计算机安全架构演进与HarmonyOS安全设计实践

付天福

华为消费者业务 首席安全架构师

HUAWEI

- **HarmonyOS安全设计理念**
- 如何利用HarmonyOS安全能力保护你的数据
- HarmonyOS隐私保护策略
- 总结

HUAWEI

“超级终端”给安全与隐私带来全新体验和挑战

用户体验
如同使用一个超级设备

三方开发者
可基于抽象的超级设备开发服务

多端分布式平台

HUAWEI

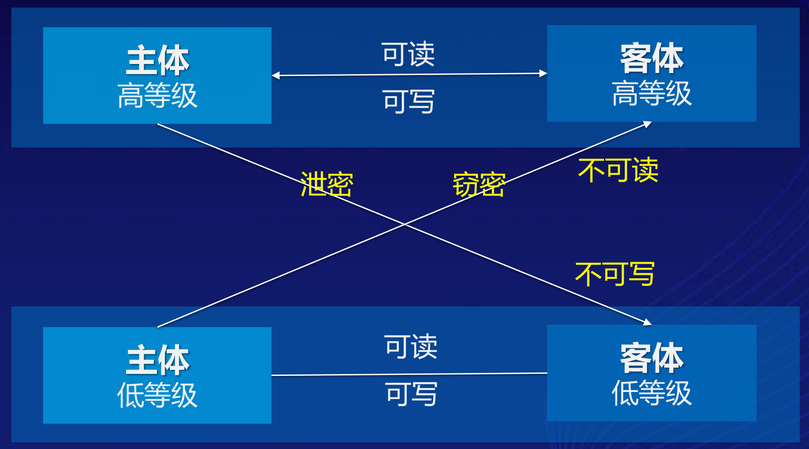
分级安全系统理论是HarmonyOS安全架构的核心逻辑

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）

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。



正确的人
（数据的主体信任等级）

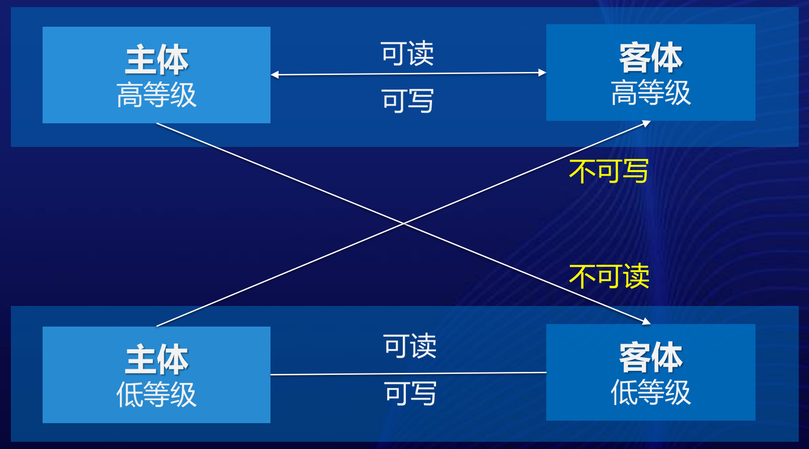
正确的设备
（数据的载体环境属性等级）

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）

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。



正确使用数据
（数据的客体隐私敏感等级）

HUAWEI

HarmonyOS安全目标：确保正确的人用正确的设备正确使用数据

正确的人

正确的设备

正确使用数据

HUAWEI

- HarmonyOS安全设计理念
- **如何利用HarmonyOS安全能力保护你的数据**
- HarmonyOS隐私保护策略
- 总结

HUAWEI

正确的人

正确的人：基于零信任网络架构的身份认证与访问控制架构

用户协同认证与访问控制SDK

3 分布式跨设备互助与协同

- 持续信任等级评估
- 细粒度/持续认证与访问控制

2 用户协同认证与调度

- 用户身份管理
- 认证器动态编排

1 多因素协同认证

秘密信息认证	可信持有物认证	生物特征认证	持续认证
What do you know 证明知道秘密	What do you have 证明持有可信物	Who are you 证明符合生物特征	Always be you 证明一直是“你”特征
锁屏密码 应用密码	配件 ...	人脸 ...	划屏/输入 声纳...

HUAWEI

参考NIST AAL分级-设备身份凭据信任分级标准

NIST将认证凭据定义为9类

- **AAL1**：单因素认证凭据对应**AAL1**级；**AAL2**：多因素认证凭据组合或自带多因素的认证凭据；**AAL3**：在**AAL2**的基础上增加了硬件保护

编号	NIST凭据分类	解释
1	Memorized Secrets	各种密码（由用户选定并且记忆的机密信息。）（Something you know）
2	Look-Up Secret	一个物理的或者电子记录用来存储用户与账户分发机构之间共享一系列的机密信息（Something you have）-----如：购买windows时给的注册码；苹果的双重认证有用到，20个bit的随机数，需要用户自己记录到纸上或其他位置。
3	Out-of-Band Device	一个可以与验证方用一个与主认证通道不同的通讯通道来及帮助进行验证的物理设备（Something you have）
4	Single-Factor OTP Device	一个生成one time password的物理设备，其生成的机密信息根据时间变化而变化。（Something you have），----两台设备遵循一个协议，都生成一样的二维码，如用OTP的方式生成的旧设备的认证码
5	Multi-Factor OTP Devices	一个生成需要特定认证因素（比如指纹）激活掉的one time password的物理设备，其生成的机密信息根据时间变化而变化。（Something you have，但是被something you know 或 something you are激活）
6	Single-Factor Cryptographic Software	一个存储在磁盘或者其他‘soft’媒介密钥信息（Something you have）
7	Single-Factor Cryptographic Devices	一个通过直接连接用户终端提供支持认证操作的设备（类似于口令牌）（Something you have）
8	Multi-Factor Cryptographic Software	一个存储在磁盘或者其他‘soft’媒介密钥信息,这个媒介需要通过另外一个因素的认证来激活（Something you have，但是被something you know 或 something you are激活）
9	Multi-Factor Cryptographic device	一个设备在通过另外一个因素的认证来激活后，可以用被其保护的密钥进行密码学操作。（Something you have，但是被something you know 或 something you are激活）

