冻结的人脸认证功能将恢复正常。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，由于人脸认证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（以下简称协同认证），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能力。

- 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与本地锁屏密码共用一套防暴力破解机制，不论协同锁屏密码比对失败还是本地锁屏密码比对失败，都会导致对应用户的锁屏密码防暴计数增加，并触发防暴惩罚。

4.3 零信任网络架构

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，会主动对敏感数据访问进行安全加强处置，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处理。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结合。

5 HarmonyOS“正确的设备”系统安全架构

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 系统安全架构概述

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、漏洞防利用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5-1 HarmonyOS 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

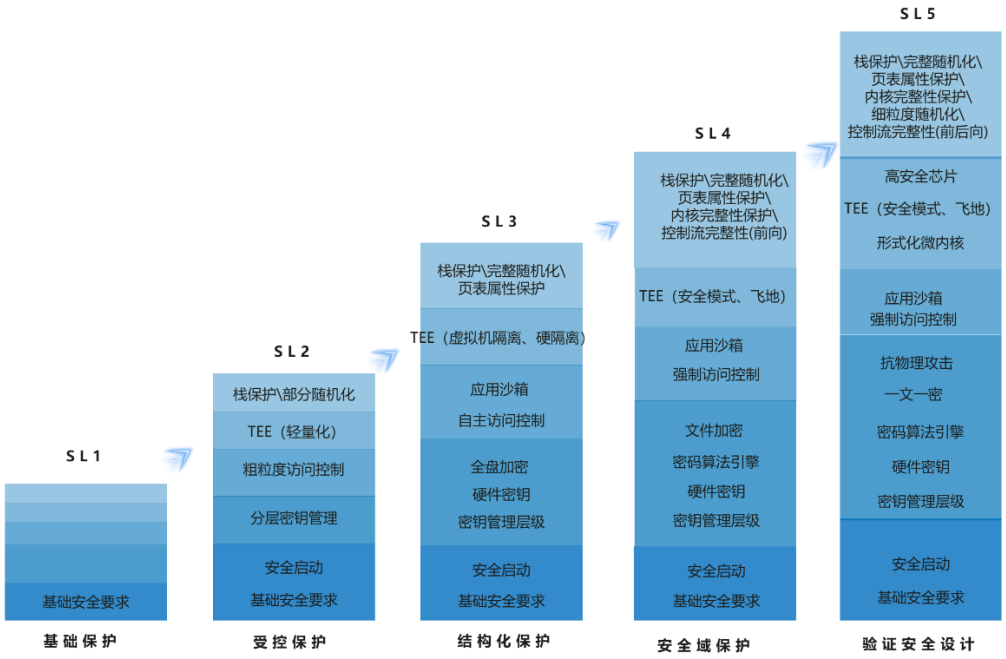
对系统公共资源提供多层级安全隔离（应用/内核/TEE OS/安全芯片），主体对客体资源的访问确保独立、有序、可控，提供了系统性的机密性和可用性机制。

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，将漏洞对系统的威胁降低最低，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。

由于设备软硬件资源限制原因，不同种类 HarmonyOS 设备上的系统安全能力会存在差异，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。

图5-2 HarmonyOS 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，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相应的安全机制。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

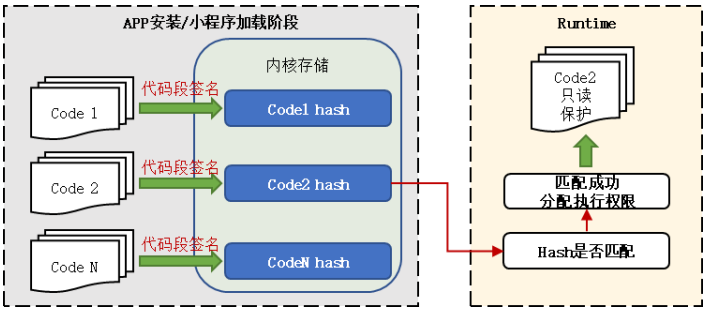
部分较新平台的设备，除了支持安全启动链之外，同时也支持可信启动。即启动过程中，设备基于芯片信任根会逐级度量系统镜像并生成度量日志，该日志既被存储于设备端，同时也可上报到远程服务器。远程服务器可基于预先存储的度量基线，检测设备加载软件的合法性。

