作者：疯壳

注：文档和视频中所有的图片及代码截图皆为示意图，具体以 HarmonyOS 官网发布内容为准。

1.1 系统定义

HarmonyOS 是一款“面向未来”的操作系统，一款面向全场景（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 创造性地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，能够支持手机、手表、平板、PC、智慧屏、AI 音箱、车机、耳机、AR/VR 眼镜等多种终端设备。

- 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，形成一个“超级虚拟终端”，可以实现不同的终端设备之间的极速连接、硬件互助、资源共享，匹配最合适的设备、提供最佳的场景体验。
- 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，降低了开发难度和成本。这能够让开发者聚焦上层业务逻辑、便捷开发应用程序，极大地提升了开发效率。
- 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。

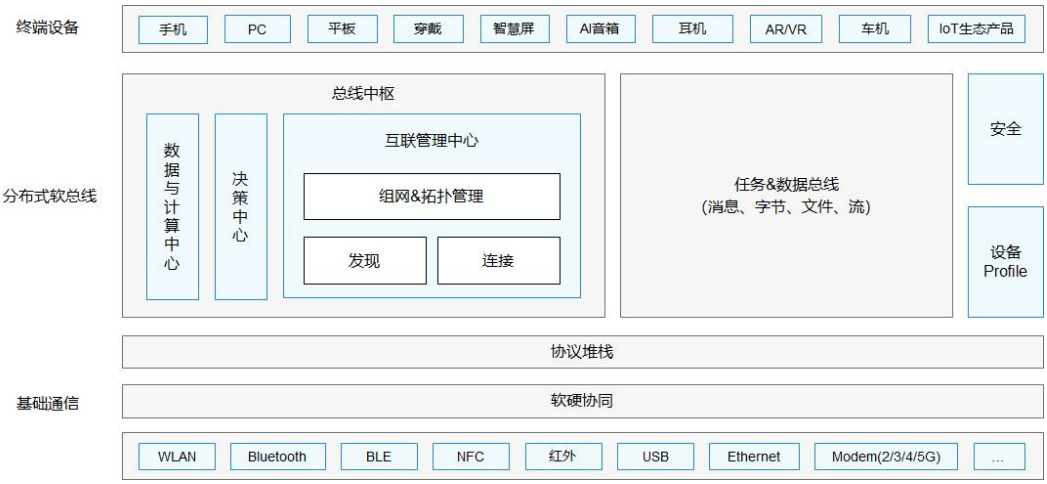
1.2 技术特性

特征 1：硬件互助，资源共享

分布式软总线

分布式软总线是手机、手表、平板、智慧屏、车机等多种终端设备的统一基座，为设备之间的无缝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，高效地传输任务和数据。分布式软总线示意图见图 1-1。

分布式软总线示意图

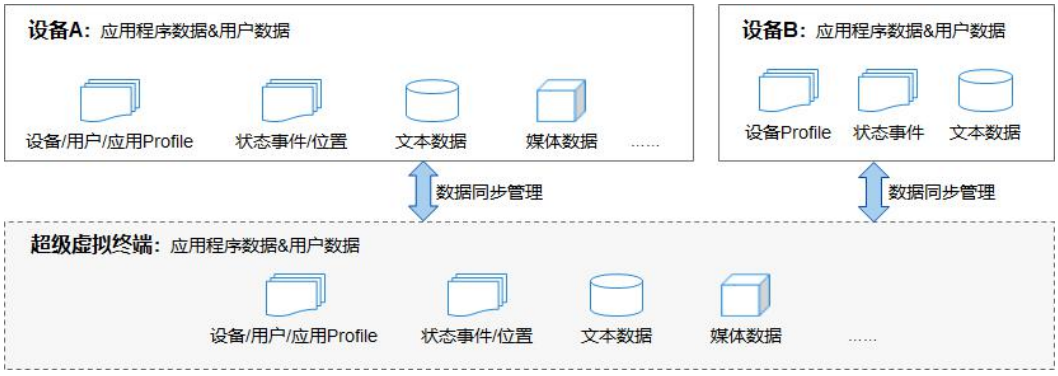


分布式数据管理

分布式数据管理基于分布式软总线的能力，实现了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 1-2。常见应用场景示例如下：