增加了硬件保护的多因子认证

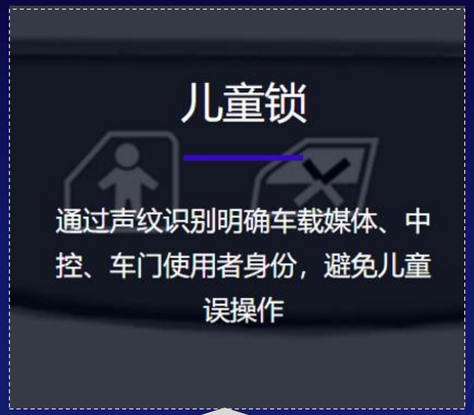
多因子认证

单因子认证

Source:https://pages.nist.gov/800-63-3/sp800-63-3.html

HUAWEI

HarmonyOS精准声纹，提供可靠、个性化的车载交互保障



声纹能力

- 唤醒/命令词/热词精准用户认证
- 说话人属性(性别/年龄/情绪)
- 用户特征聚类 (免注册/引导注册)

统一声纹认证服务

语音处理

- 声学前端处理
- 多样化音频数据分析
- 多种方式有效降噪

声纹引擎

认证引擎

- 文本相关/无关认证
- 文本融合认证

抗攻击引擎

- 抗录音攻击
- 抗合成/转换攻击

鸿蒙多设备可信互联

- 精准声纹在HarmonyOS 3.0上，认证性能全面领先：
- 误识率 <= 0.1%
- 唤醒率 >= 95%
- 仿冒检出率 >=95%
- 可支撑车载模块高精度唤醒，高敏感业务认证和执行，抵御常见仿冒和录音攻击

HUAWEI

分布式可信互联：把正确的人的正确设备安全地连起来，组成虚拟终端

设备被正确的人绑定
（安全的交换公钥凭据）

设备关系初始化阶段

所连接的设备都属于正确的人
（连接之前基于双方公私钥对完成双向身份认证，证明是已绑定的设备）

设备连接阶段

设备间传输的数据只有正确的人可访问
（基于认证结果完成会话秘钥协商，对传输数据进行加密与完整性保护）

数据传输阶段

HUAWEI

分布式协同认证：分布式生物特征共享与协同认证能力

分布式采集与认证能力共享（便捷性）

使用超级终端不同入口认证人的身份，
像使用单个设备一样便捷

分布式认证能力互助和协同（安全性）

使用超级终端对人的认证强度，
像使用高安全设备一样安全

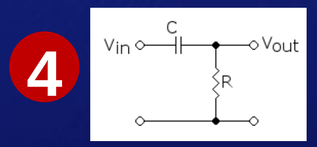
HUAWEI

正确的设备

正确的设备： 确保全场景设备运行环境可靠安全

HUAWEI

基于独立安全芯片能力，实现安全根，保障系统完整性和高安全隔离



传感器高通滤波器

•构建独立安全芯片信任根：

- Hi601X：具备基本安全存储、安全计算根能力
- Hi602X：在Hi6010基础上，接管CPU启动控制权
- Hi603X：彻底接管CPU的外网设备（磁盘、摄像头、指纹人脸、网络等）控制权，在CPU攻陷下系统仍然可信

① 自研安全芯片“信任根”：能够防物理攻击，同时提供密钥存储、加密、安全计算能力，**确保可信能力不依赖CPU和OS的安全。**

② 自研高安全TEE OS（CC EAL5+认证）：形式化验证内核，确保程序无漏洞。**保证鸿蒙OS被攻陷时，密钥、加解密、高安全服务等不被攻陷。**

③ PKI硬件加密机：所有鸿蒙OS程序升级和APP，均通过PKI加密机签名。

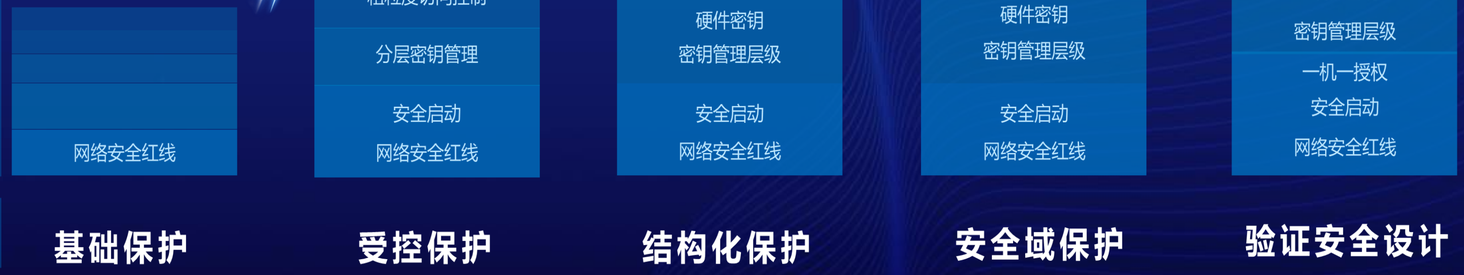
④ 传感器高通滤波器：通过传感器高通滤波器，将语音8KHZ频率高频部分过滤，**杜绝利用传感器实施语音监听**

HUAWEI

严格定义设备安全能力分级，基于分级实施访问控制

图：设备安全架构参考设计

划分设备安全等级
对应安全能力要求



HUAWEI

分布式终端OS安全设计目标及认证等级情况

设计目标
（参考桔皮书）

OS：以整体达到B1级为目标
数据安全：以达到B2级要求为目标
关键数据：以B3级要求为目标
核心子系统：以A1要求为目标

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
D	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

认证	认证对象	时间
安全内核CC EAL5+	TEE内核	2019
CC EAL5+	MSP安全核	2020
ASIL-D	TEE内核	2020
安全内核CC EAL6+	TEE内核（正在测试）	2022
EMVCo	inSE芯片	2018
国密认证	芯片	2019
MDPP	整机	2019
中国CC（EAL4+）	整机	2020

