HarmonyOS 3 安全技术白皮书

文档版本 V1.0

发布日期 2022-08-15

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 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 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”分级系统安全架构，介绍了系统安全分级的体系架构，基于成本、风险、能力综合平衡为不同类型的设备构建对等的安全能力。通过对芯片安全、硬件安全、内核安全、漏洞防利用、安全隔离环境、形式化验证等关键技术的介绍，为开发者提供了一套“乐高式”系统安全能力的灵活组装与搭配的能力。
- 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，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，围绕最小权限授权、应用生命周期治理、可信设备生态构建，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。
- 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 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。带来简捷，流畅，连续，安全可靠的全场景交互体验。

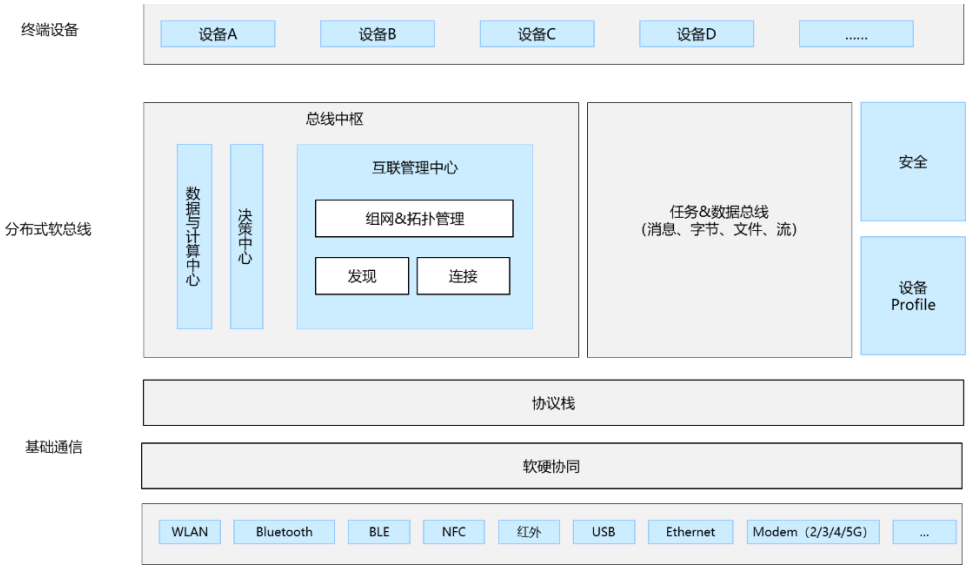
2.2 HarmonyOS 技术特征

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。

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。

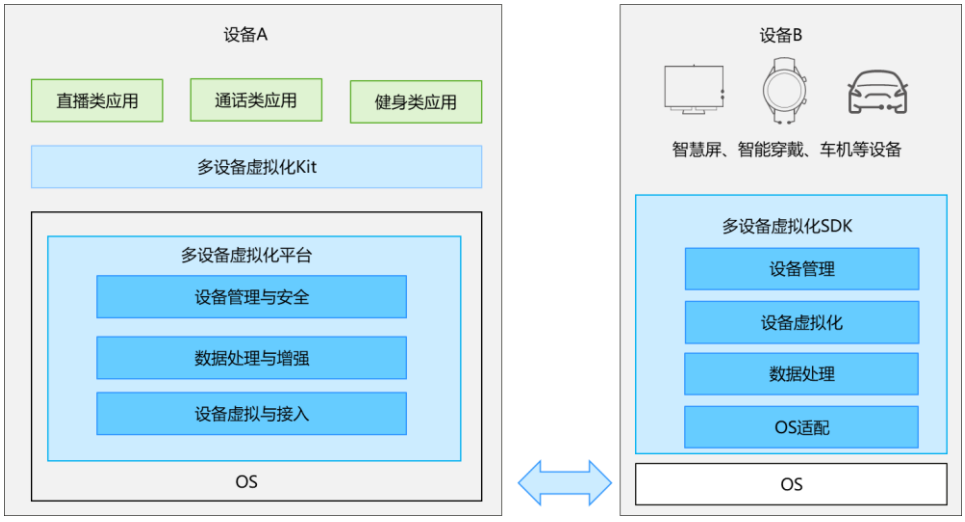
图2-1 分布式软总线示意图



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

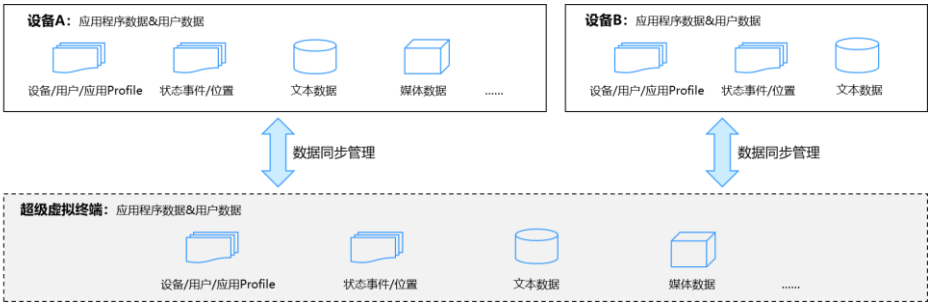


分布式数据管理

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

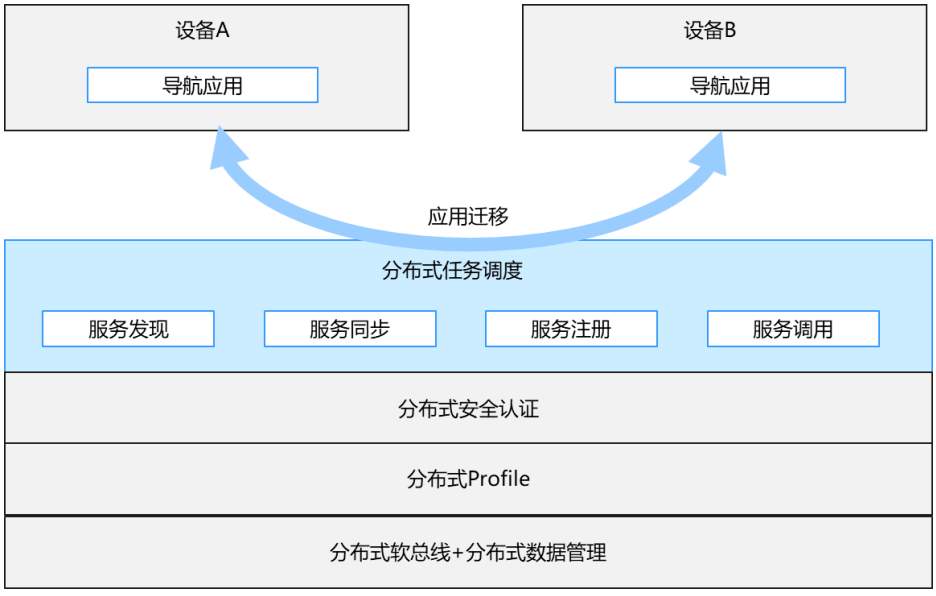
图2-3 分布式数据管理示意图



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

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 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。

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

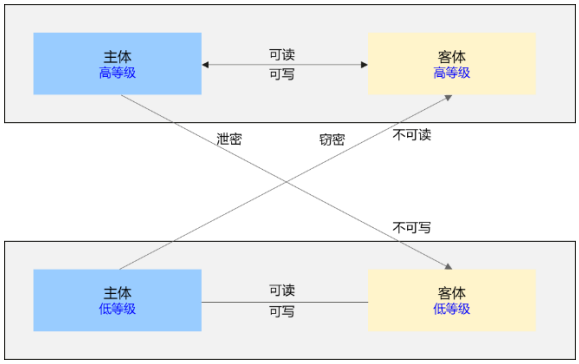
在主流的操作系统中，MS-DOS 大体在 D 级，Windows NT/UNIX 大体在 C1~C2 级水平，B1 级采用多级安全模型，它对敏感信息提供更高级的保护，例如安全级别可以分为秘密、机密和绝密级别。B2 级安全要求计算机系统中所有对象加标签，包括主体、环境、客体进行严格的标记，在严格的标签等级基础上，来实施机密性和完整性保护。