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 代码强制签名流程

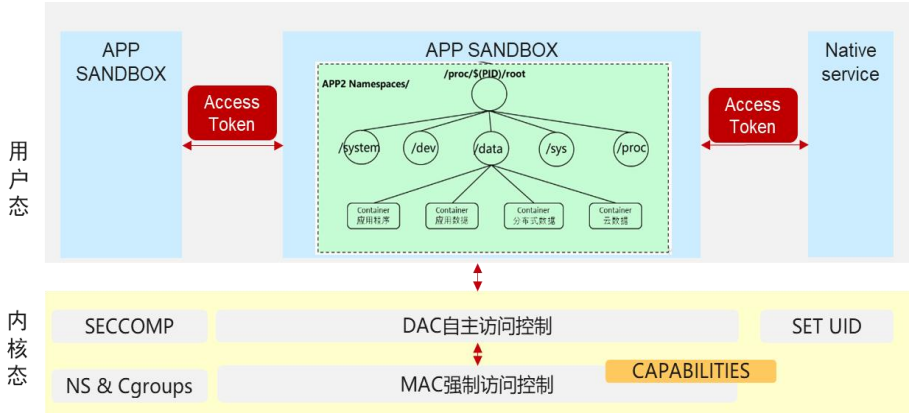


5.3 隔离和访问控制

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5-4 隔离访问控制架构

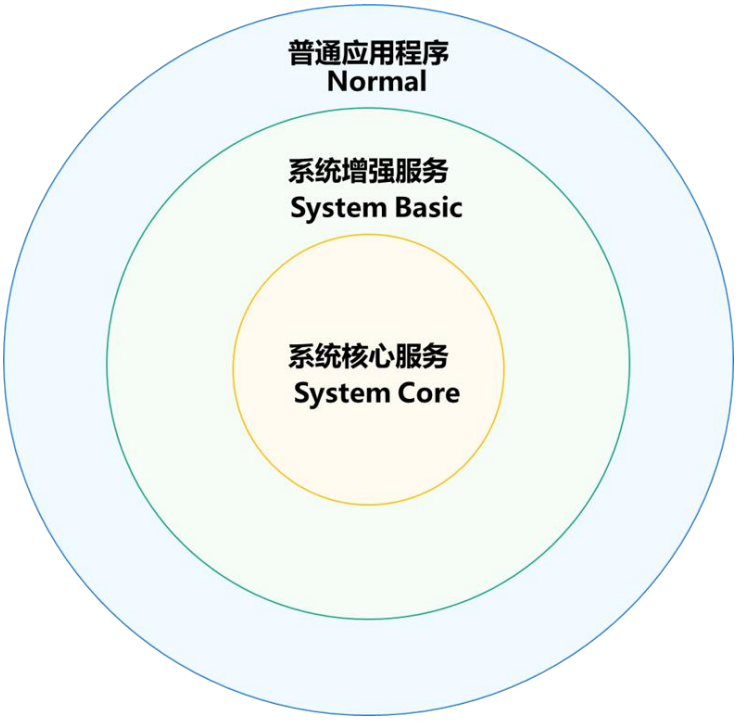


Access Token

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。

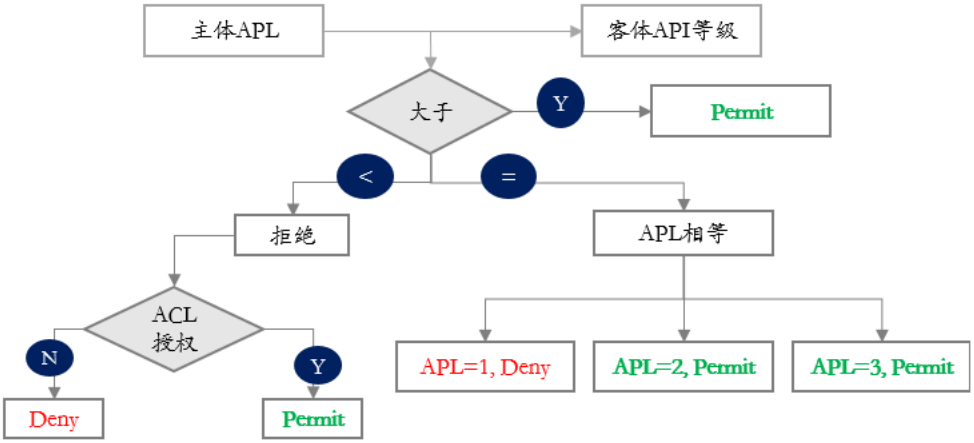
图5-5 HarmonyOS 洋葱圈模型权限管理框架



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	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	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	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。