HUAWEI

正确的使用数据

HUAWEI

正确使用数据：定义数据隐私级别 确保数据流通安全可信

GDPR

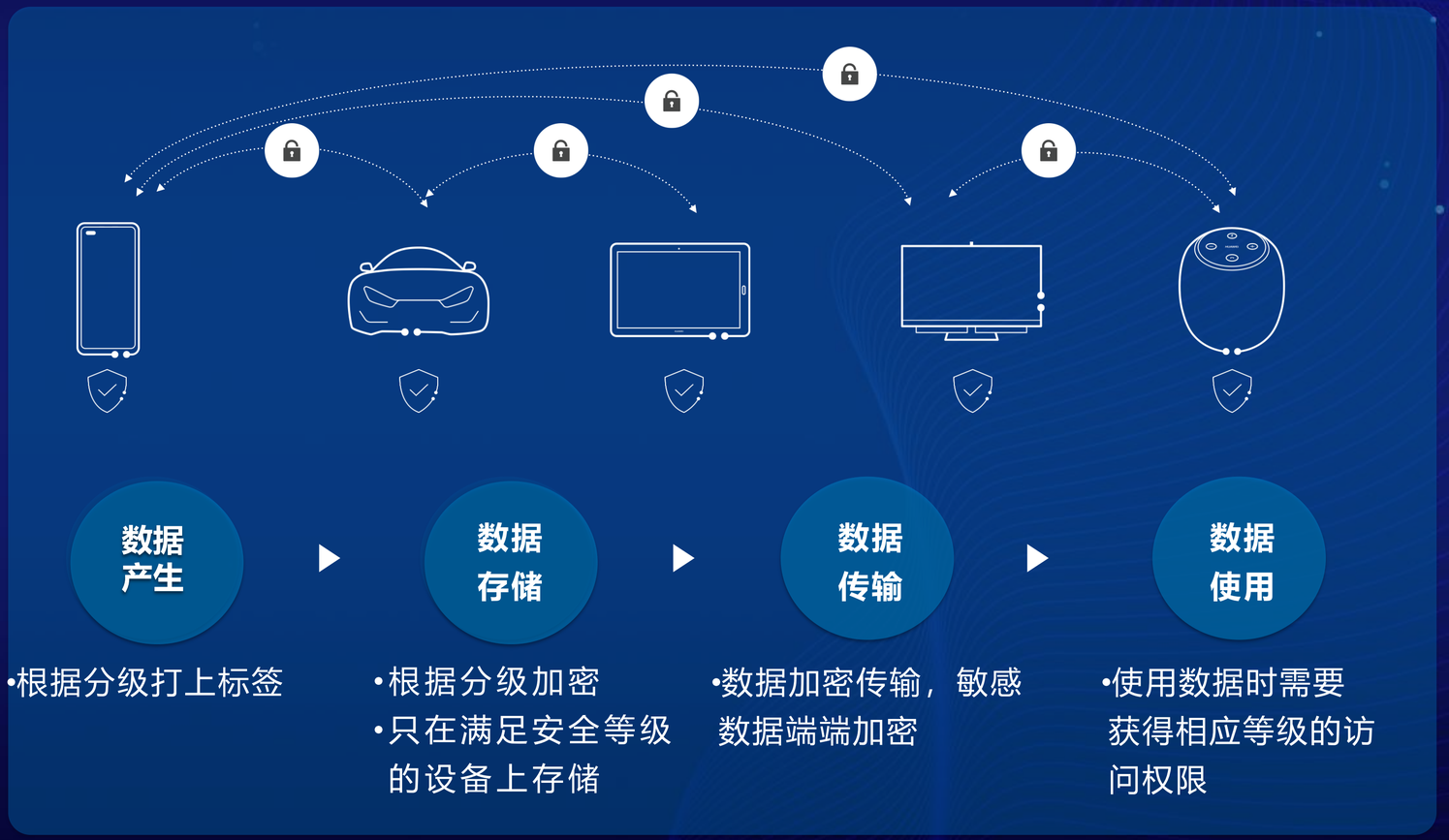
HIPPA

NIST

……

数据分类分级保护标准

分级	举例
S4	身份认证：指纹、人脸、密码 财务数据：银行卡号、支付信息 健康信息：血压、心率
S3	运动信息：步数、距离 位置信息：GPS记录、位置历史 用户生成数据：录音、照片
S2	联系方式：电话、传真、邮箱 网络地址：IP地址、蓝牙MAC地址
S1	一般个人信息：性别、国籍、出生地 应用个性化配置：闹钟、铃声 网络状态：网络类型、网络连接状态
S0	设备型号、厂家、尺寸、版本



HUAWEI

在应用生命周期实施生态治理：可追溯可运营能治理

1

数据分类分级

设备分类分级

隐私权限管理

……

2 开发阶段

（开发工具）

开发

开发者实名认证

发布

开发者证书签名

3 发布阶段

（应用市场）

检测

验证开发者证书签名

安全隐私检测

上架

应用市场签名

下架

违规应用下架

4 运行阶段

（操作系统）

安装

验证应用市场签名

应用来源可信

运行

隐私权限保护

AI未知威胁检测

更新

禁止未经检测的热更新/自更新

操作系统全生命周期应用生态治理能力

① **通过标准规范约束应用和设备：**严格定义的应用安全隐私规范和设备系统安全能力分类分级模型，确保生态“高标准严要求”。

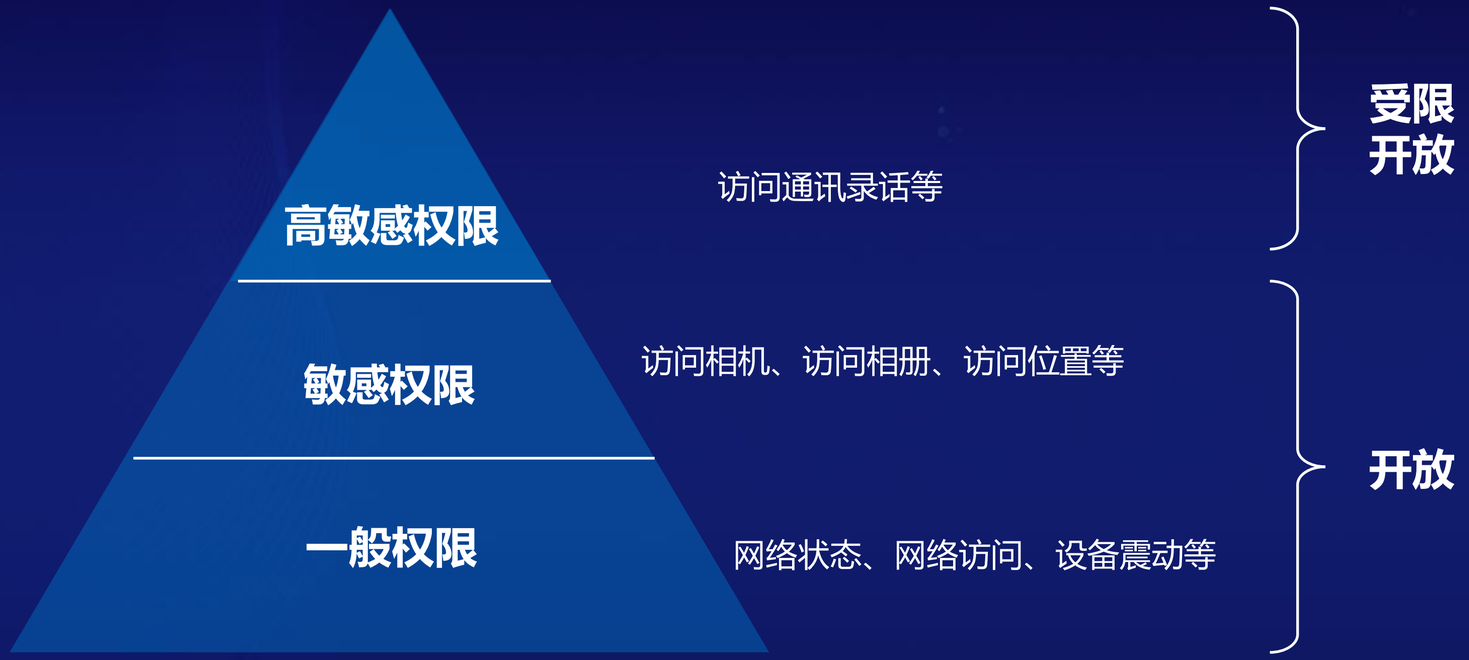
② **开发者实名认证：**确保生态产品（应用、设备）开发者“责权利”对等，违规行为可追责。