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

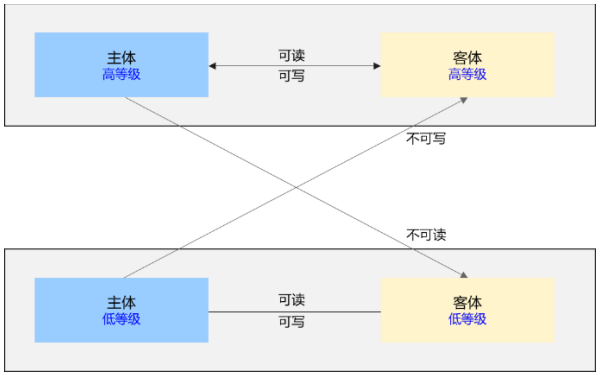
✓ 不上读-主体不可读安全级别高于它的客体（数据）

✓ 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都经过 HarmonyOS 的应用市场签名，确保仿冒、伪造的应用无法运行。
- 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，证书由华为官方签名，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：

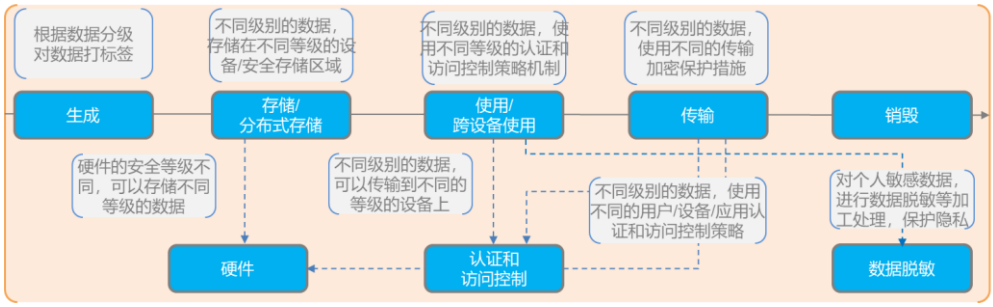
- ✓ 严重：业界法律法规中定义的特殊数据类型，涉及个人的最私密领域的信息或者一旦泄露可能会给个人或组织造成重大的不利影响的数据
- ✓ 高：数据的泄露可能会给个人或组织导致严峻的不利影响
- ✓ 中：数据的泄露可能会给个人或组织导致严重的不利影响
- ✓ 低：数据的泄露可能会给个人或组织导致有限的不利影响
- ✓ 公开（无风险）：对个人或组织无不利影响的可公开数据

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，如华为帐号、社交帐号等
	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

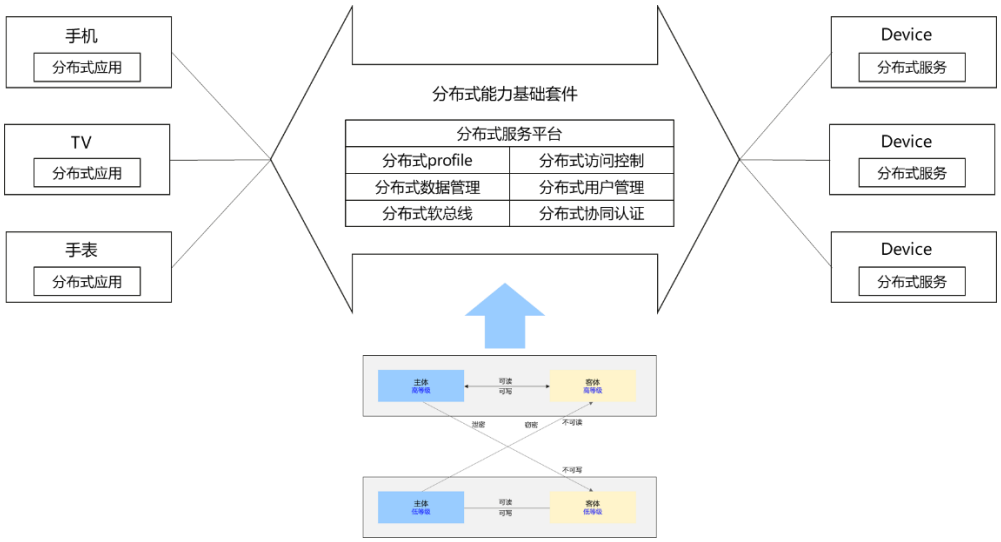
在数据分级基础上，对数据的访问严格遵循分级的生命周期管理：

图3-1 数据访问生命周期管理



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



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。

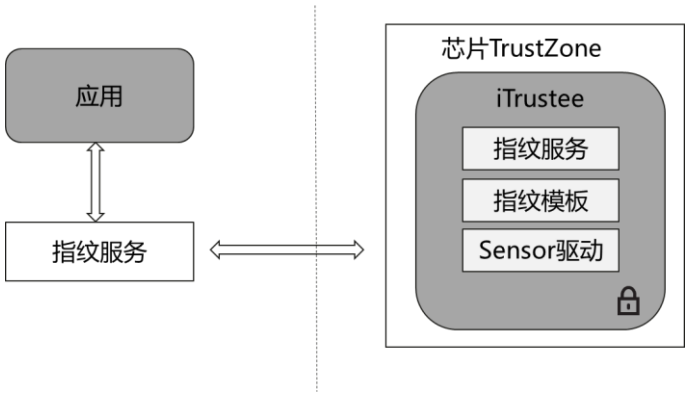
4.1 生物认证

指纹认证

HarmonyOS 目前可提供电容指纹、光学指纹及超声波指纹识别的支持。三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识别技术类型。

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。

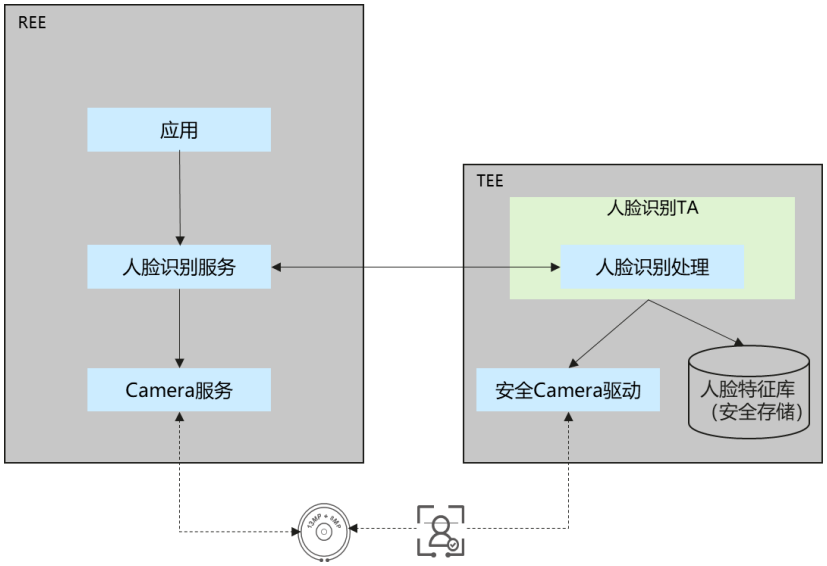
指纹识别提供便利的身份识别的同时，用户更容易忘记锁屏密码。HarmonyOS 采用 72 小时内未使用密码解锁则强制要求用户输入密码解锁，以便加强用户记忆，减少忘记密码的异常情况发生。

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原生支付应用，2D 人脸识别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识别类型。

HarmonyOS 的人脸识别安全框架图如下（部分高通与 MTK 平台使用的通用人脸框架）：

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。

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

  用户所绑定的蓝牙配件可作为“可信持有物”，以认证用户身份。协同认证提供多因子叠加的增强认证能力，在蓝牙配件连接到手机且处于佩戴状态时后，当用

户在手机上发起锁屏解锁，手机会为蓝牙配件发放持续佩戴 TOKEN。当蓝牙设备断开连接，或被用户摘下时，该 TOKEN 会失效，无法和手机完成持续佩戴检测。

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。

5 HarmonyOS“正确的设备”分级系统安全架构

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，提供了一套系统安全参考架构。并基于该参考架构，形成了 HarmonyOS 设备安全分级规范。本章尝试对 HarmonyOS 设备的系统安全架构及安全分级要求中的典型安全技术进行阐述。

