HUAWEI

< HDC.Together >

华 为 开 发 者 大 会 2 0 2 0

HarmonyOS安全和隐私设计

- **HarmonyOS安全设计理念**
- 如何利用HarmonyOS安全能力保护你的数据
- 利用HarmonyOS安全使能生态伙伴
- 总结

“超级终端”给安全与隐私带来全新体验和挑战

HUAWEI

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

分级安全系统理论是HarmonyOS安全架构的核心逻辑

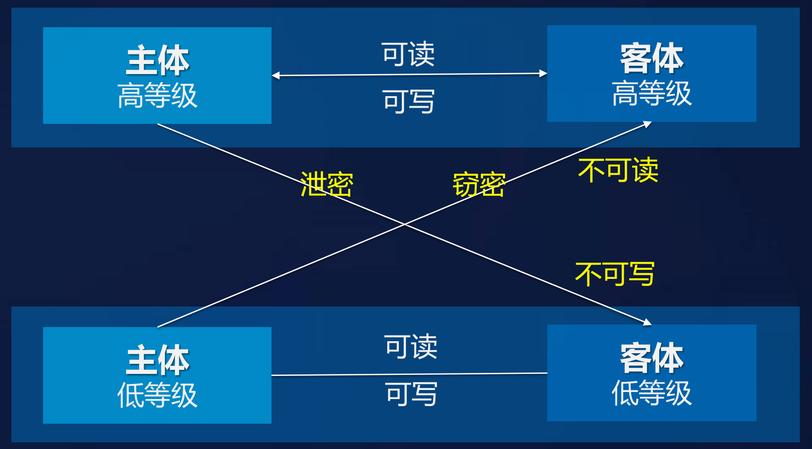
HUAWEI

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）

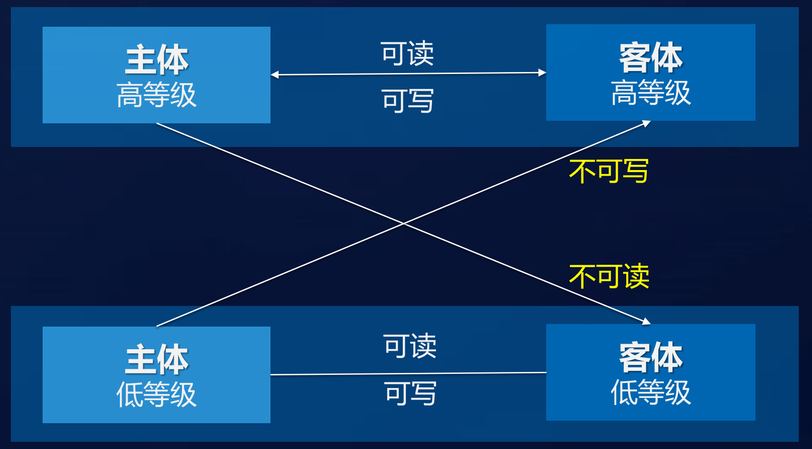
正确的设备
（数据的载体环境属性等级）