- 分布式数据流转（例如，手机访问其他设备的视频，并转移到智慧屏播放）。
- 分布式数据同步（例如，记事本内容实时跨设备更新）。

分布式数据管理示意图

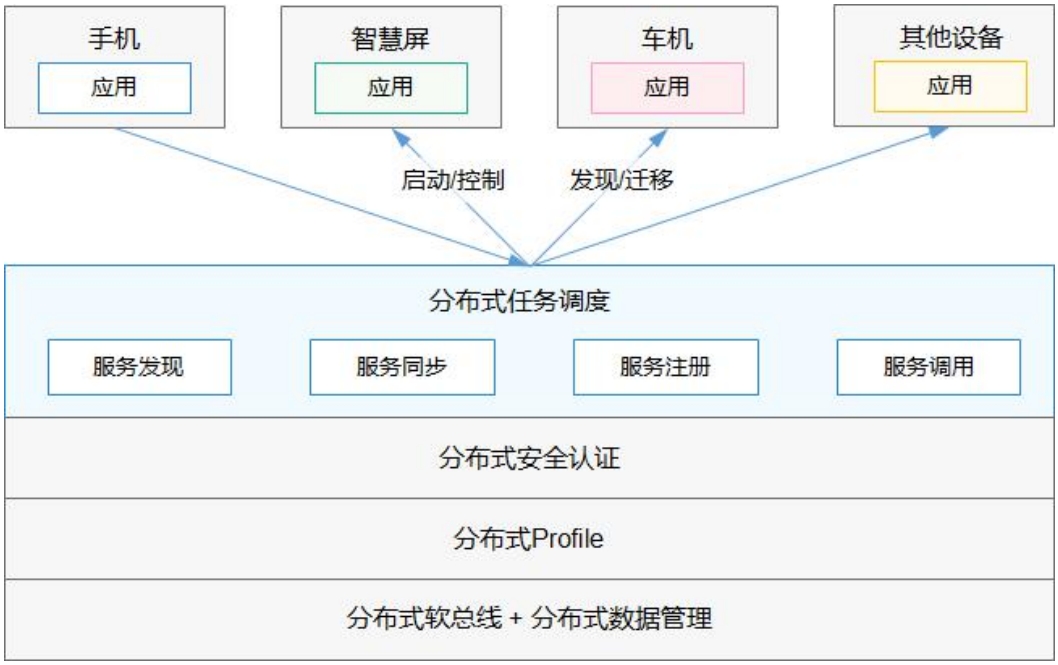


分布式任务调度

分布式任务调度基于分布式软总线、分布式数据管理、分布式 Profile 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、绑定/解绑、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、资源使用情况并结合用户的习惯和意图，选择最合适的设备运行分布式任务。分布式任务调度示意图见图 1-3。常见应用场景示例如下：

- 分布式业务迁移：功能跨设备无缝迁移，提供持续服务。例如，上车前，在手机上规划好导航路线；上车后，导航自动迁移到车载大屏和车机音箱；下车后，导航自动迁移回手机。