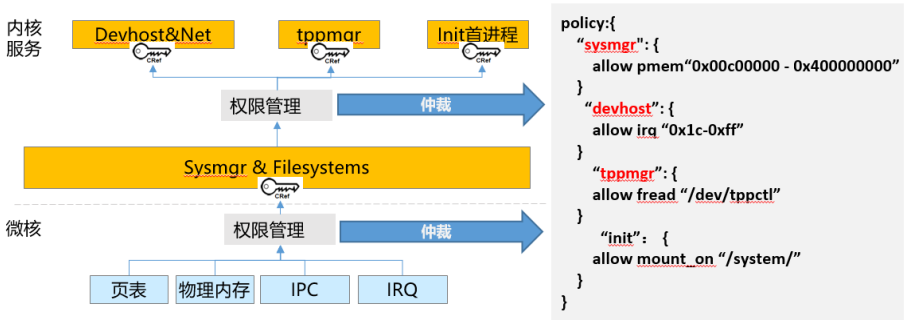
图5-6 Access Token 的访问控制规则图



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，对具有高权限权限的本地进程实施基于权能的强制访问控制，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5-7 Harmony 强制访问控制规则



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 TEE（Trusted Execution Environment ，可信执行环境）和 REE（Rich Execution Environment，普通执行环境）。通过特殊指令 SMC 在 CPU 的 TEE 和

REE 之间切换来提供硬件隔离。在 TEE 中，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（-PIC/-PIE、REOLO）、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。

*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。

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。

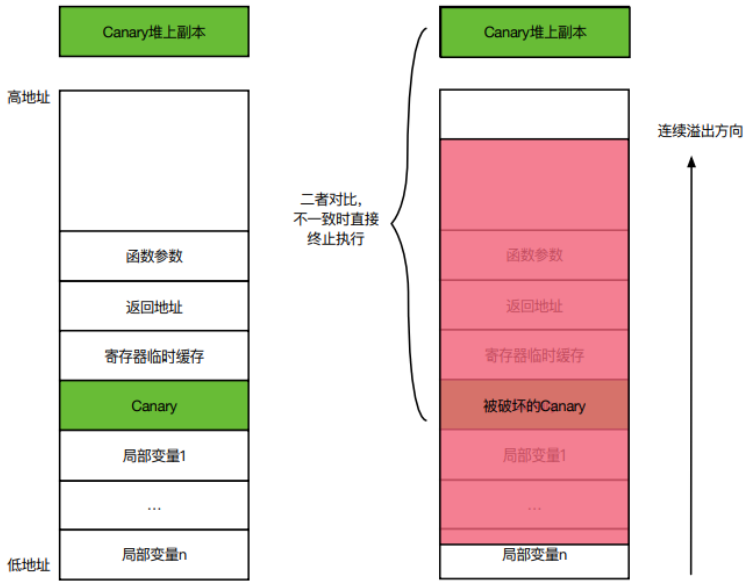
HarmonyOS 利用独立安全芯片的高安全环境（物理安全级），实现锁屏密码保护、文件加密、生物特征保护与识别、密钥管理、可信根、防回退等安全服务。从而在硬件层面为 HarmonyOS 设备的基础安全能力提供保障。

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。

6 HarmonyOS“正确的访问数据”分级访问控制架构

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。

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}

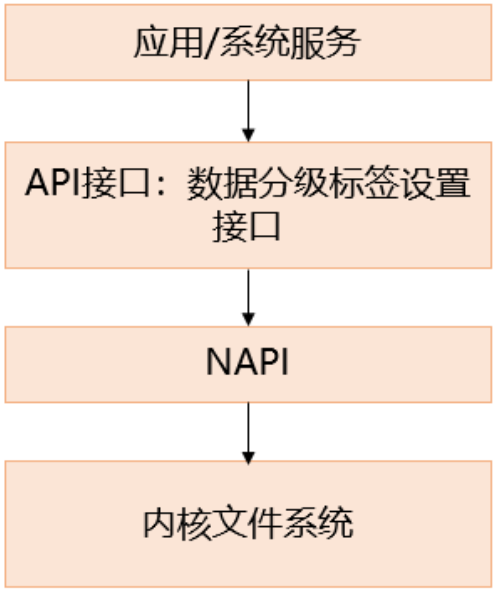
安全目标、潜在影响	低	中	高
机密性 对于信息的访问和披露通过加密和访问控制等手段进行保护，包括个人隐私和专利信息。	未授权的信息披露可能会对组织运行/组织资产/个人产生有限的不利影响。	未授权的信息披露可能会对组织运行/组织资产/个人产生严重的不利影响。比如造成罚款，形象遭到负面影响等。	未授权的信息披露可能会对组织运行/组织资产/个人产生严重或灾难性的不利影响。比如造成公司重大商业损失，声誉损失，退出特定行业等
完整性 防止信息被非法修改和销毁，确保信息的完整性和真实性	未授权的信息修改和信息销毁可能对于组织运行/组织资产/个人产生有限的不利影响	未授权的信息修改和信息销毁可能会对组织运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

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，业务应用可以通过调用风险等级标签的设置 API，设置应用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；



应用需要根据 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；同时应用需要评估对应设备的安全等级，应用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。