5.1 HarmonyOS 设备安全分级规范

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

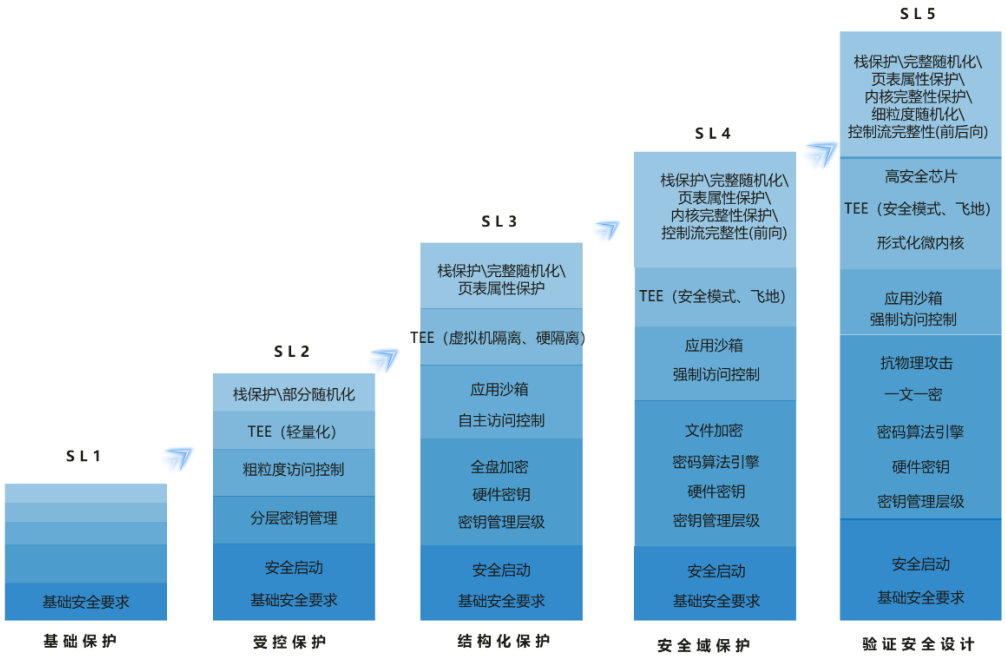
HarmonyOS 系统安全架构如下图所示：

图5-1 HarmonyOS 系统安全架构

上图为典型的 HarmonyOS 单设备系统安全架构，在不同种类 HarmonyOS 设备上的实现会存在差异，取决于设备的威胁分析（风险高低）和设备的软硬件资源。HarmonyOS 在参考业界权威的安全分级模型基础上，结合 HarmonyOS 实际的业务场景和设备分类，将 HarmonyOS 设备的安全能力划分为 5 个安全等级：SL1-SL5。HarmonyOS 操作系统生态体系中，要求高一级的设备安全能力，默认是包含低一级的设备安全能力。

分级概要可参考下图：

图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，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。

以下章节分别介绍每个安全等级中典型的关键安全技术。

5.2 系统安全等级 SL1

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。

5.3 系统安全等级 SL2

设备唯一密钥

设备唯一密钥是在硬件中固化的一个唯一标识，设备制造阶段写入。设备唯一密钥由于具备唯一性，在 HarmonyOS 中多作为根密钥用于密钥派生。

在更高安全等级的 HarmonyOS 设备中，设备唯一密钥的访问控制会更加严格，如软件无法访问，仅能通过硬件密码引擎访问该信息，并进行密钥派生。

密钥管理

HarmonyOS 给应用提供密钥管理服务 HUKS，包括密钥全生命周期管理、加解密计算服务、证书管理等功能。HarmonyOS 应用开发者基于 HUKS 可进行密钥、证书的生命周期管理和加解密算法调用。

HarmonyOS 对密钥访问做了严格的权限控制。密钥仅可由生成密钥的应用访问；在密钥生成时, HUKS 记录了应用的 UID、签名、包名等信息，供应用访问密钥时进行身份验证。HarmonyOS 应用可以使用身份认证功能来增强密钥的访问控制，如生物认证和 PIN 码，HUKS 确认身份认证结果后才允许相应的密钥访问与操作。

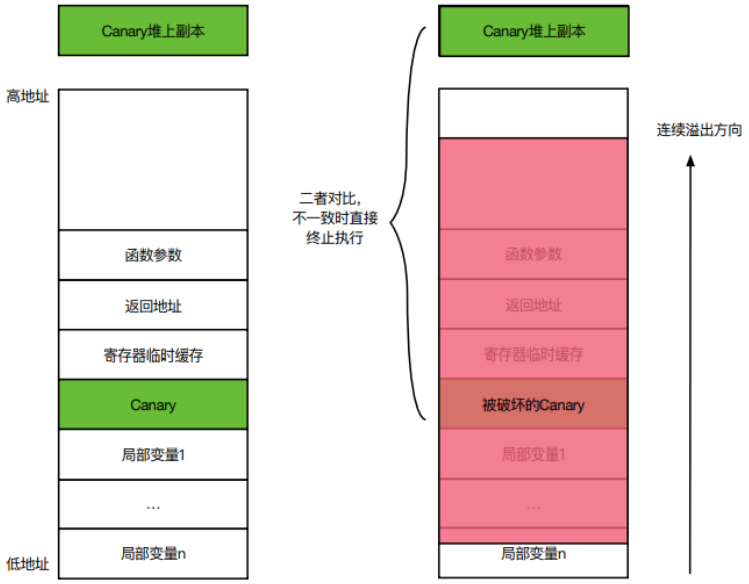
HarmonyOS 提供了 Key Attestation 功能，可以基于注入到设备的设备证书对密钥做认证。设备证书是设备唯一的，每个设备拥有自己的设备证书。同时 HarmonyOS 提供了 ID Attestattion 认证功能，可以向云端提供可信的设备 ID 认证能力，包括认证 SN、IMEI 等设备标识。

在更高安全等级的 HarmonyOS 设备中，密钥管理服务的软件架构实现会发生变化，如在高安 HarmonyOS 设备中，密钥管理服务会基于可信执行环境甚至高安芯片实现。

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5-3 栈保护原理



自主访问控制

1985 年 TCSEC 橘皮书中提出了两种著名的访问控制模型，自主访问控制和强制访问控制。

自主访问控制广泛应用于文件系统权限设计，HarmonyOS 从 SL2 安全等级开始要求设备支持自主访问控制模型。自主访问控制包含经典的 UNIX 权限检查和 ACL 访问控制列表，是基于用户、组、权限来实现的；拥有文件的用户可以将对象的权限分配给其他用户，称“自主”。

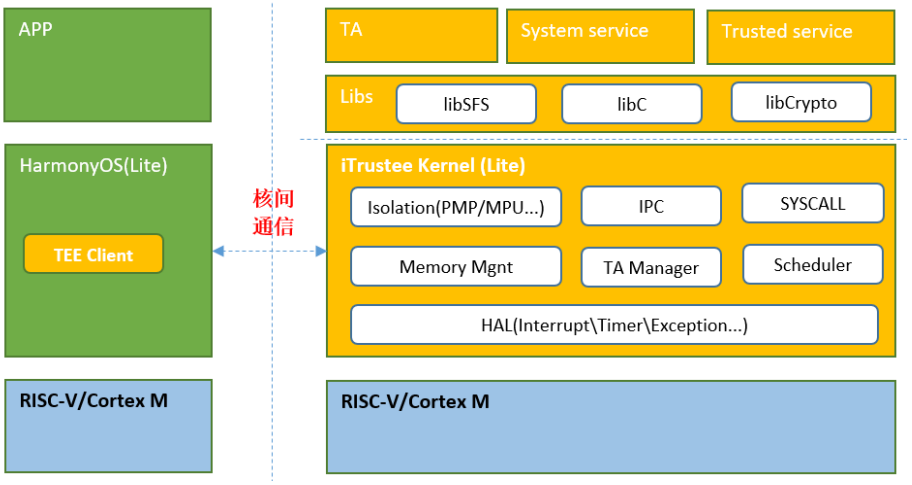
自主访问控制模型的特点是授权的实施主体自主负责赋予和回收其他主体对客体资源的访问权限。权限可传递，管理较为松散，所提供的安全防护相对比较低，无法适用于更高安全要求的 HarmonyOS 设备。