分布式任务调度示意图

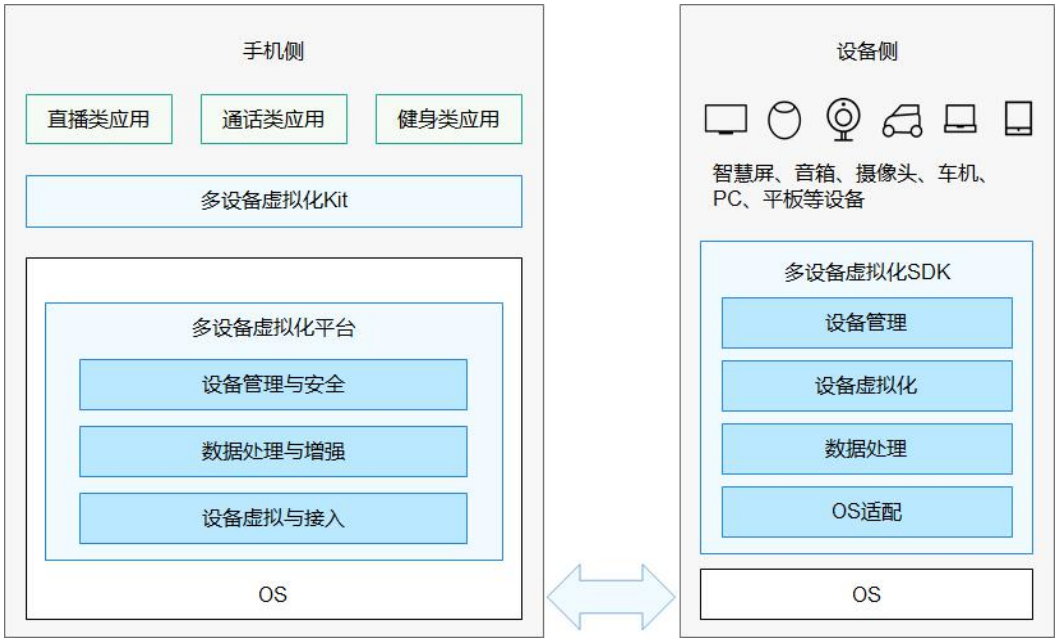


分布式设备虚拟化

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，将周边设备作为手机能力的延伸，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最佳的执行硬件，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 1-4。

应用场景举例：借助智慧屏、智能音箱、摄像头可以边做家务边视频通话，解放双手、随心会话。

分布式设备虚拟化示意图

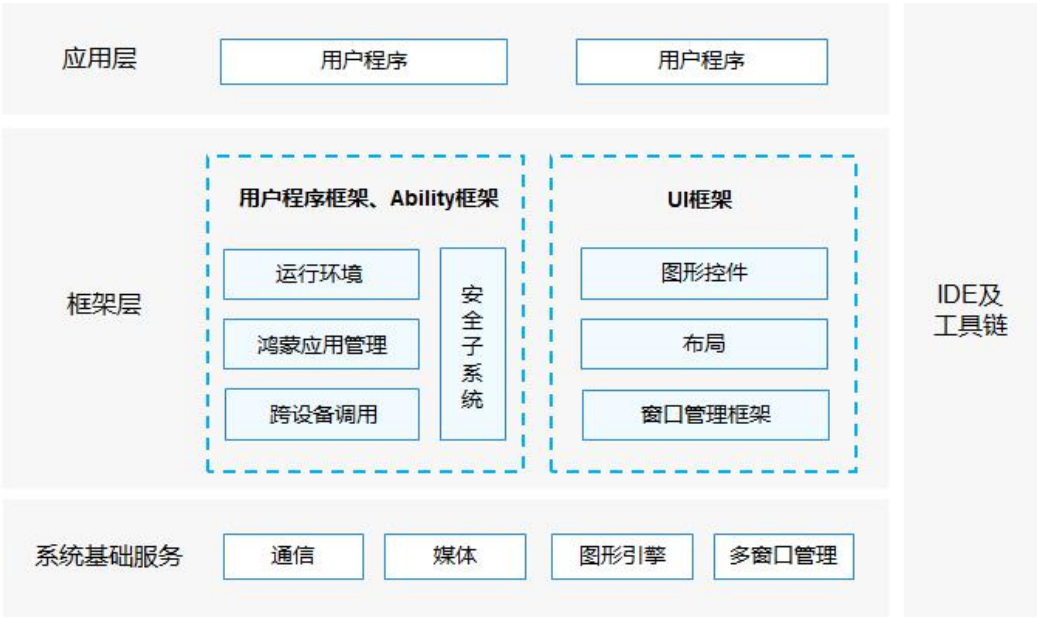


特征 2：一次开发，多端部署

HarmonyOS 提供用户程序框架、Ability 框架以及 UI 框架，能够保证开发的应用在多终端运行时保证一致性。一次开发、多端部署示意图见图 1-5。

- 多终端软件平台 API 具备一致性，确保用户程序的运行兼容性。
- 支持在开发过程中预览终端的能力适配情况（CPU/内存/外设/软件资源等）。
- 支持根据用户程序与软件平台的兼容性来调度用户程序。