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	基于 HarmonyOS 新架构， HarmonyOS 提供 EL5 加密机制： 应用可被独立调度且不允许后台驻留，因此，当应用被调度时，它的数据沙箱的加密密钥被激活；当应用被终止或者挂起时，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

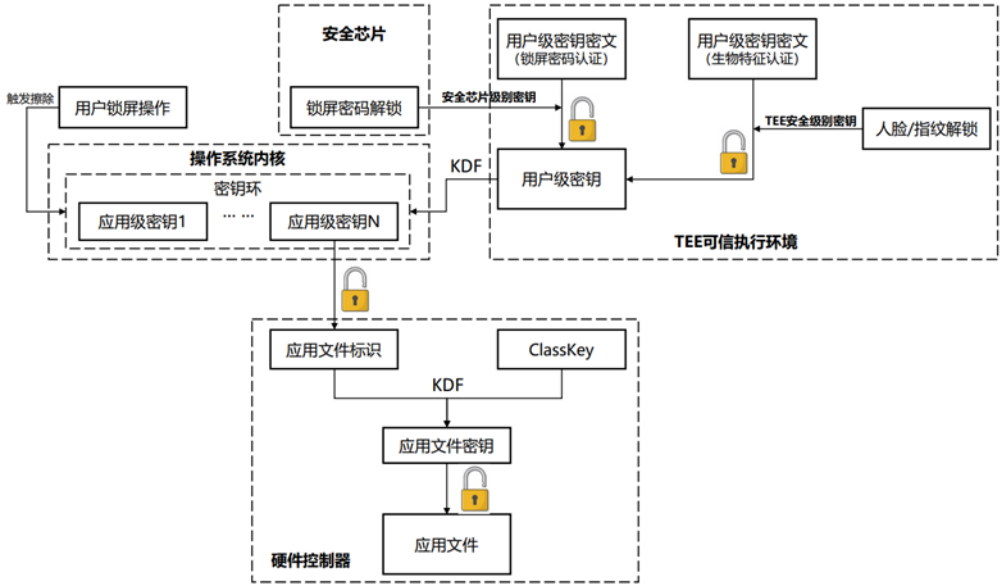
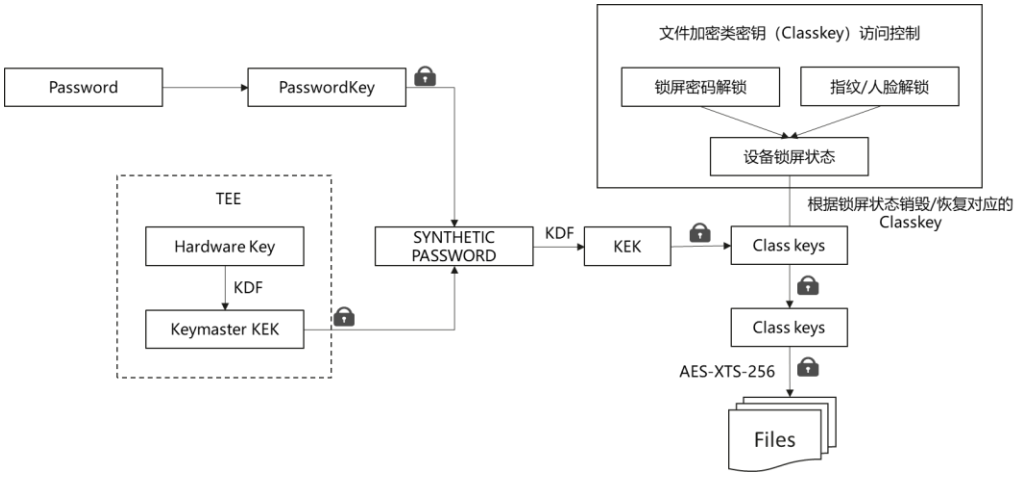


图6-2 HarmonyOS 移动终端设备文件级加密的密钥层级



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。

6.3 HarmonyOS 数据传输安全机制

HarmonyOS 分布式连接安全

为保证分布式系统的连接安全，实现用户数据在分布式场景下各个设备之间的安全流转，需要保证设备之间相互正确可信，即设备和设备之间建立过信任关系，并能够在验证信任关系后，搭建安全的连接通道，实现用户数据的安全传输。设备之间的信任关系包括同一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的安全连接，提供基于同账号的设备认证能力。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 Wi-Fi 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，在两个设备间建立共享秘密信息，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参与建立的共享秘密信息，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 Wi-Fi 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。当消费者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