轻量化可信执行环境

轻量化设备同样可能存在安全业务及数据的保护需求，而受限于硬件资源规格，这类设备可能无法部署常规的可信执行环境。

轻量化的 HarmonyOS 设备可另辟蹊径，采用资源开销较少的轻量化可信执行环境，用于部署少量的安全业务，如密钥管理、安全连接等。下图为典型的 HarmonyOS 轻量化可信执行环境：基于 RISC-V/Cortex-M 等低端处理器实现，利用核间隔离机制，选取设备的某个物理核部署可信执行环境。

图5-4 轻量化可信执行环境



ARM 在 Cortex A 处理器的 Trustzone 技术大获成功后，于 ARM 的低端处理器 Cortex M33 上推出了 TrustZone-M 技术，用于物联网类设备。基于 TrustZone-M 构建的可信执行环境，同样适用上图的架构，也被视为轻量化的可信执行环境。

5.4 系统安全等级 SL3

地址空间随机化

在早期的栈溢出漏洞利用中，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。SL3 的 HarmonyOS 设备，要求支持核心保护对象的随机化，包括栈、共享库、mmap、VDSO 等。

更高安全等级的 HarmonyOS 设备，还需要支持更为完整的地址空间随机化，包括代码、堆等。

值得注意的是，32 位设备的随机熵过低，地址空间随机化的价值较低；随机化技术在 64 位环境下方能发挥更高的价值。

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 设备的推荐做法。

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。

硬件加解密引擎

现代处理器中集成了部分密码学指令，如哈希和对称算法指令，这类指令借助处理器的高性能，往往可发挥出较高的运算性能；而专用密码学计算电路则指各类 SOC 中的加解密引擎单元。相比软件基于处理器专用指令实现的密码算法，这类引擎在能效比和安全上优势明显，且支持更多的算法类型。

SL3 安全等级的 HarmonyOS 设备应提供硬件加密引擎，用于数据加解密及密钥派生等操作。在具备硬件加解密引擎的 HarmonyOS 设备上，硬件加解密加速引擎支持的主要算法参考如下：

- 对称算法：如 AES-128、AES-256、SM4 等
- 哈希算法：如 SHA256、HMAC-SHA256、SM3 等
- 公钥算法：如 RSA2048、ECDSA-P256、ECDH-P256、SM2 等

真随机数发生器

设备应支持随机数的生成，用于密钥、IV、盐值生成。应采用密码学意义上的安全随机数，保证不可预测性。

HarmonyOS 设备提供符合 NIST SP800-90A 标准的 CTR_DRBG 随机数发生器，及满足 NIST SP800-90B 标准要求的硬件熵源。

5.5 系统安全等级 SL4

设备刷机及改制行为管控

通过刷入特权软件版本，从而额外获得更多权限并危害设备安全是攻击者及黑灰产常用的手段。HarmonyOS 支持设备刷机及改制行为管控。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一律切换到商用签名，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，方允许。

可信执行环境

SL4 安全等级的 HarmonyOS 设备支持可信执行环境技术，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（-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 提供可信显示与输入能力 **TUI**，提供了无法截屏的 TUI 显示技术来保护可信应用显示的内容，采用与外部隔离的显示。当显示时完全阻止 REE 侧对该显示区域的访问，可防止恶意应用对于显示和输入的劫持和篡改。确保恶意程序既看不到显示屏上的信息，也无法访问触摸屏。TUI 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汉 字、英文字母、符号和数字，支持定制界面，输入键盘按键随机化支持丰富的控件支持、窗口管理，界面使用终端的 UI 风格

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。

文件系统分级加密

SL4 安全等级的 HarmonyOS 应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，HarmonyOS 提供了以下几种不同的方案：与设备锁屏密码配合的数据加密方案（CE/SECE/ECE）和与设备锁屏密码无关的加密方案（DE），默认采用前者数据保护方案。此类方案中加密数据的类密钥（Class Keys）与锁屏密码相关，被用户锁屏密码和设备唯一密钥共同保护。

详细内容可参考数据安全章节。

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。尽管 CFI 无法阻止攻击者利用已知漏洞，甚至改写函数指针， 但它可严格限制可被有效调用的目标范围，这使得攻击者在实践中利用漏洞变 得更加困难。

HarmonyOS 采用 Clang CFI 及栈保护技术以缓解 ROP/JOP 攻击威胁内核。

强制访问控制

HarmonyOS 支持强制访问控制特性，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 root 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。

HarmonyOS 同时也支持 seccomp 特性，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。

内核完整性保护*

虽然 Secure Boot 和 Verified Boot 确保了启动时软件的合法性及完整性，但合法代码中仍然可能存在漏洞会被攻击者利用。

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。

5.6 系统安全等级 SL5

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。

此功能依赖产品部署特定的安全芯片。

形式化验证 + 微内核

HarmonyOS 的可信执行环境的内核采用了微内核架构，通过简化内核功能，模块化设计，将系统服务更多地在内核之外实现，微内核只提供最基础的服务，系统服务更多的在用户态，通过按需扩展，提升性能降低攻击面，通过加强细颗粒度权限设计，使得 HarmonyOS 可信执行环境具备如下优势：良好的扩展性，通过构筑分布式设备统一的安全内核，能承载更多异构设备各种业务的能力诉求，如多核支持、按需并发、大小核调度等。易于实现与调试，通过提供稳定的底层库接口，降低应用开发移植难度，支撑安全业务生态发展。

此外，HarmonyOS 可信执行环境首次实践了形式化方法，通过形式化方法显著提升可信执行环境内核及关键模块的安全等级，重塑可信安全。形式化方法是使用数学定理证明的方式从源头验证系统正确，无漏洞的有效手段，传统验证方法如功能验证，模拟攻击等只能在选择的有限场景进行验证，而形式化方法可通过数据模型验证所有软件运行路径，通过验证核心模块，验证核心 API 及进程隔离，权限管理等高层机制的正确性，保证无数据竞争、无内存访问错误等。

通过采用形式化方法，HarmonyOS 的可信执行环境的微内核通过了高等级安全认证 CC EAL5+，未来可进一步挑战更高安全目标。

防物理攻击

SL5 安全等级的 HarmonyOS 设备，其核心安全模块需具备防物理攻击的能力，物理攻击主要包括侧信道攻击和故障注入。核心安全模块主要包括独立安全芯片（含安全元件）、硬件加解密引擎、熔丝存储等。

独立安全芯片采用数字传感器和主动屏蔽层技术防御故障注入和物理攻击。数字传感器电路在检测到故障注入时，会发出告警让系统做出相应防护措施。主动屏蔽层覆盖在独立安全芯片的关键电路上，当芯片遭受物理攻击时，触发主动屏蔽层告警，攻击者难以绕过主动屏蔽层窃取关键电路上的敏感信息。

公钥密码引擎需具备高级侧信道防护能力以及故障注入防护能力。安全防护措施主要体现在算法调度设计上， ECC 点乘 针对常见的 SPA 和 DPA、Zero Point 等攻击方

法，主要通过引入随机数密钥加掩、坐标随机化、随机加掩、计算过程中间值加掩、关键参数校验、椭圆曲线在线校验等安全设计，以削减物理攻击风险；RSA 模幂则引入每 bit 密钥多次模乘、运算中间值加掩、随机插入伪密钥、防地址监测、输入参数 CRC 校验等安全设计，来抵御物理攻击风险。

对称算法引擎同样需具备高级侧信道防护能力以及故障注入防护能力。其关键点在于：全路径均衡掩码防护算法、高安全 Sbox 掩码防护设计、关键中间值 CRC 完整性保护、时间冗余防故障注入逻辑比较运算

eFUSE：eFUSE 用于系统的敏感信息如根密钥，需要进行机密性保护和完整性保护。其敏感数据会带有 CRC 校验值，用于防护故障注入攻击；在 eFUSE 关键区域需要部署数字传感器，增强故障注入防护攻击能力。eFUSE 的自身鲁棒性同样需要增强，如部分关键控制 reg 做备份和冗余设计。