一次开发、多端部署示意图



特征 3：统一 OS，弹性部署

HarmonyOS“硬件互助，资源共享”和“一次开发，多端部署”的系统能力为各种硬件开发提供了全栈的软件解决方案，并保持了上层接口的统一和分布式能力的统一。

HarmonyOS 通过组件化和小型化等设计方法，做到硬件资源的可大可小，在多种终端设备间，按需弹性部署，全面覆盖了 ARM、RISC-V、x86 等各种 CPU，从百 KB 到 GB 级别的 RAM。

1.3 技术架构

HarmonyOS 整体遵从分层设计，从下向上依次为：内核层、系统基础服务层、框架层和应用层。系统功能按照“系统 > 子系统 > 功能/模块”逐级展开，在多设备部署场景下可按子系统粒度裁剪，每个子系统内部又可按照功能粒度裁剪。HarmonyOS 技术架构如图 1-6 所示。

图 1-1 HarmonyOS 技术架构

架构图删除，待开源后获取新的 --reviewed by 张伟

内核层

HarmonyOS 采用多内核设计（Linux 内核、HarmonyOS 微内核或者 LiteOS），支持针对不同资源受限设备选用适合的 OS 内核。内核抽象层（KAL）通过屏蔽多内核差异，对上层提供基础的内核能力，包括进程/线程管理、内存管理、文件系统、网络管理和外设管理等。

系统基础服务层

系统基础服务层是 HarmonyOS 的核心能力集合，通过框架层对应用程序提供服务。该层包含以下几个部分：

- **系统基本能力子系统集**：为分布式应用在 HarmonyOS 多设备上的运行、调度、迁移等操作提供了基础能力，由分布式软总线、分布式数据管理&文件管理、分布式任务调度、方舟运行时、分布式安全和隐私保护等组成。其中，方舟运行时提供了 C/C++/JS 多语言运行时和基础的系统类库，也为使用方舟编译器静态化的 Java 程序（即应用程序或框架层中使用 Java 语言开发的部分）提供运行时。
- **基础软件服务子系统集**：为 HarmonyOS 提供公共的、通用的软件服务，由图形图像、分布式媒体、分布式 AI、多模输入、MSDP&DV、事件通知、电话服务、分布式 DFX 等子系统组成。
- **增强软件服务子系统集**：为 HarmonyOS 提供针对不同设备的、差异化的能力增强型软件服务，由平板业务软件、智慧屏业务软件、车机业务软件、IoT 业务软件等子系统组成。
- **HarmonyOS 驱动框架（HDF）&硬件抽象适配层（HAL）**：是 HarmonyOS 硬件生态开放的基础，向上对硬件服务提供硬件能力抽象，向下提供各种外设驱动的开发框架和运行环境。
- **硬件服务子系统集**：为 HarmonyOS 提供公共的、通用的硬件服务，由泛 Sensor、位置、电源、USB、生物识别等硬件服务子系统组成。
- **专有硬件服务子系统集**：为 HarmonyOS 提供针对不同设备的、差异化的硬件服务，由平板专有硬件服务、车机专有硬件服务、穿戴专有硬件服务、IoT 专有硬件服务等子系统组成。

根据不同设备形态的部署环境，基础软件服务、增强软件服务、硬件服务、专有硬件服务的子系统集内部可以按子系统粒度裁剪，每个子系统内部又可以按功能粒度裁剪。

框架层

框架层为 HarmonyOS 的应用程序提供了 Java/C/C++/JS 等多语言的用户程序框架和 Ability 框架，以及各种软硬件服务对外开放的多语言框架 API；同时为采用 HarmonyOS 的设备提供了 C/C++/JS 等多语言的框架 API，不同设备支持的 API 与系统的组件化裁剪程度相关。