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）

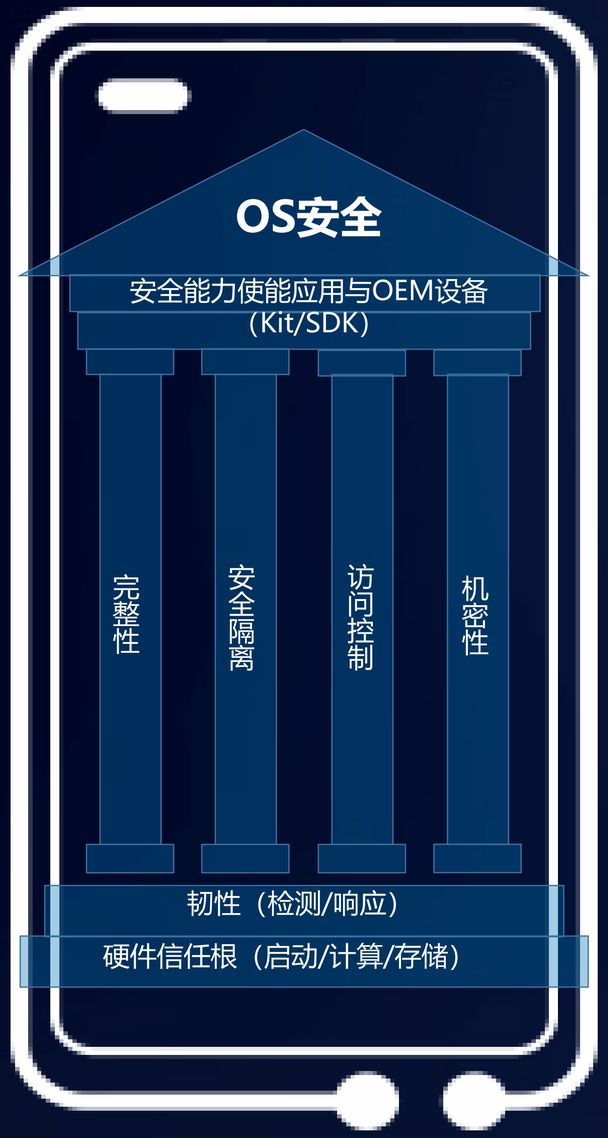
✓**不上写**-主体不能写入安全级别高于它的客体（数据）

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。

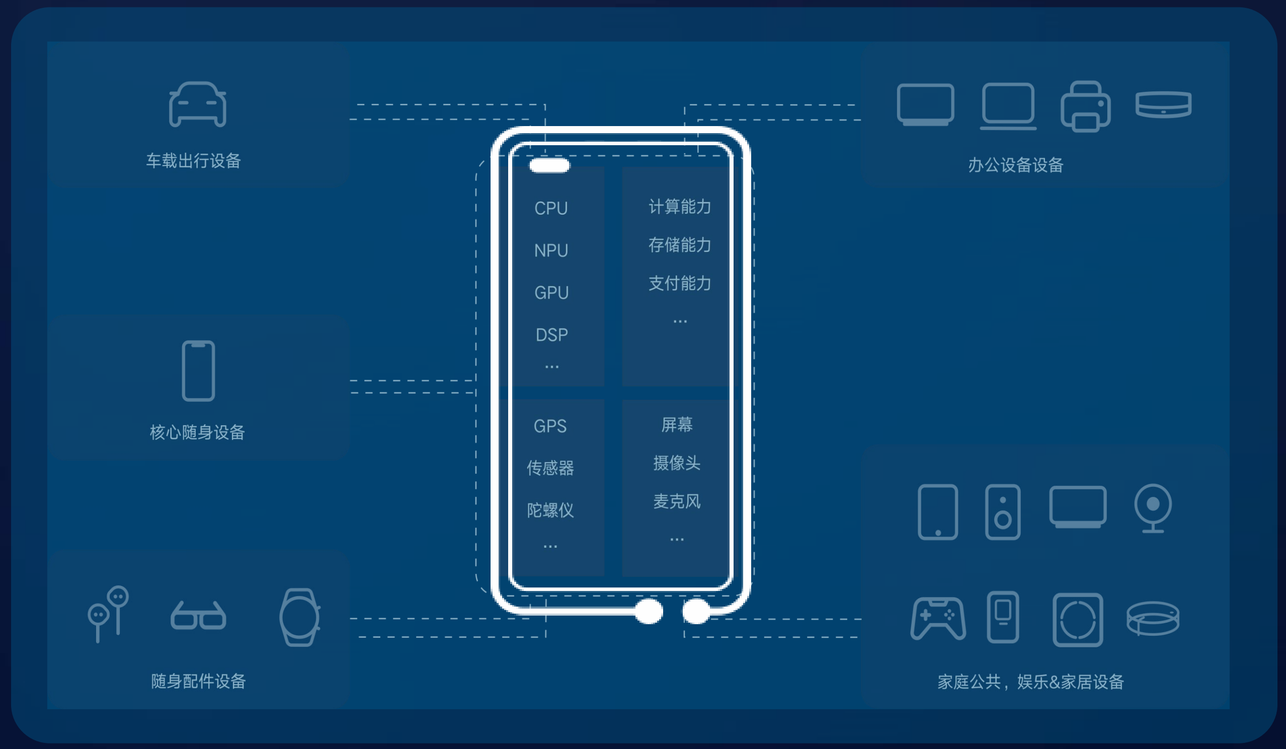


正确使用数据
（数据的客体隐私敏感等级）

HarmonyOS从单机向分布式构建分级安全架构



HarmonyOS超级终端
One Super Device



- HarmonyOS安全设计理念
- **如何利用HarmonyOS安全能力保护你的数据**
- 利用HarmonyOS安全使能生态伙伴
- 总结

HarmonyOS安全目标：确保正确的人用正确的设备正确使用数据

HUAWEI