5.7 设备分布式可信互联

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帐号设备之间的可信关系，以及点对点绑定的设备可信关系。

同一华为帐号的设备连接安全

为保护登录同一华为帐号设备的安全连接，提供基于同帐号的设备认证能力。设备在登录帐号后，将会在端侧生成椭圆曲线公私钥对，作为本机在该帐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。

当同帐号的设备在近场被软总线发现并进行同帐号组网时，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，确保只有同帐号的设备能解密。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帐号的场景，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 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。

当点对点绑定的设备在近场被软总线发现并连接时，设备认证服务将基于可信关系建立时双方交换存储的对端公钥身份认证凭据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与同帐号类似的方式对通道上传输的数据进行端端加密保护，确保只有点对点绑定的设备才能解密。

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 数据分级规范

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，如华为帐号、社交帐号等
	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

数据隐私分类	数据类型	数据分级	举例
	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

6.2 数据安全与用户隐私生命周期管理概览

HarmonyOS 参照数据的风险分级，提供了基于全生命周期的数据保护能力。根据数据在智能终端设备上的处理的过程，数据生命周期包括生成（Create）、存储（At Rest）、使用（In Use）、传输（Transmit）、销毁（Destroy）这几个阶段：

生成：智能终端和其上的应用软件通过采集、直接生成、从其它终端接收或其它方式转入等方式产生数据的过程。

存储：数据在智能终端设备上存留的过程。

使用：数据在智能终端设备上被访问、处理等操作的过程。

传输：数据离开源设备、转移到目的设备的过程。销毁：数据在智能终端设备上被销毁，保证其不可被检索、访问的状态。

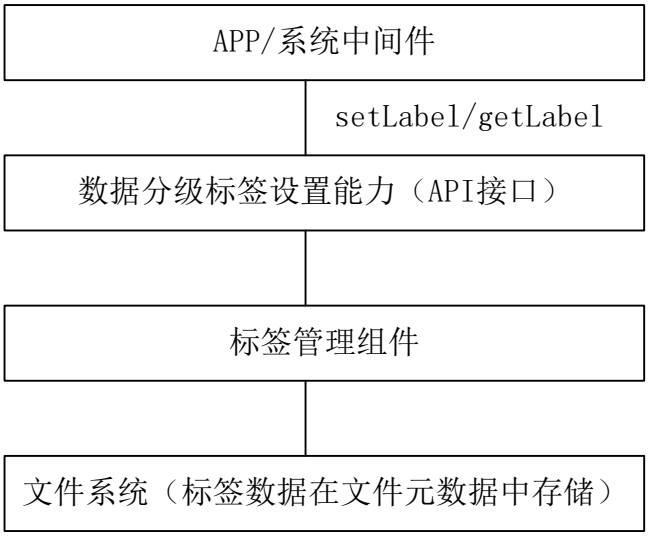
6.3 数据生成（Create）的安全机制

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；

HarmonyOS 设置风险等级标签的 API 如下：

API 接口	API 功能
public int setLabel(Context context, String filePath, String labelName, String labelValue, int flag)	该接口用于为文件设置风险等级和相应的保护策略。 其中的 labelValue 用于说明设置的是风险等级标签，labelValue 用于说明风险等级，设置的范围从 S0 到 S5；
public String getLabel(Context context, String filePath, String labelName)	该接口用于获取文件的风险等级；
public int getFlag(Context context, String filePath, String labelName)	该接口用于获取文件风险等级的辅助信息；

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

6.4 数据存储（At Rest）的安全机制

数据存储阶段，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。

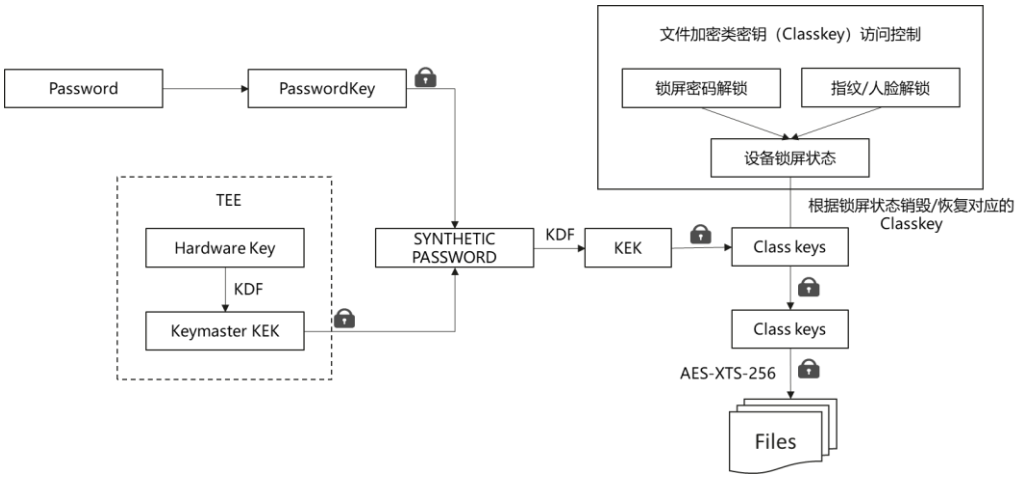
基于不同的数据风险等级，HarmonyOS 提供了以下几种方案（以手机系统为例）：

- 与设备锁屏密码配合的数据加密方案（CE/SECE/ECE）：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：

- 凭据加密方案（CE）：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，如图库、联系人、短信、日历、通话记录，重新锁定屏幕后数据仍然可以被访问。
- 增强型加密方案（SECE）：在 CE 方案基础上增强。在设备锁定时，受 SECE 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。
- 全面加密方案（ECE）：在 SECE 方案上进一步增强。在设备锁定时，受 ECE 方案保护的文件不能打开或者新建，直至用户解锁设备。

- 与设备锁屏密码无关的加密方案（DE）：DE 类保护方案中数据是否可访问与设备锁定状态无关，受 DE 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。
- 完全不加密的方案（NE）：数据完全不加密，这种情况极少，比如 OTA 升级包。

图6-1 文件加密层级



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；

HarmonyOS 基于数据的风险等级，对数据提供了不同等级的保护能力：

对于严重级别（S4）数据，HarmonyOS 最高可以提供 ECE 的文件保护能力；

对于高风险级别（S3）数据，HarmonyOS 最高可以提供 SECE 的文件保护能力；

对于中风险级别（S2）以及低风险级别（S1）数据，HarmonyOS 最高可以提供 CE/DE 的文件保护能力；

6.5 数据使用（In Use）的安全机制

数据使用阶段，HarmonyOS 提供了自主访问控制（本地文件系统沙盒）以及强制访问控制能力，确保只有正确的应用才能够访问对应的数据；

HarmonyOS 分布式文件系统提供了分布式沙盒的能力，保证跨设备的数据访问也遵循只有正确的应用才能够访问对应数据的原则；

HarmonyOS 通过对文件加密密钥的管控，提供了 ECE（全面加密方案）/SECE（增强型加密方案）文件保护增强能力，用于高风险等级数据在使用过程中的访问控制增强处理，确保有设备访问权限（能够解锁设备）的用户才能够使用这些高风险数据；

HarmonyOS 通过对文件加密类密钥（Class Keys）采用不同的保护方式，不同的数据加密方案（DE/CE/SECE/ECE）提供了不同的文件保护能力；

数据加密方案	ClassKey 的生命周期	文件保护模式
设备加密 方案（DE）	设备开机之后对应的 ClassKey 可用	设备开机之后，对应的文件可以使用
凭据加密方案（CE）	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 可用	设备开机，同时用户输入正确的锁屏密码解锁设备之后，对应的文件可以使用
增强型加密方案（SECE）	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 可用； 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 Claakey； 设备被用户再次解锁之后，对应的 Classkey 在系统中恢复；	在设备锁定时，受 SECE 方案保护的文件不能打开，但可以新建和写入文件

数据加密方案	ClassKey 的生命周期	文件保护模式
全面加密方案（ECE）	设备正常使用，并且解锁了设备之后对应的 ClassKey 可用； 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；	在设备锁定时，受 ECE 方案保护的文件不能被打开或者新建，直至用户解锁设备。