③ **应用与设备“实名”认证：**任何违规行为，应用与设备生命周期可追溯。

④ **生态可治理可运营：**基于开发者实名、应用程序“实名”、鸿蒙设备“实名”，实施生命周期运营，任何违规行为可归责、可管控。

HUAWEI

应用权限：根据资源/数据的分类分级，匹配正确的权限



权限分类分级

1. 依照数据分类分级标准，制定数据类权限分类分级原则
2. 根据功能或服务对设备的安全威胁影响程度，制定功能/服务类权限分类分级原则

权限开放原则

1. 普通应用使用率较高且合理的权限，开放使用，隐私相关权限需用户授权
2. 特殊类别的普通应用需要的权限受限开放

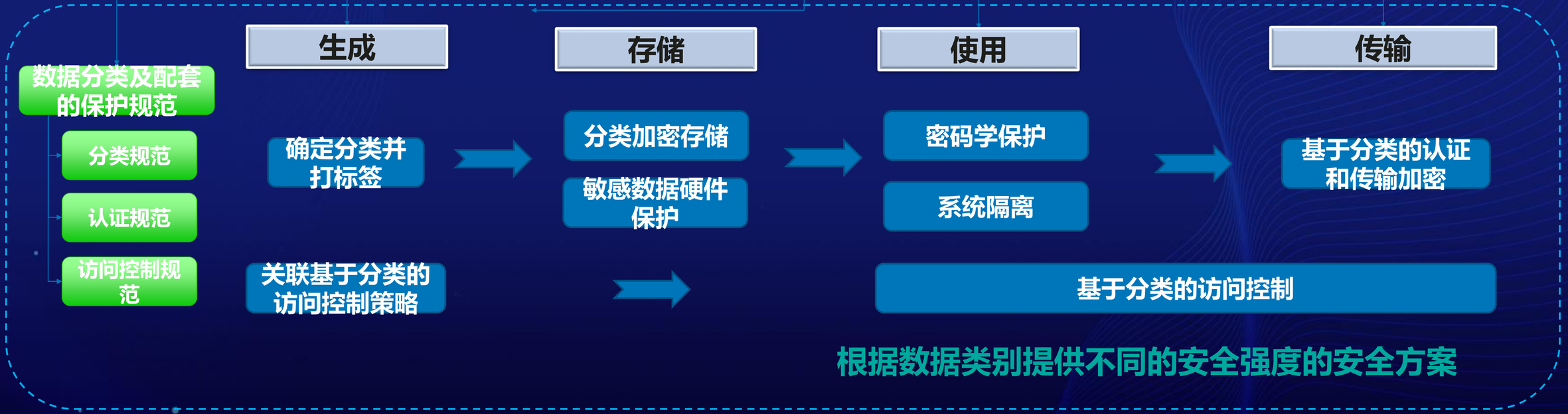
HUAWEI

在数据的生命周期实施分级安全保护

构建数据全生命周期的分类分级保护解决方案，实现正确的人通过正确的设备访问正确的数据

分类：根据数据的重要性或者风险来决定提供相应的保护，合理的分配资源，以有限资源提供更完善的保护以及满足合规。

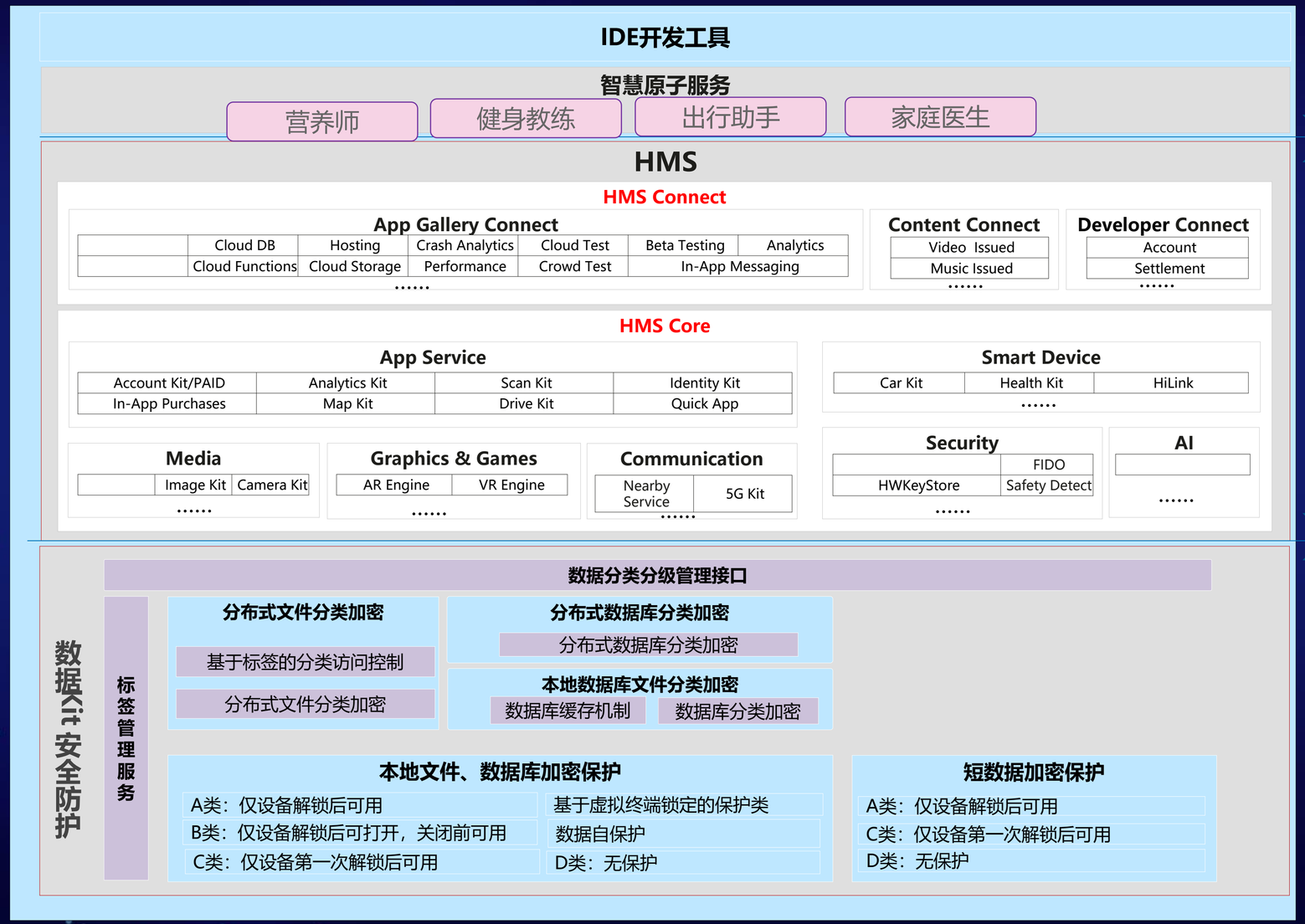
针对数据分类制定全生命周期的保护方案：越重要的数据攻击难度更大



根据数据类别提供不同的安全强度的安全方案

HUAWEI

数据Kit安全架构:IDE集成数据Kit的接口、权限控制，简化开发



3

简化和规范对于KIT和分类分级平台能力的调用，降低开发成本和出错可能性

- 以较小的开发代价做正确的事情（默认的集成规范和规则，根据开发场景主动的匹配）