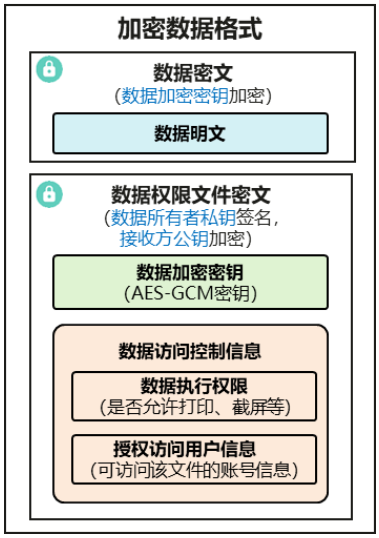
设备登陆账号后，数据加密分享服务会基于账号身份生成两对椭圆曲线公私钥对，分别用于消息签名和数据加解密，并在系统密钥管理服务内进行管理。

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**。

发送方生成的加密数据格式



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数据执行权限为 HarmonyOS 上的应用权限，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。

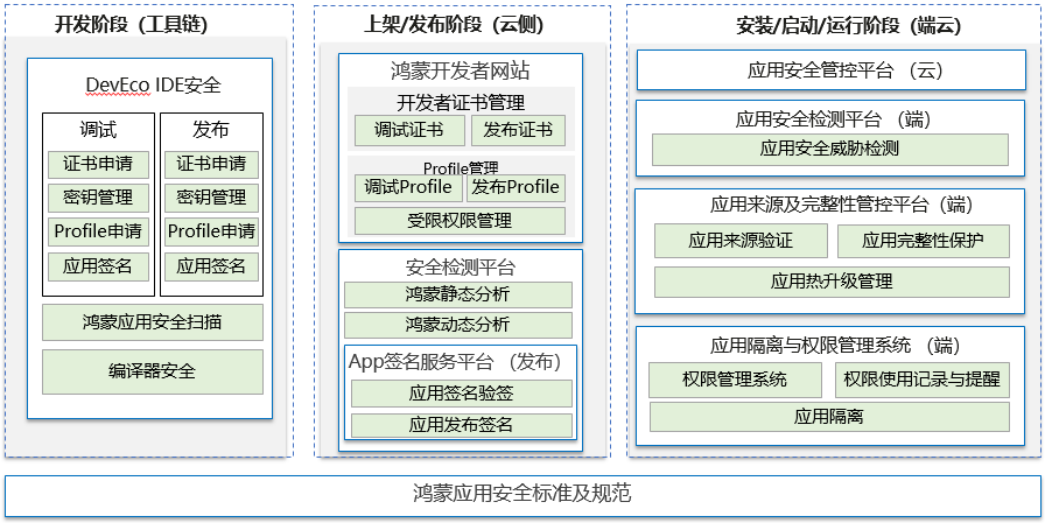
HarmonyOS 的恢复出厂设置，支持对存储数据的安全擦除。通过给物理存储器发送命令，进行覆写操作，完成底层数据擦除。擦除后数据是全 0 或者全 1，确保用户的敏感数据不能通过软硬件手段恢复，能够保护用户设备转售、废弃后的数据安全。

7 HarmonyOS 应用生态治理架构

HarmonyOS 对于应用生态提供了相应的纯净治理机制，来确保运行在超级终端上的应用程序满足 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。

7.1 HarmonyOS 应用程序生命周期治理架构概述

图7-1 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。

图7-2 HarmonyOS 应用程序生命周期关键技术和措施

如图 7-2 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。

7.2 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 Studio 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 Studio 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：依据国家互联网信息办公室 2016 年 6 月 28 日发布的《移动互联网应用程序信息服务管理规定》，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。

7.3 HarmonyOS 应用程序“纯净”上架

当发布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 不仅对应用的包（Package）进行了签名，对应用运行的内存页表也进行了签名，不只是保证应用安装时的可信，也保证应用运行时的可信，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。

7.4 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：HarmonyOS 应用上架到 HarmonyOS 应用市场分发前，应用市场会对应用进行严格地审核，确保 HarmonyOS 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。HarmonyOS 应用签名是 HarmonyOS 应用必须包含的内容，用于校验 HarmonyOS 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。

    1) 隐私权限授权（访问前）：应用访问敏感数据或者能力前需要申请相应的权限，当应用申请权限时，开发者必须填写权限使用理由字段，以便帮助用户理解应用申请此权限的合理性并作出正确的选择；

2) 隐私指示器（访问中）：敏感数据或能力（例如，麦克风）被应用持续访问时，通过状态栏显示实时提醒用户，便于用户感知应用访问行为；

3) 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。

8 HarmonyOS 安全标准遵从与认证

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 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。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 HarmonyOS 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 HarmonyOS 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。

HarmonyOS 版本已获得认证：

认证名称	认证对象	颁发机构	说明
CC EAL 6+	HarmonyOS 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	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 HarmonyOS 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	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 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 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。