6.6 数据传输（Transit）的安全机制

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。

6.7 数据销毁（Destroy）的安全机制

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。

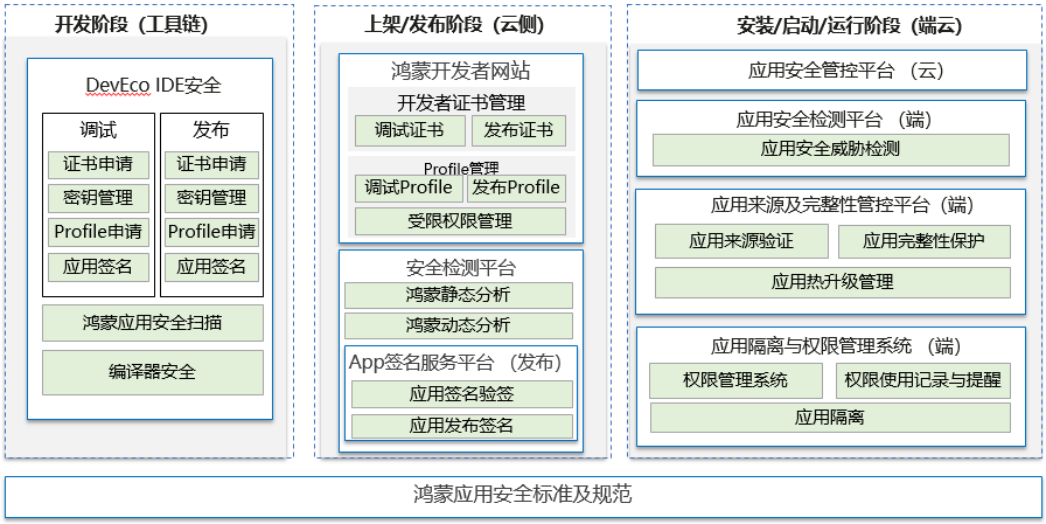
HarmonyOS 的恢复出厂设置，支持对存储数据的安全擦除。通过给物理存储器发送命令，进行覆写操作，完成底层数据擦除。擦除后数据是全 0 或者全 1，确保用户的敏感数据不能通过软硬件手段恢复，能够保护用户设备转售、废弃后的数据安全。

7 HarmonyOS 生态治理架构

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，来确保运行在超级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。

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。

7.2 HarmonyOS 应用程序“纯净”开发

对于 HarmonyOS 开发者，提供开发者注册、帐号管理、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密钥的生成和管理，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 开发者需要注册帐号，注册帐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。

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 同时支持对于 Android 应用的兼容运行，对于来自华为应用市场的 Android 应用本身会经过严格的检测和人工审核保持纯净， 对来自第三渠道未经过华为检测和人工审核的应用， 华为构建了纯净模式进行安全认证确认是否是用户清楚风险，由于三方渠道存在风险不可控，用户使用时基于风险判断，谨慎安装非官方来源的应用。

HarmonyOS 为应用程序全新设计了安全与隐私保护机制：

- 纯净来源：鸿蒙应用只能来自于华为应用市场，对于 Android 应用通过纯净模式管控安装方式，包括对安卓应用的非应用市场的管控机制，安装时需认证用户的身份，在纯净模式增强模式打开时，则禁止三方来源的管控。HarmonyOS 系统鸿蒙应用禁止热更新。
- 存储沙箱：取消了存储访问权限，保护了 APP 的数据安全。
- 纯净运行：对违规/恶意/病毒风险应用进行数据隔离和行为隔离处置，用户也可自主对应用进行数据和行为隔离，隔离后的应用无法获取用户敏感数据（电话本、短信、通话记录、日历），同时也无法获取后台弹窗、悬浮窗、位置信息、媒体和文件的权限。
- 纯净权限：HarmonyOS 系统鸿蒙应用取消了短信、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。

  安全中心：集中展示终端的安全状态、风险画像，建立一个闭环的问题解决方案，为用户提供安全可靠的设备环境，让用户放心使用各种业务。

7.5 HarmonyOS 应用程序“隐私”可控

隐私是用户的基本权利，用户对自己的隐私拥有完整的控制权，隐私保护是产品设计的基石，和业务体验相辅相成。

系统提供的隐私保护两个基本原则：

- **透明可知：**对应用的隐私行为，用于都清晰可见，并可根据自己的意愿进行下一步决策，充分掌控自己的隐私。
- **用户可控：**应用从系统获取用户隐私相关的信息，为用户提供更好的服务，必须经过用户确认。

基于上述原则，HarmonyOS 为保护消费者的隐私，防止应用过度获取相关隐私数据，提供权限生命周期的保护机制，主要包括：

- 针对应用使用隐私数据的权限管理机制；
- 针对位置信息、相机、麦克风、存储、通讯录实现的隐私指示器，用于在使用过

程中的用户提醒

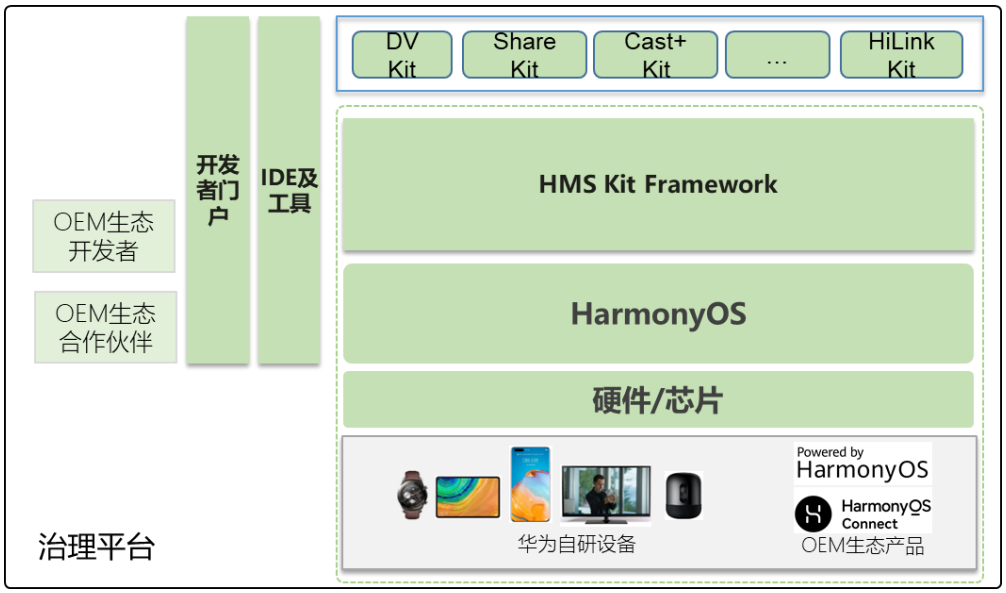
- 针对应用使用后的应用行为记录，可以让用户清晰的查看应用的行为。
- 针对可能存在的不合理使用情况，系统提供了隐私保护建议，让用户可以根据建议调整应用的隐私相关设置。

7.6 HarmonyOS 设备生态治理架构概述

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7-2 HarmonyOS 设备生态治理平台



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

7.7 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，需要对厂商能够溯源，并且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帐号，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。

7.8 HarmonyOS 生态设备安全认证

合作伙伴在开发完成设备后， 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。

7.9 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）。

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。

在 HarmonyOS 2 版本上，我们已获得：

认证名称	认证对象	颁发机构	说明
CC EAL 5+	TEE 安全操作系统微内核	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。TEE 安全操作系统微内核获得 CC EAL5+认证。
CC EAL2+	iTrustee 5.0 可信执行环境	荷兰 NSCIB	华为可信执行环境的安全操作系统 iTrusttee5.0 获得 CC EAL2+认证。
IT 产品信息安全认证 EAL4+	HarmonyOS 2	中国网络安全审查技术与认证中心	该认证基于《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，该标准以等同采用国际 CC 标准的国标 GB/T 18336 为基础框架，依据 CC 评估方法对 HarmonyOS 2 进行全方位评估。获得 该认证意味着 HarmonyOS 2 得到全方位评估和验证，能够更好地保护消费者的数据安全。

ISO/IEC 27701	华为终端有限公司华为终端软件	英国标准协会	ISO/IEC 27701 隐私信息管理体系从组织治理、法律合规、流程规范、信息技术、监督审计等多个维度，提供了一套完整的个人数据处理方法和隐私信息管理的框架。该认证意味着华为终端软件在持续优化设计、研发、运营和运维服务等环节，已经拥有完备的个人信息保护管理体系。