- 前置检查，减小修复的代价

2

合理的使用平台能力，支撑业务需要

- 向下调用安全平台能力，对数据提供基于分类分级的保护方案，
- 向上开放接口，同时屏蔽底层数据分类保护对业务造成的影响

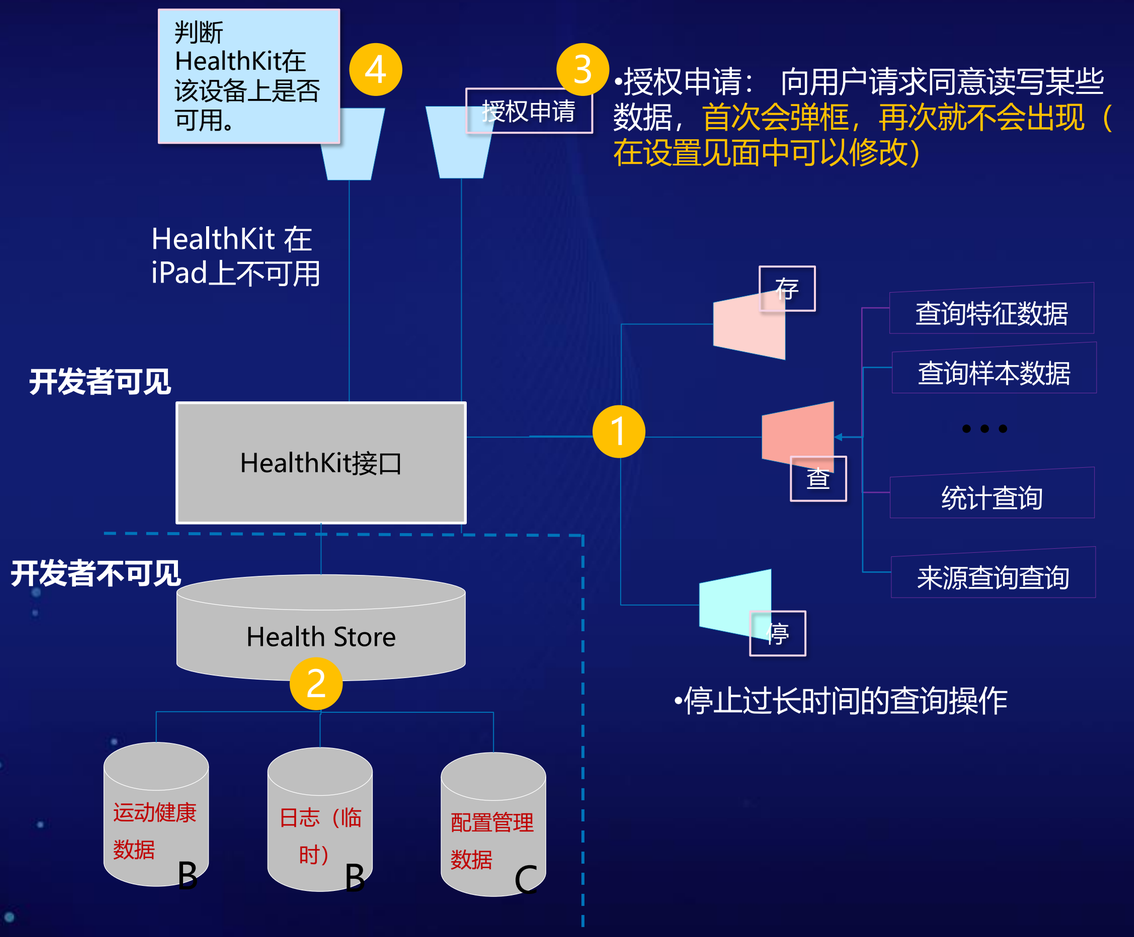
1

构建分布式场景下的分类分级平台能力

- 构建文件系统和端数据的分类保护能力
- 构建分布式数据管理的分类分级保护能力
- 构建分布式场景下的数据标签方案，标签伴随数据在虚拟终端内流动

HUAWEI

以Health Kit为例：对健康画像的全生命周期进行了严格的管理



1 **数据生成**：提供接口，便于APP使用：Health kit定义了丰富的运动和健康数据类型（共109种），数据被封装成严格定义的对象，数据携带唯一身份标签、权限等信息，实现数据全生命周期管理，并且简化数据记账流程，方便基于数据的计费与受益。下表为HealthKit定义的心率数据对象示例：

域	值
单位	次/分钟
数值	75
标识码（全局唯一）	FEBE1DFB-F3A6-4197-A2A6-04D8CEA657BD
数据来源	“Health”（13.2.3）（创建该数据的OWNER）
设备名称	Watch (13.2.3)（创建数据的设备）
系统签名	FEBE1DFB-F3A6-4197-A2A6-04D8CEA657BD（系统签名防篡改）
访问权限	L4（最高敏感权限）
数据生成时间	(2020-01-20 09:37:42 -0500 - 2020-01-20 09:37:42 -0500)