9 HarmonyOS 典型高安全业务能力介绍

HarmonyOS 典型高安全业务能力介绍，通过对诸如华为账号、Huawei Pay、手机交通卡、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。

9.1 华为账号

华为账号是用户用于访问所有华为以及华为合作伙伴提供的产品、网站和服务的账号，是用户在华为生态的数字身份证。

用户使用华为账号登录终端设备后，将可以使用这台设备的华为云服务，例如华为支付、钱包、应用市场、云空间、华为商城、游戏中心、华为视频、华为音乐、运动健康等；用户也可以使用华为账号登录访问华为云、华为云会议、华为开发者联盟、华为官网等网站和服务。用户还可以使用华为账号一键登录功能登录 HarmonyOS 生态应用。

华为账号安全设置

用户在注册或更换密码时，需设置长度为 8 位以上的强密码，至少包含字母，数字，特殊符号中的两种，且不能包含 3 个及以上连续相同的字符。

账号登录后会引导用户设置安全要素，或者在账号中心->账号安全中设置：安全手机号，安全邮箱，紧急联系人，实名认证等。在用户重置密码时，这些安全要素将被用来验证用户身份。

您在使用账号过程中，您可以通过登录设备管理来实时查看您的登录的设备信息，若出现异常登录设备可将其移除。

华为账号安全策略

数以千计的华为自有应用，以及数以万计的三方开发者应用选择使用华为账号，因此安全是华为账号的基石。

华为账号安全策略：华为账号选择双因素认证作为华为账号安全的起点。在华为账号双因素认证的基础上，业务可通过业务级安全措施来进一步保障业务安全，例如，用户通过双因素登录后，支付业务可通过支付密码进一步保护支付业务安全。

双因素认证：用户通过验证两个认证要素完成身份验证，可以从用户知道的（例如账号密码，锁屏密码等）、用户持有的（例如短信验证码，受信任设备等）、用户生物特征（例如人脸，指纹等）中选择两个认证要素。例如用户在新设备登录华为账号时，验证密码和手机验证码。双因素认证技术可抵御非法访问者，提高认证的可靠性。

主动安全提醒：在您的账号发生重大更改时，例如，密码发生更改，或者在新设备上使用华为账号登录时，华为会以短信、电子邮件和推送通知等方式知会您。如有异常发生，华为会提示您更改账号密码，请立即前往“账号中心”的“更改密码”来更改您的密码。如需更多帮助，请联系华为在线客户寻求帮助。

账号风控

华为账号风控基于全流程和全场景的风险识别机制和对抗机制，确保用户在注册，登录，重置密码等账号生命周期管理中，保护用户信息的安全性。

华为账号风控采用了多种策略和程序来保护您的账号。这包括限制重新尝试登录和尝试重设密码的次数，保持欺诈监控以帮助在发生攻击时进行识别，以及定期回顾策略以让我们针对可能影响客户安全性的任何新情况作出调整。

用户数据隐私保护策略

华为账号会对用户敏感信息进行加密保存和传输。对于任意三方想要获取华为账号的敏感信息，确保有用户授权同意。

9.2 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号和设备的其他信息，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 TLS 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用户的 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。

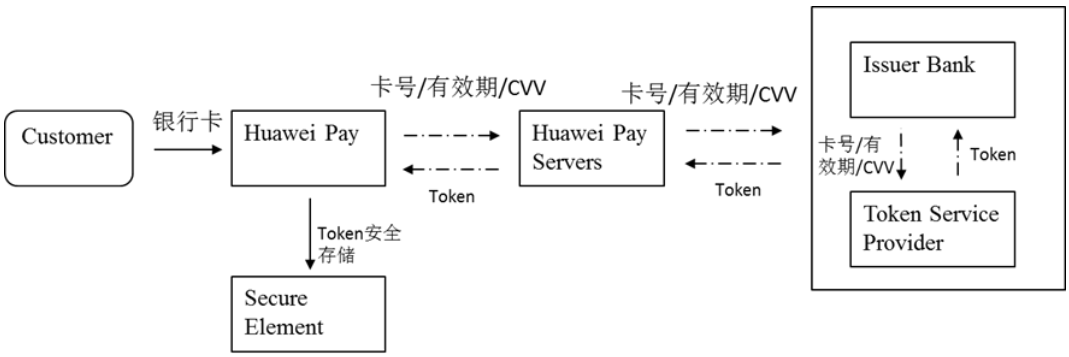
如果用户接受该条款与条件，华为会将所接受条款以及 CVV 码发送到发卡机构，并执行“绑定”流程。有关您设备的信息（例如，姓名、设备型号以及绑定 Huawei Pay 所需的华为手机，以及添加付款卡时您大致的位置（如果启用了“定位服务”）。发卡机构将使用此信息，决定是否批准将付款卡添加到 Huawei Pay。