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 HUAWEI Pay、手机盾、手机交通卡、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。

9.1 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帐户和设备的其他信息，发送给发卡机构。发卡机构将使用此信息，决定是否批准将付款卡添加到 Huawei Pay。

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

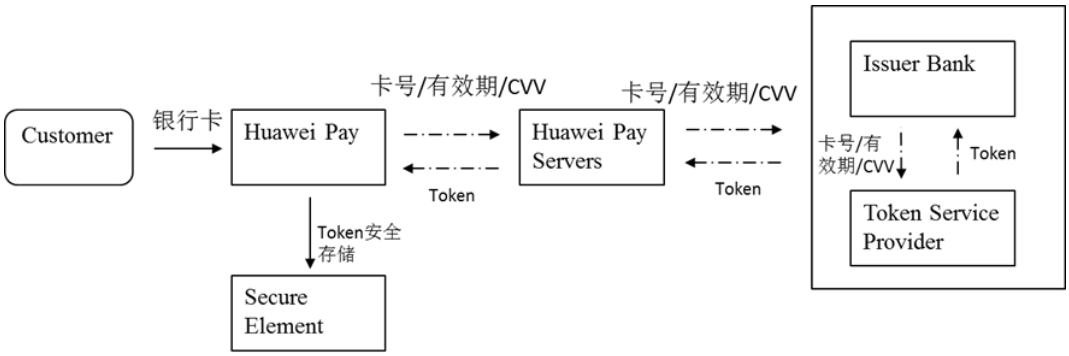
“绑定”流程会执行以下两项操作：

- 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，确保帐号华为帐号和银行卡属于同一用户所有。

图9-1 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。

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

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 通过了国际 PCI-DSS 认证；并通过了 VISA PCI-CP、CDCVM 安全认证；符合支付行业权威安全标准要求。

9.2 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 app 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 app 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 app 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。

9.3 手机盾

二代 U 盾（USB 盾，音频盾等）是目前银行主要的网络交易安全解决方案，但由于使用的是额外安全硬件，存在不便于携带、易损坏、易丢失、使用率低、用户体验不佳的缺点。而具有移动支付类功能的 APP，在使用银行支付通道进行交易时，安全策略主要采用绑定手机号，以短信方式进行交易确认，安全风险高，用户在支付过程中总担心资金会被窃取。华为手机盾结合内部独立的安全元件（Secure Element），安全

元件是业内公认、经过认证的芯片，支持银行的手机证书业务，将传统的 USB 插拔式 U 盾与手机结合，变为随身携带的手机盾，为电子支付提供金融级的硬件保护。

在用户开通手机盾时，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。随后银行 APP 将在该安全空间生成独立的公私密钥对和证书，同时要求用户在可信 UI 界面输入用户识别 PIN 码来保护生成的密钥数据。

用户在使用手机盾时，首先通过可信 UI 界面认证用户的身份，随后安全单元会使用开通过程中生成的私钥对用户的交易请求进行签名。银行在处理该交易请求时，会对此交易进行验签。

用户在注销（关闭）手机盾时，系统会直接销毁安全元件中存储的公私钥密钥对，且不可恢复。

从证书公私钥产生到证书销毁，整个生命周期内，证书私钥将始终位于安全元件内，保障证书密钥安全不外泄。

手机盾应用浏览

对应用进行包名、签名检查，必须为官方版本才会出现在管理界面，防止恶意应用仿冒。通过华为钱包 APK 浏览界面及管理入口，一键查询及管理手机上安装的手机盾类应用。

手机盾开关

为了避免后台程序及应用恶意调用银行证书，在系统中提供开关设置，开关效果类比于传统 USB 盾插拔动作，关闭开关后，所有与证书相关的业务都无法进行，为用户提供真正可掌控的硬件安全体验。

9.4 电子身份证

网络电子身份标识 eID 是华为和公安三所联合开发的身份证应用，电子身份证在公安部门认可的场合可以承担与物理身份证相同的功能，能够在不泄露用户明文身份证信息的情况下，使用公安部门提供的加密信息完成在线身份认证，还能在刷卡终端的配合下实现刷手机乘车等功能，另外还提供认证接口给其他第三方手机应用，用于快捷可信的身份认证。

用户在手机钱包应用提供的入口中即可完成 eID 的开通，开通过程中，用户使用手机 NFC 读取物理身份证，并录入人脸信息，在手机端经过活体检测后，将人脸图像加密后上传至公安服务器，公安服务器校验完成后，下发 eID 信息至手机。在此过程中，

人脸图像的采集、加密均在 iTrustee®安全 OS 中完成，确保了数据的安全性。eID 开通后，公安服务器下发的 eID 信息保存在独立安全芯片 inSE 中，只有特定程序才能访问。而在开通过程中使用的中间数据，如人脸图像等在开通流程结束后将删除，不会保存在手机中。

全过程华为遵循 eID 相关标准规范，提供 eID 在终端侧的全生命周期管理，为用户提供便捷安全的网络数字身份服务。华为 eID 方案基于华为安全芯片 InSE、安全 Camera、iTrustee®安全 OS，为开通、下载、使用和注销流程提供端到端的高安全保护。

9.5 车钥匙

手机车钥匙遵循国际车联网联盟(The Car Connectivity Consortium，简写为 CCC)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。

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，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

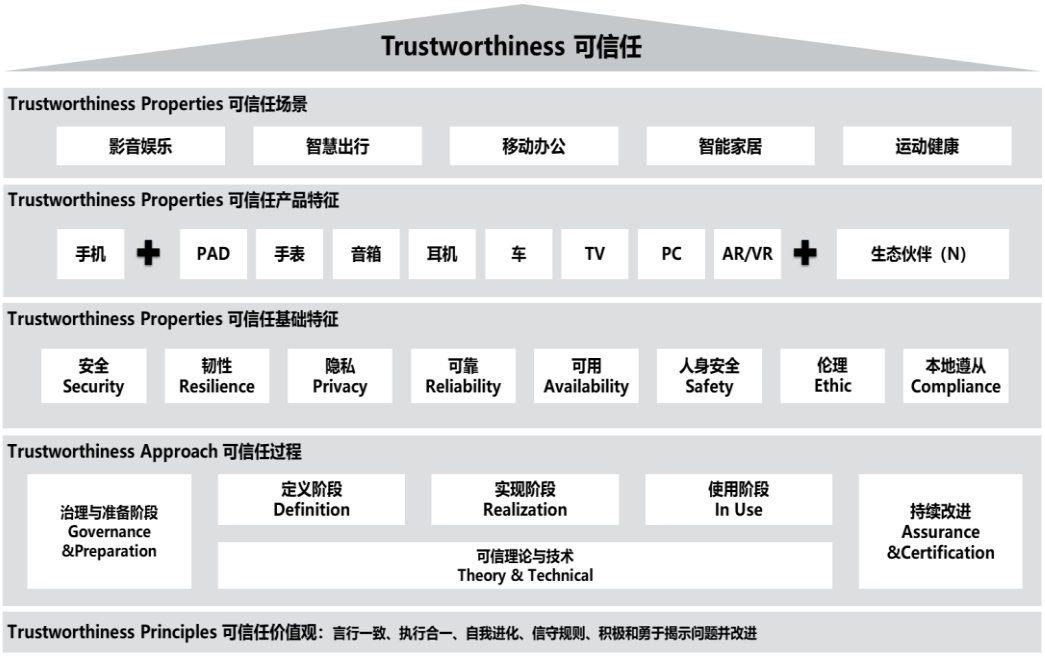
今天，人类社会正在迈向万物互联的智能世界，全场景、全连接、智慧化等发展趋势，对消费者产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买一个产品的基本条件。可信不仅仅是产品外在表现的结果，更是产品内在实现的过程，是结果和过程双重可信的高质量。

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 奇点安全实验室

由业界顶级安全研究员领衔的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，保障 HarmonyOS 产品和解决方案用户的隐私和安全：