2 **At Rest**：调用分类保护的平台能力，对数据的提供合理的保护

3 **In Use**：实现对敏感数据的严格访问控制，保护数据的安全

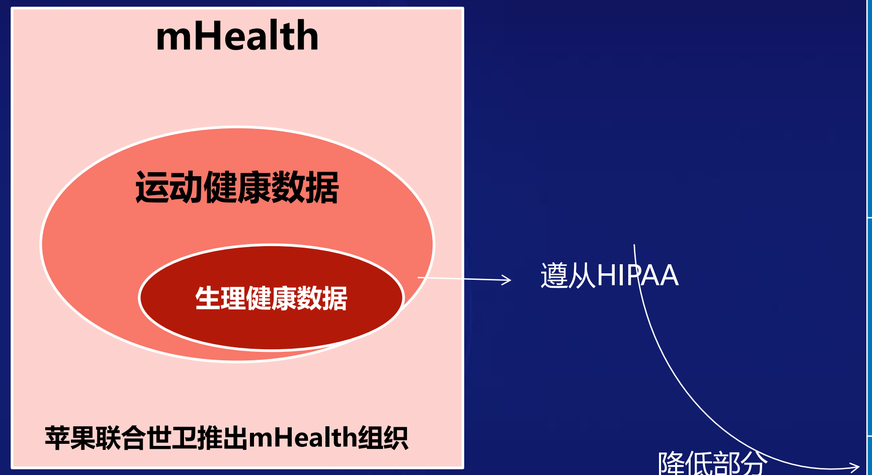
4 **In Transit**：通过Kit的部署限制，管控数据跨设备的流动

HUAWEI

At Rest：Health Kit对运动健康数据进行分类分级的加密存储

2 At Rest：调用分类保护的平台能力，对数据的提供合理的保护

- **Apple HealthKit数据根据《HIPPA》法规分成2大类，其中，生理健康数据为敏感个人数据**



遵从HIPAA

降低部分敏感数据保护方案

移动健康 (mHealth) 定义为由移动设备支持的公共医疗健康服务。移动设备包含移动电话，患者监控设备，个人数字设备，或者其他无线设备

数据分类/细分类别		分类说明
运动健康数据 **User's Health Data**	❑**特征样本（HKCharacteristicType)** ▪个人信息（性别、血型、生日），... ❑**数量样本（HKQuantityType)** ▪身体测量、健身数据、主要特征、营养摄入，... ❑**类别样本（HKCategoryType)** ▪生殖健康（睡眠分析、排卵测试、月经、性行为） ❑**关系样本（HKCorelationType)** ▪食物与血压关系，... ❑**锻炼样本（HKWorkoutType)** ▪太极、有氧运动、HandCycling，...	• Health and fitness apps • Healthcare institutions • Health and fitness devices
日志类数据（临时） **Temporary journal files**		• Fitness data gathered during exercise when device is locked
HealthKit配置管理数据 **Management data**		• Access permissions • Names of devices connected to HealthKit • Scheduling info used to launch apps
医疗ID数据（用于急救，手机不解锁也能显示） **Medical ID information**		• Medical conditions • Allergies & Reactions • Medications

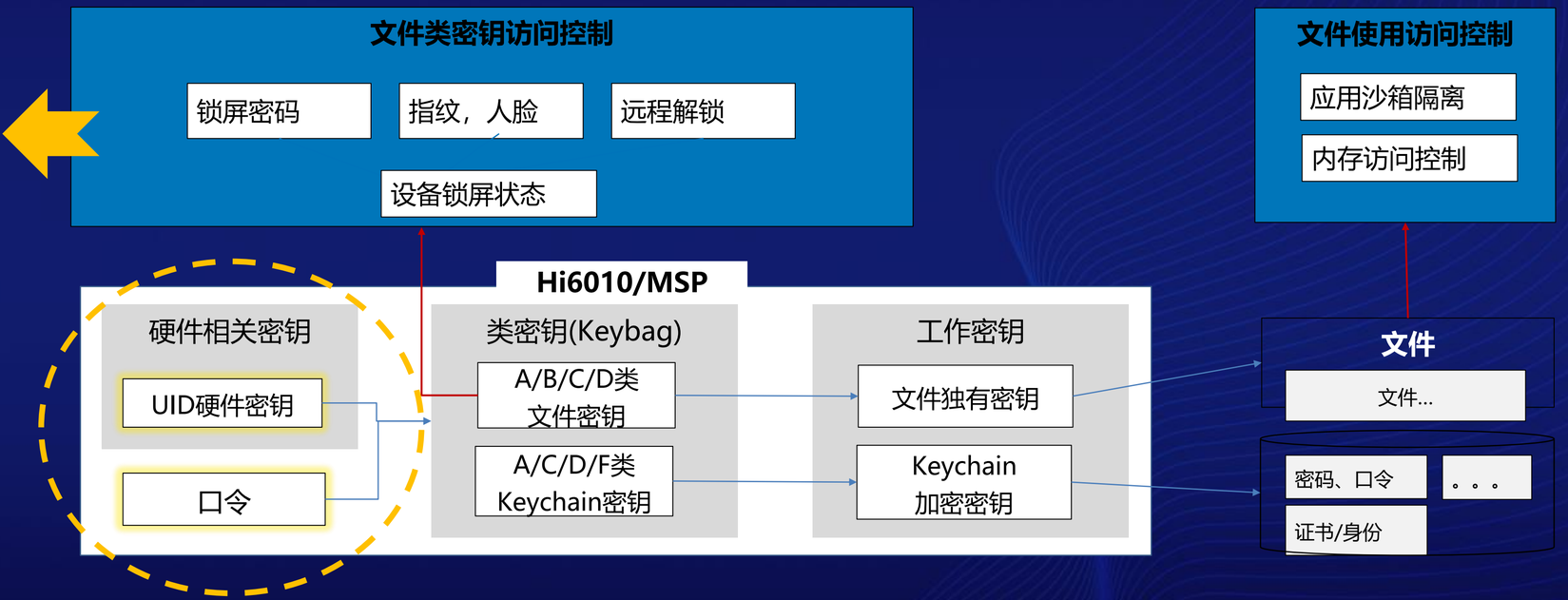
HUAWEI

数据加密存储的密钥完全掌握在用户手里，任何第三方不可解密

保护高敏感数据的类密钥由基于设备的根秘钥和用户脑子里的口令派生出来，因此除非用户在设备上输入正确的口令才可以解密敏感数据

文件保护措施	访问控制	数据示例
A类：未锁定状态下	**锁屏后立即丢弃密钥，不可读**	健康数据(体重、血压)
B类：锁定状态下	**锁屏状态下，不可打开已关闭的文件**	健康数据，邮件附件后台下载
C类：首次解锁后	**开机首次解锁后可读。类似全盘加密。默认类别。**	通讯录、照片
D类：始终可用	**锁屏可读的数据**	医疗救援信息、闹钟、壁纸等