“绑定”流程会执行以下两项操作：

- 设备下载代表银行卡的凭证文件。
- 手机将付款卡与安全元件绑定。

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9-1 Huawei 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。

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指纹或设备密码认证后，才会允许进行支付。如果可用，指纹即为默认的支付方式；但是用户可随时使用密码来代替指纹。如果尝试通过匹配指纹 1 次不成功，会自动提供密码输入选项。

使用 Huawei Pay 进行非接触式支付

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

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

暂停使用、移除付款卡

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

Huawei Pay 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

Huawei Pay 通过了国际 PCI-DSS 认证；符合支付行业权威安全标准要求。

9.3 手机交通卡

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

交通卡开卡

用户在钱包应用中支付完开通交通卡所需的费用后，发起开卡请求。华为的可信服务平台（SEI TSM）在主安全域（ISD）的 SCP（Secure Channel Protocol）的保护

下，为待开通的交通卡创建一个单独的 SSD，将对应交通卡的卡应用按照 GP Card（GlobalPlatform Card）规范转换为 APDU 指令。在 ISD 的 SCP 的保护下，将 APDU 指令下载到安全芯片中，并完成卡应用的实例化，然后将卡实例让渡给为之创建的 SSD。SSD 的秘钥由交通卡公司的可信服务平台（SP TSM）管理。SP TSM 将一卡一秘的卡片秘钥等个人化数据，通过使用 SSD 的秘钥建立 SCP 加密保护下载到 SE 中的交通卡卡应用内。至此卡片在手机中开通成功。

交通卡余额充值

用户在钱包应用中支付完想要充值的金额后，发起余额充值请求。SP TSM 在确认收到了款项支付完成的通知后，通过充值初始化指令向 SE 中的卡片应用发起随机数的挑战，卡片收到挑战后，使用卡内秘钥计算并返回计算结果。SP TSM 使用该卡片的秘钥验算卡片回复的计算结果，验算成功则表明 SP TSM 验证卡片合法性成功。随后 SP TSM 再使用卡片秘钥做另一次计算，并将计算结果封装在充值指令中下载的 SE 中的卡片应用内，卡片也需要做一次验算，验算成功则表明卡片对 SP TSM 的合法性认证成功，所以卡片会将本次的充值金额数，累加在卡内的余额存储区域。由于卡片秘钥分别存储在 SE 中的卡应用内和 SP TSM 的硬件加密机内，秘钥在两个端点的存储均为硬件安全级别，且没有第三者能知晓该秘钥，故充值只能依靠交通卡公司的 SP TSM 完成。

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 SE 中的交通卡进行非接触界面的通信。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。

交通卡移除到云端

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

交通卡退卡

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

9.4 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 Digital Key 数字密钥规范。

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应用，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，HarmonyOS 的可信服务管理平台（TSM）会作为安全元件的管理者，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可信的服务管理器（TSM）将车辆的数字密钥下载到手机中。从而将自己的智能手机变成汽车钥匙。

用户的数字钥匙存储在智能手机的独立安全单元(Secure Element)中。它是业内公认的、经过认证的芯片。安全级别达到金融级的标准。

当用户进行恢复出厂设置后，设备会主动禁用车钥匙和删除车钥匙以保证用户财产的安全。

10 构建具备韧性的 HarmonyOS 安全体系架构

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利用，在漏洞发生后最快速度恢复业务和修复漏洞”。

10.1 HarmonyOS 可信工程

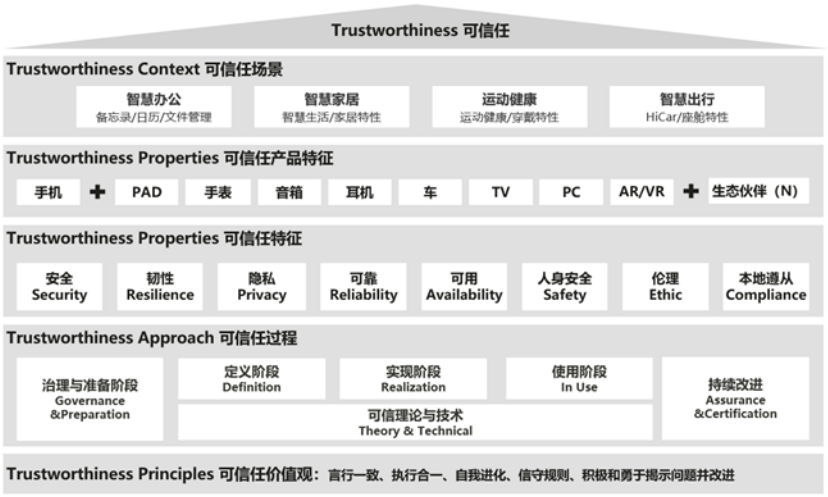
今天，人类社会正在迈向万物互联的智能世界，全场景、全连接、智慧化等发展趋势，对消费者产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买一个产品的基本条件。可信不仅仅是产品外在表现的结果，更是产品内在实现的过程，是结果和过程双重可信的高质量。