应用层

应用层包括系统应用和第三方非系统应用。HarmonyOS 的应用由一个或多个 FA（Feature Ability）或 AA（Atomic Ability）组成。其中，FA 有 UI 界面，而 AA 无 UI 界面。FA/AA 均能够实现特定的业务功能，支持跨设备调度与分发，为消费者提供一致、高效的应用体验。

1.4 系统安全

在搭载 HarmonyOS 的分布式终端上，要保证“**正确的人，通过正确的设备，正确地使用数据**”。

- 通过“分布式多端协同身份认证”来保证“正确的人”。
- 通过“在分布式终端上构筑可信运行环境”来保证“正确的设备”。
- 通过“分布式数据在跨终端流动的过程中，对数据进行分类分级管理”来保证“正确地使用数据”。

正确的人

在分布式终端场景下，“正确的人”指通过身份认证的数据访问者和业务操作发起者。“正确的人”是确保用户数据不被非法访问、用户隐私不泄露的前提条件。HarmonyOS 通过以下三个方面来实现协同身份认证：

- **零信任模型**：HarmonyOS 基于零信任模型，实现对用户的认证和对数据的访问控制。当用户需要跨设备访问数据资源（例如，通过平板操作手机屏幕）或者发起高安全等级的业务操作（例如，对安防设备的操作）时，HarmonyOS 会对用户进行身份认证，确保其身份的可靠性。
- **多因素融合认证**：HarmonyOS 通过用户身份管理，将不同设备上标识同一用户的认证凭据关联起来，用于标识一个用户，来提高认证的准确度。
- **协同互助认证**：HarmonyOS 通过将硬件和认证能力解耦（即信息采集和认证可以在不同的设备上完成），来实现不同设备的资源池化、以及能力的互助与共享，让高安全等级的设备协助低安全等级的设备完成用户身份认证。

