系统安全

在搭载 HarmonyOS 的分布式终端上，可以保证“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

资料来源： HarmonyOS 官网
https://developer.harmonyos.com/cn/docs/documentation/doc-guides/harmonyos-security-0000000000011934

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

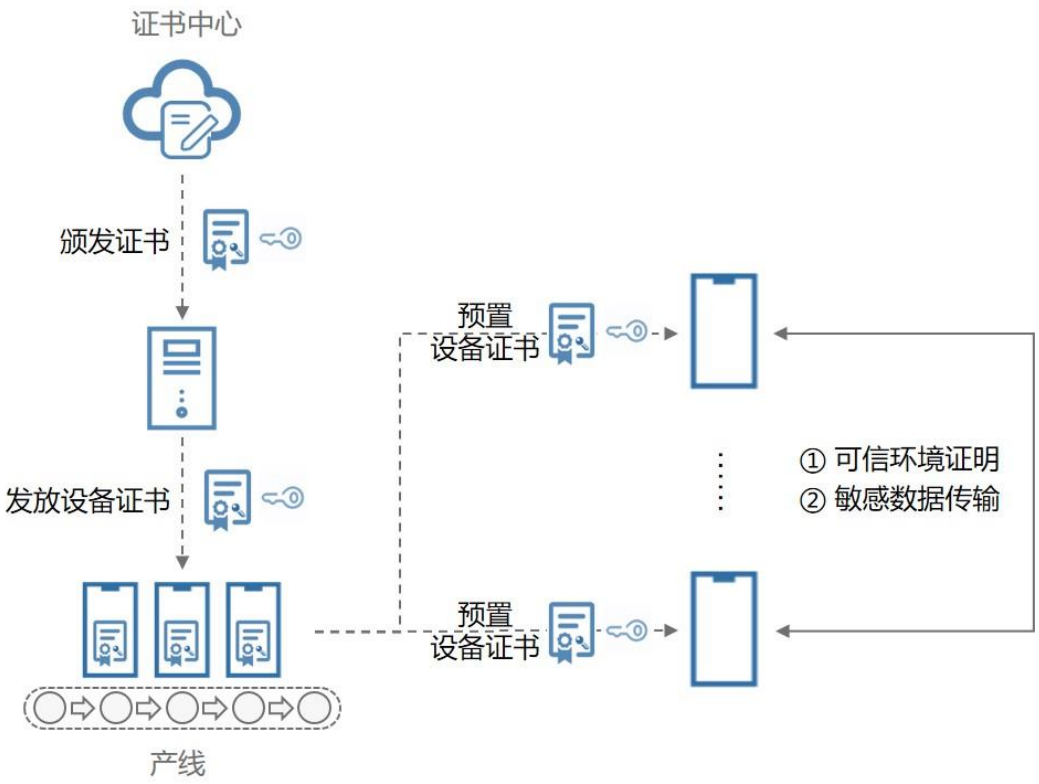
提供了基于硬件的可信执行环境（TEE，Trusted Execution Environment）来保护用户的个人敏感数据的存储和处理，确保数据不泄露。由于分布式终端硬件的安全能力不同，对于用户的敏感个人数据，需要使用高安全等级的设备进行存储和处理。HarmonyOS 使用基于数学可证明的形式化开发和验证的 TEE 微内核，获得了商用 OS 内核 CC EAL5+的认证评级。

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 所示。

图 1 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：**根据数据所在的国家或组织的法律法规与标准规范，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、使用和传输。

- **数据存储：**HarmonyOS 通过区分数据的安全等级，存储到不同安全防护能力的分区，对数据进行安全保护，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（多个设备通过华为帐号建立配对关系），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，安全地传输数据。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。

资料来源： HarmonyOS 官网
https://developer.harmonyos.com/cn/docs/documentation/doc-guides/harmonyos-security-0000000000011934