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10-1 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。

10.2 HarmonyOS 安全攻防实验室

华为终端奇点安全实验室是由业界顶级安全研究员组建的一支安全研究和渗透测试团队，通过如下活动，持续对 HarmonyOS 产品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 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

10.3 HarmonyOS 漏洞奖励计划

华为非常重视自身产品和业务的安全问题，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业务的安全性，因此，我们发布了 HarmonyOS 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/P/Pure 系列
平板	MatePad
穿戴	智能手表
IoT	智慧屏/路由/音箱等

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://device.harmonyos.com

10.4 HarmonyOS 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客户的意见，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。

11 HarmonyOS 安全能力开放使能生态

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。同时，为生态设备提供专业 CBB、安全模组、独立芯片等。

11.1 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。

11.2 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。

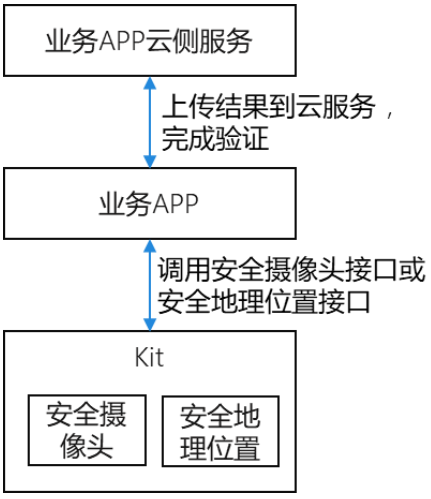
应用设备状态检测（Device Verify）

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。
HarmonyOS 系统向应用提供安全摄像头和安全地理位置能力，如下图所示：



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。

11.3 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。

11.4 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，但可以将公钥共享给对方，对方在对公钥进行验证后，使用公钥对消息使用加解，并传递给私钥持有者，私钥持有者使用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。

11.5 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或安全芯片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、包名、签名等信息，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、密钥访问控制方式等属性。其中，证书链是由每台设备唯一拥有的设备证书签发，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。

11.6 在线认证服务 Online Authentication Kit

在线认证服务提供免密认证框架，支持 FIDO（Fast Identity Online）、IIFAA（International Internet Finance Authentication Alliance）、SOTER 标准免密认证协议，提供免密身份认证的相关能力，既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，几乎所有的设备厂商都支持 FIDO 免密认证协议，同时众多生态应用厂商包括中国工商银行，中国银行，农业银行，交通银行等各大行，以及众多证券，金融应用等也广泛使用该能力。HarmonyOS 当前构建了基于 FIDO UAF 的免密身份认证功能，应用可以通过接入本地的 FIDO 服务实现开通、使用、关闭免密身份认证等能力。

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。当前 HarmonyOS 提供了 IFAA 免密认证模

块，提供移动端接入免密身份认证的相关能力（IFAA 在本文中指 HarmonyOS 中的免密认证模块，IIFAA 特指联盟及相关技术规范）。

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。目前，SOTER 已广泛应用于微信指纹支付、公众号/小程序等授权接口，并已通过相应验证。当前 HarmonyOS 提供了 SOTER 模块，可为移动端业务提供相关的免密认证能力。

11.7 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。

11.8 系统安全控件&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
- 文档扫描 picker

11.9 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_CCM；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应用账号密码，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。

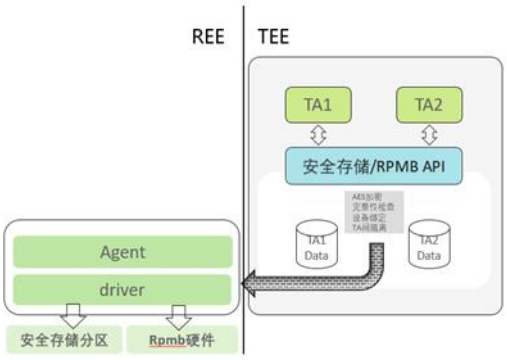
11.10 可信执行环境

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。

11.11 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。

A 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	应用 lication Programming Interface	应用软件编程接口
APK	Android Package	Android 安装包

英文缩写	英文全称	中文全称
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 应用 lication	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

英文缩写	英文全称	中文全称
UID	User Identifier	用户身份标识符
mmap	memory-m 应用 ed	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
TSM	trusted service manager	可信服务平台
APDU	应用 lication 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