1. 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
2. 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
3. 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 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 提供的基础安全能力，为上层业务应用程序以 API、Kit、SDK 形式向开发者能力开放。同时，为生态设备提供专业 CBB、安全模组、独立芯片等形式进行适配对接，详细请参考开发者网站：
https://developer.huawei.com/consumer/cn/doc/development/Security-Guides/sdk-version-0000001117302118

11.1 HarmonyOS 数据安全能力开放

HarmonyOS 作为系统底座为上层业务应用提供**安全可信、快速精准、轻便高效、覆盖广泛**的安全能力，围绕“生态应用程序的开发与使用”持续输出全流程、专业化的解决方案及系统服务。其中，**数据安全能力**作为 HarmonyOS 安全能力的重要组成部分，已广泛应用于各种场景并为应用提供了业务竞争力优势，数据安全能力包含“**短数据安全存储**”和“**文件分级保护**”，提供保护用户数据安全、安全可控地获取系统数据的能力。数据安全能力调用量持续增长，已在各类银行、理财、支付等涉及大量数据安全隐私保护的应用中发挥势能。

短数据安全存储：

关键短数据（Asset）存储提供安全处理短小的敏感数据的能力，包括安全存储、删除、更新、查询短敏感数据的能力，可覆盖多种存储及管理短敏感数据的场景；

应用中通常有一些短小的敏感数据非常重要，如用户名密码、信用卡信息、App Token 等。它们的长度在 64 字节以内，安全要求很高。

能力特点：

1. 安全：密钥存储在 TEE 安全世界（密钥安全），最优加解密算法（算法安全），数据加密存储（数据安全）等。

2. 便捷：可覆盖多种存储及管理短敏感数据的场景。使用该能力，可以大大节省安全性开发的时间，包括对加解密算法的选择及密钥管理的安全性保护等。

文件分级保护：

根据数据分级，制定数据全生命周期安全的管控策略和保护要求，业务在使用场景中遵从并采用相应的安全保护措施。

文件分级保护为数据提供分级标签化的能力，支持文件 S4-S0 风险等级的设置和读取。数据风险等级及对应的定义见下表：

风险等级	风险标签	定义	样例
严重	S4	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	健康状况、个人的信用卡等信息
高	S3	数据的泄露可能会给个人或组织导致严峻的不利影响	个人实时精确定位信息、运动轨迹等
中	S2	数据的泄露可能会给个人或组织导致严重的不利影响	个人详细通信地址、姓名昵称等
低	S1	数据的泄露可能会给个人或组织导致有限的不利影响	国籍、出生地、教育程度等
公开（无风险）	S0	对个人或组织无不利影响的可公开数据	公开发布的产品介绍、公开的会议信息、外部开源的代码等

应用场景：文件分级可用于为数据设置风险等级，设置风险等级后，终端设备将数据按照对应等级的文件保护方案进行加密保护。并且开发者还可以在规则范围内，调整配套的保护手段。

能力特点：

1. 安全：为文件设置风险等级，可以根据文件风险等级分级提供配套的保护方案，为不同风险等级的数据提供对应的身份认证方案。
2. 便捷：使用能力可以节省安全性开发的时间，对文件进行分级标签化设置，提升数据安全。并且在手机上开发的应用，迁移到其他的设备上，无需因为底层安全能力的差异而额外做适配工作。

11.2 HarmonyOS 本地认证能力开放

HarmonyOS 提供本地认证能力，当前以**本地人脸识别能力**进行开放，本地人脸识别能力基于深度神经网络开发，结合 3D 结构光技术，提供安全、可靠的本地人脸认证能力，具有高精准度、高安全级别的人脸比对、活体检测等重要功能。

本地认证能力在金融理财、社交通信、影音娱乐、移动办公等应用程序中发挥积极作用，同时也不断赋能更多实用场景，让场景更加丰富、让使用更加安全，目前，已应用于支付宝、民生银行、工行等应用程序，在用户快速登录、认证等场景中拥有数以亿计的调用量，月活用户达数千万级别。

本地人脸识别能力使用前置摄像头获取人脸特征图像，并通过算法分析人脸特征，用于人脸比对。

场景介绍：人脸识别可用于登录、支付或其他需要人脸对比的场景。部分机型具有 3D 人脸识别能力，具有高安全性，可用于大额支付。

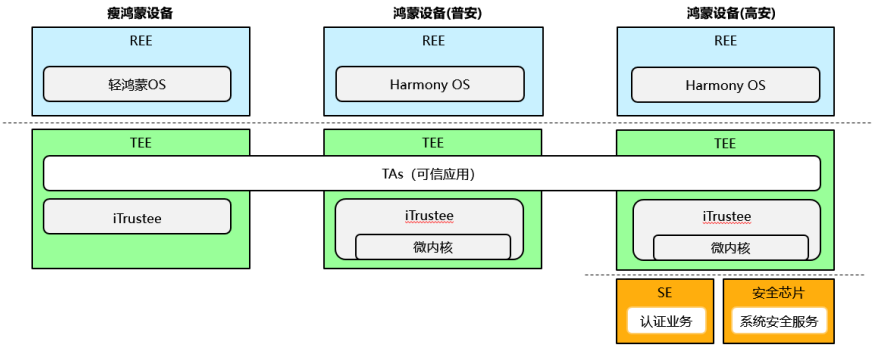
能力特点：

1. 快速：目前该算法基于深度神经网络开发，快速完成人脸比对。
2. 轻便：利用本能力可大大节省算法开发的时间，让您的应用更加轻便。
3. 广泛：可覆盖多种识别场景。

11.3 HarmonyOS 设备安全能力开放

“正确的设备”章节系统化地介绍了 HarmonyOS 构建了功能强大的**可信执行环境**（TEE），该能力为高安全业务提供了基础安全底座，在金融业务、本地生物识别、数字版权保护、数字认证等业务领域发挥着大的价值。

图11-1 HarmonyOS TEE 解决方案



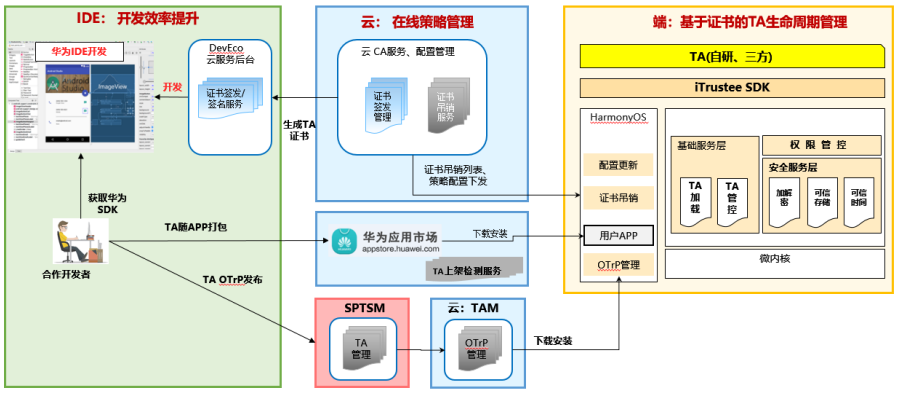
HarmonyOS 构建了支持多种形态的可信执行环境，覆盖各种芯片架构和产品形态，基于 HarmonyOS 可信执行环境开发的可信应用（TA），可跨多个产品部署，“一端开发、多端部署”。

为了方便基于 HarmonyOS 可信执行环境开发安全应用和业务，HarmonyOS 对生态伙伴开放可信执行环境能力。主要在两个层面开放：

- 通过 HarmonyOS 的 SecurityKit（REE 侧），提供基础的安全能力，应用可在 REE 侧直接使用相关安全能力（Asset，HUKS）。
- 开放可信应用的开发和部署，允许三方可信应用部署在 HarmonyOS 可信执行环境中，通过高安全能力支撑垂直行业安全业务场景。

针对第二类能力开放场景，HarmonyOS 提供了配套的 SDK/DDK 开发套件和可信应用 TA 的部署服务，HarmonyOS 的合作开发者可通过华为提供的开发套件和部署服务，实现可信应用在 HarmonyOS 设备的开发和部署，其逻辑如下图所示。

图11-2 HarmonyOS TEE 能力生态开放架构示意图



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	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

英文缩写	英文全称	中文全称
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
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

英文缩写	英文全称	中文全称
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
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
2021-05-15	初始版本