正确的设备

在分布式终端场景下，只有保证用户使用的设备是安全可靠的，才能保证用户数据在虚拟终端上得到有效保护，避免用户隐私泄露。

- **安全启动**

确保源头每个虚拟设备运行的系统固件和应用程序是完整的、未经篡改的。通过安全启动，各个设备厂商的镜像包就不易被非法替换为恶意程序，从而保护用户的数据和隐私安全。

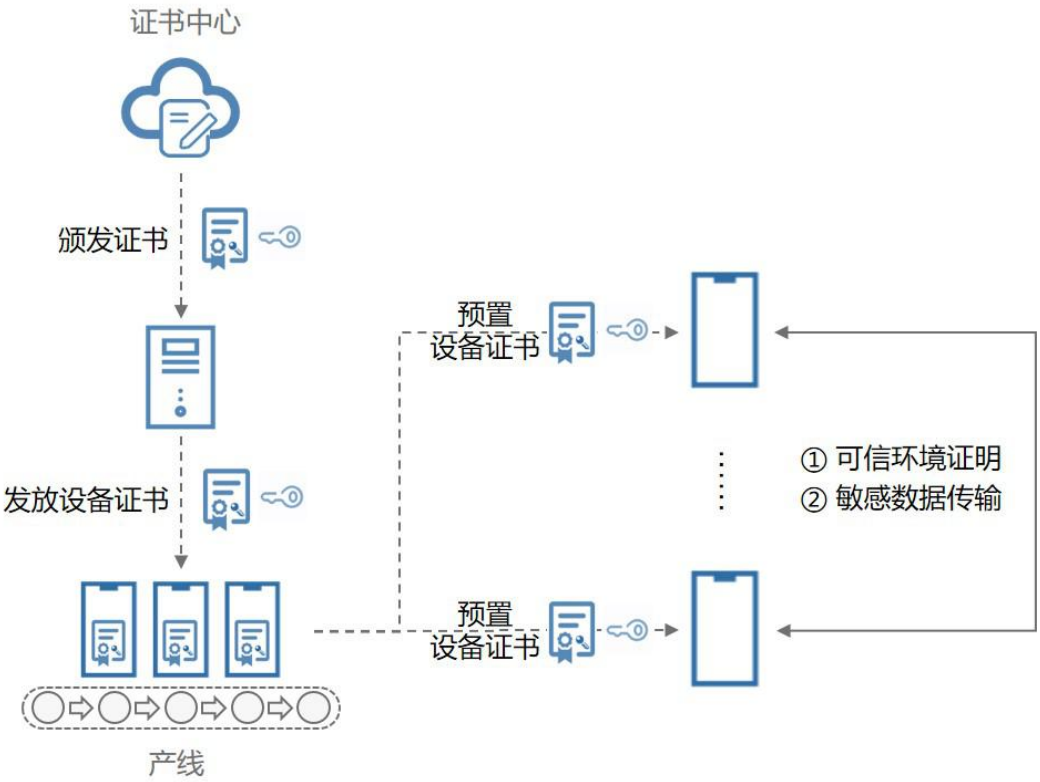
- **可信执行环境**

  提供了基于硬件的可信执行环境（TEE）来保护用户的敏感个人数据的存储和处理，确保数据不泄露。由于分布式终端硬件的安全能力不同，对于用户的敏感个人数据，需要使用高安全等级的设备进行存储和处理。HarmonyOS 使用基于数学可证明的形式化开发和验证的 TEE 微内核，获得了商用 OS 内核最高安全等级 CC EAL5+的认证评级。

- **设备证书认证**

  支持为具备可信执行环境的设备预置设备证书，用于向其他虚拟终端证明自己的安全能力。对于有 TEE 环境的设备，通过预置 PKI（Public Key Infrastructure）设备证书给设备身份提供证明，确保设备是合法制造生产的。设备证书在产线进行预置，设备证书的私钥写入并安全保存在设备的 TEE 环境中，且只在 TEE 内进行使用。在必须传输用户的敏感数据（例如密钥、加密的生物特征等信息）时，会在使用设备证书进行安全环境验证后，建立从一个设备的 TEE 到另一设备的 TEE 之间的安全通道，实现安全传输。如图 1-7 所示。

图 1-2 设备证书使用示意图



正确地使用数据

在分布式终端场景下，需要确保用户能够正确地使用数据。HarmonyOS 围绕数据的生成、存储、使用、传输以及销毁过程进行全生命周期的保护，从而保证个人数据与隐私、以及系统的机密数据（如密钥）不泄漏。

- **数据生成：**根据各国的法律法规和标准，对数据进行分类分级，并且根据分类设置相应的保护等级。每个保护等级的数据从生成开始，在其存储、使用、传输的整个生命周期都需要根据对应的安全策略提供不同强度的安全防护。虚拟超级终端的访问控制系统支持依据标签的访问控制策略，保证数据只能在可以提供足够安全防护的虚拟终端之间存储、传输和使用。
- **数据存储：**HarmonyOS 通过区分文件的安全等级，存储到不同分区，对文件进行安全保护，并提供密钥全生命周期的跨设备无缝流动和跨设备密钥访问控制能力，支撑分布式身份认证协同、分布式数据共享等业务。
- **数据使用：**HarmonyOS 通过硬件为设备提供可信执行环境。用户的个人敏感数据仅在分布式虚拟终端的可信执行环境中进行使用，确保用户数据的安全和隐私不泄露。
- **数据传输：**为了保证数据在虚拟超级终端之间安全流转，需要各设备是正确可信的，建立了信任关系（通过华为帐号或与手机、平板等设备建立配对关系），并能够在验证信任关系后，建立安全的连接通道，按照数据流动的规则，安全的传输数据。当设备之间进行通信时，需要基于设备的身份凭据对设备进行身份认证，并在此基础上，建立安全的加密传输通道。
- **数据销毁：**销毁密钥即销毁数据。数据在虚拟终端的存储，都建立在密钥的基础上。当销毁数据时，只需要销毁对应的密钥即完成了数据的销毁