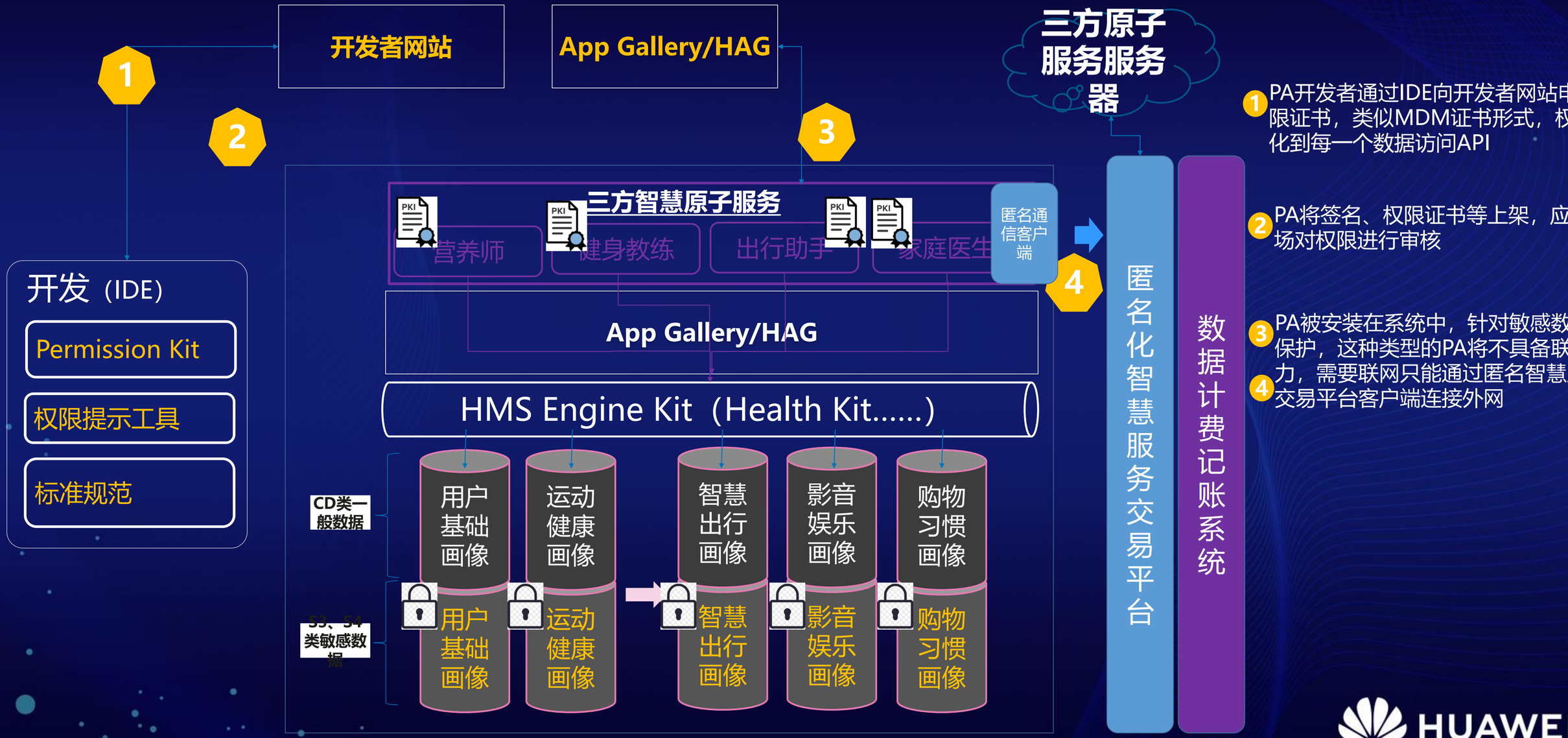
文件系统数据分类安全策略
约敏感的数据，访问控制策略越严格



加密密钥由用户手机终端芯片的唯一密钥（每个芯片都不相同，在工厂生产时预置，不可读取）和用户的屏幕锁口令生成，除了用户自己，任何人不可解密。

HUAWEI

In Use：HealthKit对PA权限细化到以每个数据为单位的权限控制



1. PA开发者通过IDE向开发者网站申请权限证书，类似MDM证书形式，权限细化到每一个数据访问API
2. PA将签名、权限证书等上架，应用市场对权限进行审核
3. PA被安装在系统中，针对敏感数据的保护，这种类型的PA将不具备联网能力，需要联网只能通过匿名智慧服务交易平台客户端连接外网
4.

HUAWEI

分布式访问控制：实现了基于设备和数据分类分级管理的数据访问控制

手机

分布式应用

TV

分布式应用

手表

分布式应用

分布式能力基础套件

分布式服务平台	
分布式Profile	**分布式访问控制**
分布式数据管理	分布式用户管理
分布式软总线	分布式协同认证

Device

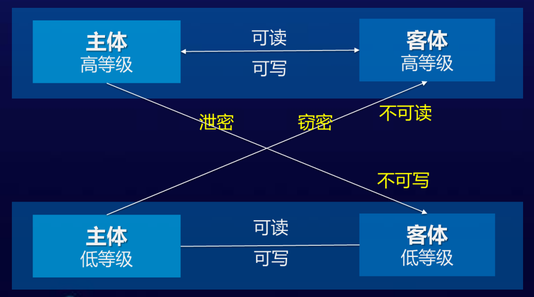
分布式服务

Device

分布式服务

Device

分布式服务

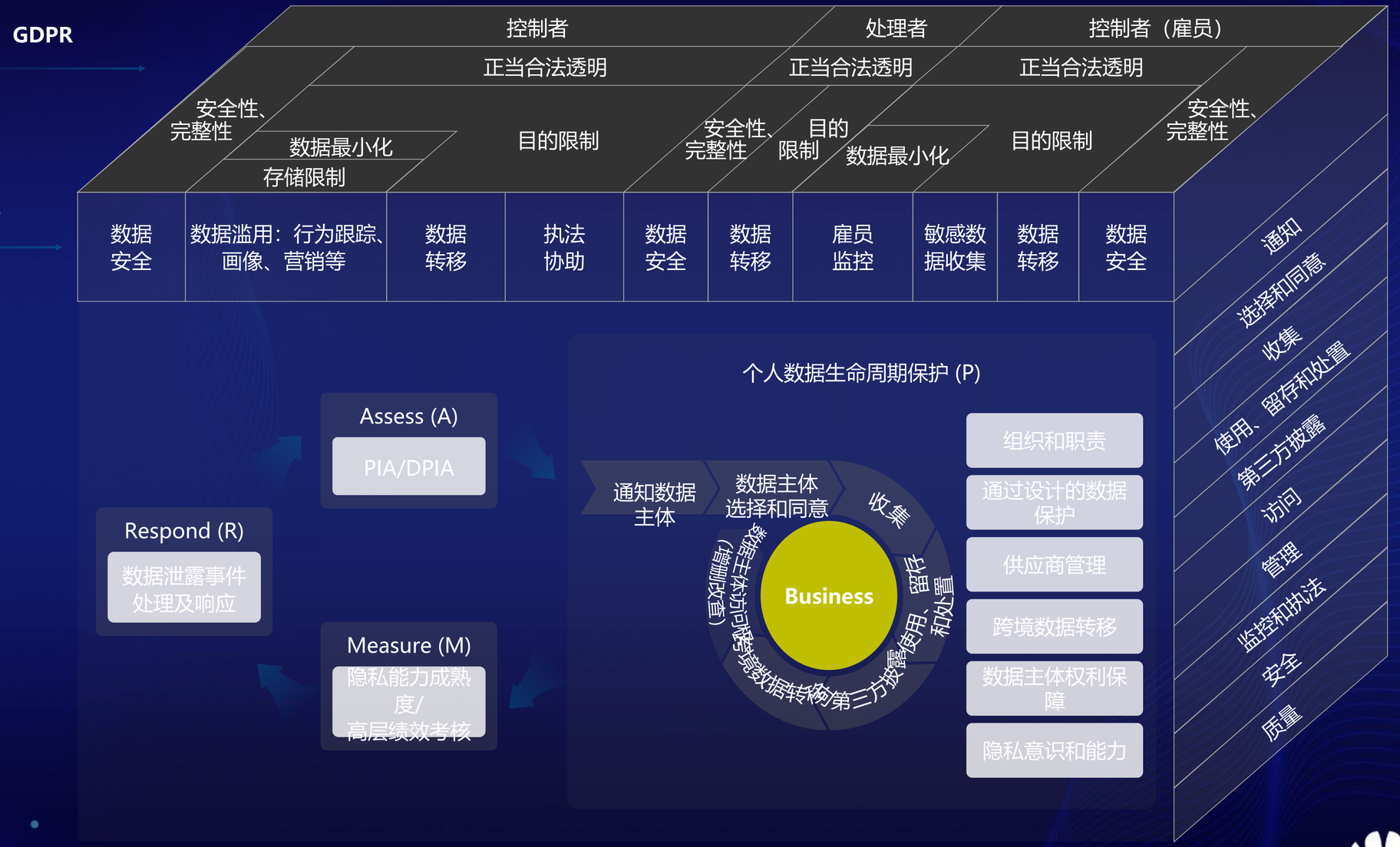


HUAWEI

- HarmonyOS安全设计理念
- 如何利用HarmonyOS安全能力保护你的数据
- **HarmonyOS隐私保护策略**
- 总结

HUAWEI

基于GDPR和GAPP合规，围绕数据全生命周期管理



HUAWEI

基于GAPP的隐私保护设计要点

1. 通知

- 收集个人数据前提供隐私通知
- 隐私声明变更需重新通知用户
- 隐私声明的内容可供用户随时查阅
- 隐私声明内容符合CBG隐私声明模板

2. 选择和同意

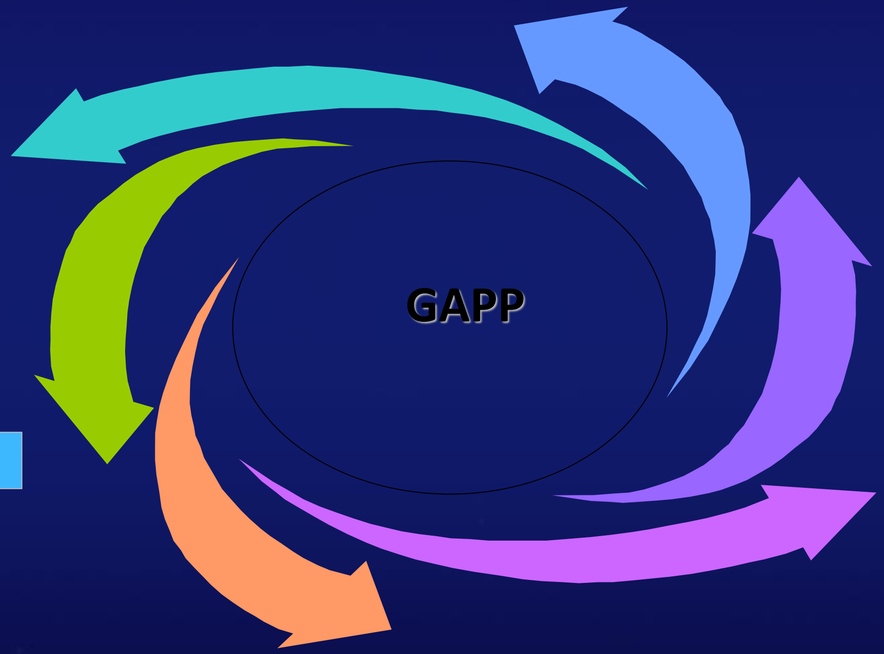
- 收集/使用个人数据前获得用户同意
- 提供撤销同意的渠道
- 保存用户同意、撤销同意记录

3. 收集

- 数据收集目的与隐私声明一致
- 数据最小化
- 保证个人数据的准确性和完整性

4. 使用、保留和处置

- 数据使用目的与隐私声明一致
- 数据存储和使用提供安全保护机制
- 有明确数据到期删除机制



5. 数据主体访问

- 验证数据主体身份
- 访问权、纠正权、删除权、限制处理权、数据可携带权、反对权、自动化决策和画像相关权利

6. 第三方披露

- 数据共享最小化
- 隐私声明中说明第三方披露数据类型、目的和接收者类别
- 第三方尽职调查
- 个人数据安全传输

7. 数据跨境转移

- 服务器部署满足3+X原则
- 数据跨境转移根据各国家和地区法律要求来执行

管理			安全	质量	监控和实施	
政策和流程	组织和资源	标准和法规	访问控制	记录和验证	执法机构调查和诉讼	投诉处理
风险评估（PIA等）	人员意识和能力		业务连续性	评估和校正	数据泄露事件响应	审计问责

- HarmonyOS安全设计理念
- 如何利用HarmonyOS安全能力保护你的数据
- HarmonyOS隐私保护策略
- **总结**

HUAWEI

构建鸿蒙OS具有韧性（缺陷少，难攻破，快修复）的安全系统

HUAWEI

接下来：

HarmonyOS系统安全能力

10:40am - 11.00am

HUAWEI