基于分布式技术的协同身份认证更加便捷安全

秘密信息

可信持有物

生物特征

行为特征

正确的人

设备间可信的连接

正确的设备

设备间安全的传输和分享数据

正确使用数据

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

HUAWEI

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	配件	人脸	划屏/输入
应用密码	…	…	声纳…

参考NIST AAL分级-设备身份凭据信任分级标准

HUAWEI

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

身份认证安全能力开放框架

- 面向开发者，以最小化学习/使用成本为原则，对内、对外开放安全能力
- 面向普通开发者和垂直行业开发者，分别提供不同的kit

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

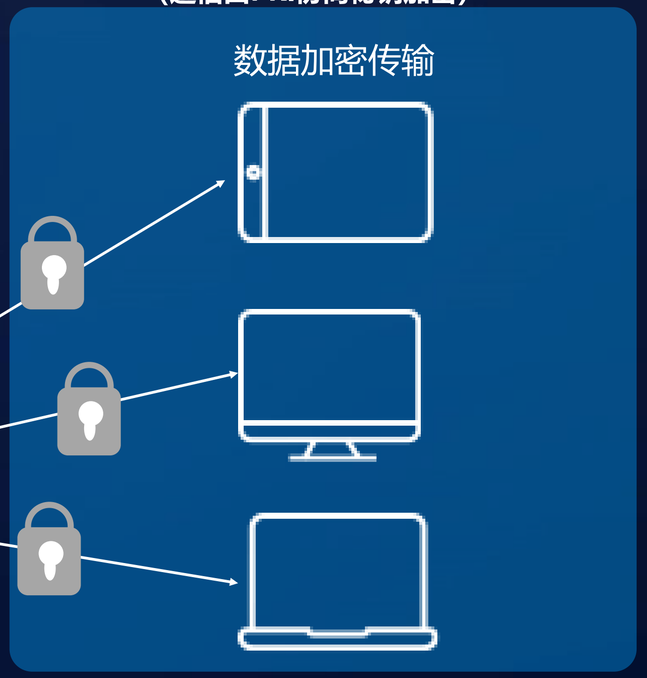
设备被正确的人绑定
（安全的交换公钥凭据）

设备关系初始化阶段

所连接的设备都属于正确的人
（连接之前用公钥实施身份认证，数据用私钥签名）

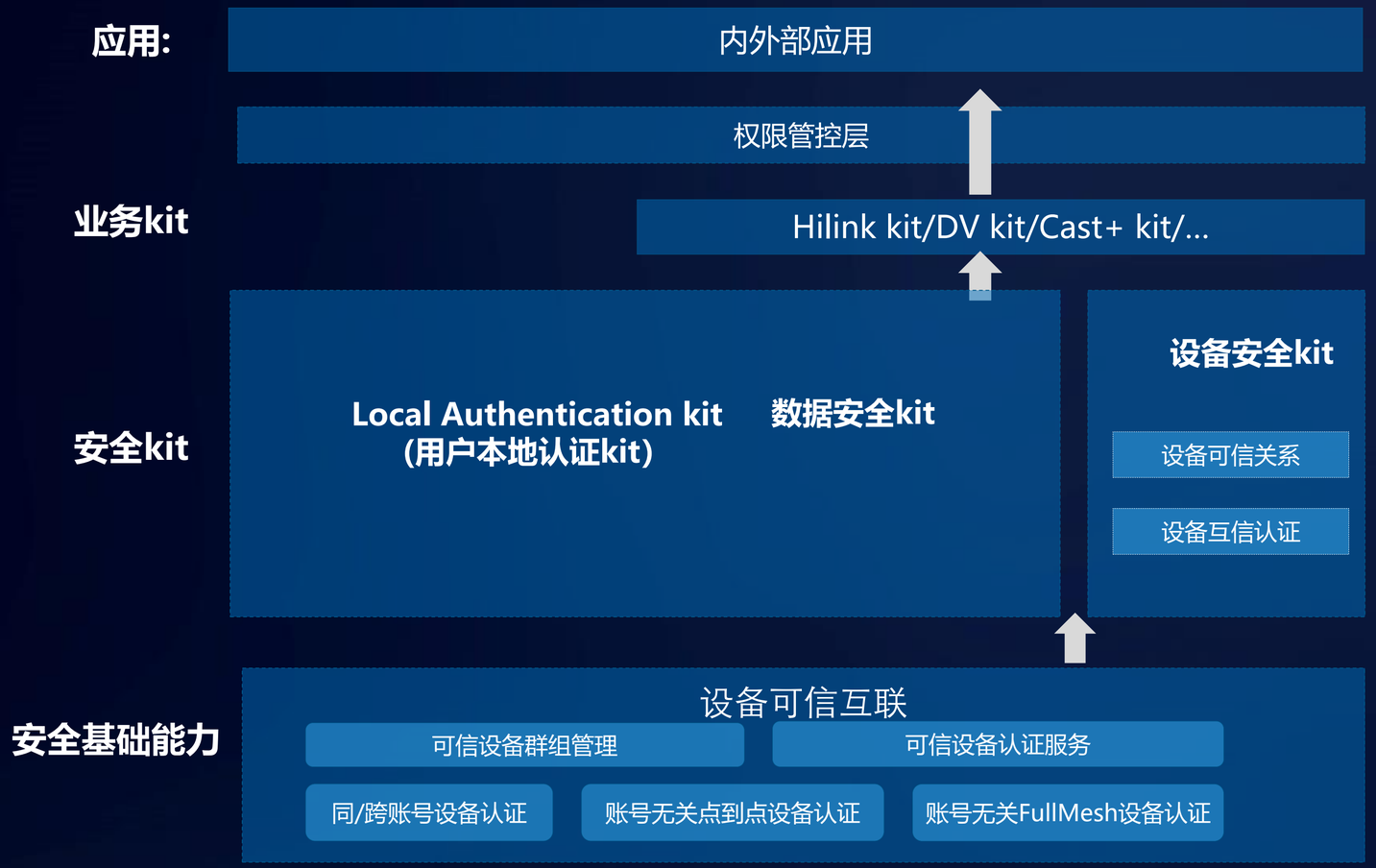
设备连接阶段

设备间传输的数据只有正确的人可访问
（通信由PKI协商秘钥加密）



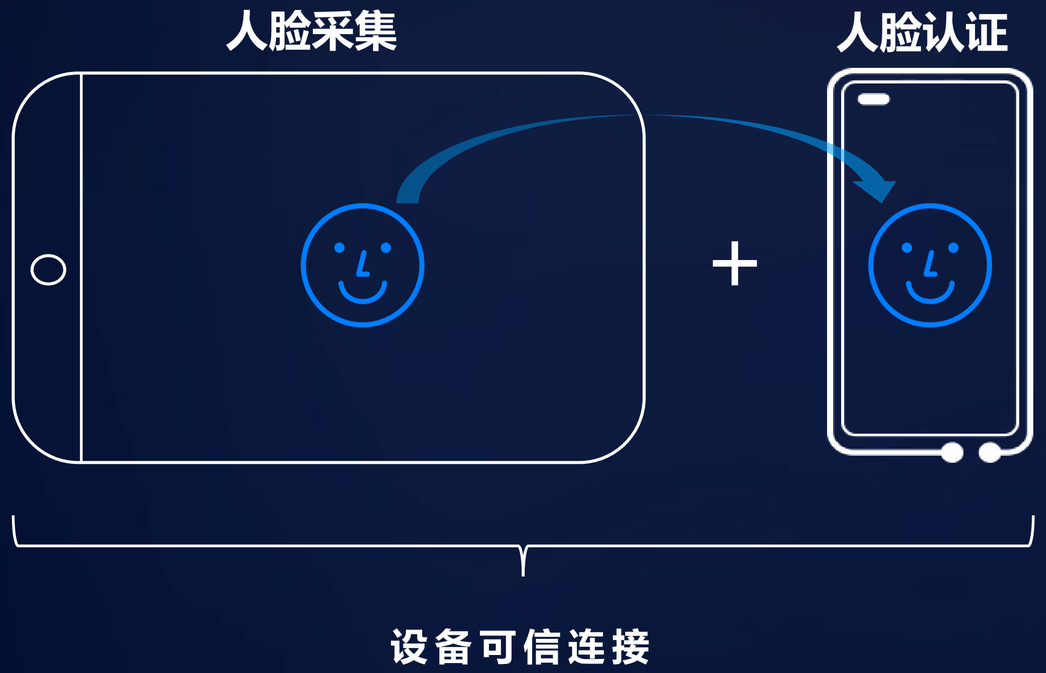
数据传输阶段

分布式可信互联能力开放



- 面向开发者，以最小化学习/使用成本为原则，对内、对外开放安全能力
- 面向普通开发者和垂直行业开发者，分别提供不同的kit
- 目前设备可信互联的安全能力集成在各业务kit中，不单独对外部应用开发者开放；

分布式协同认证：分布式生物特征共享与协同认证能力



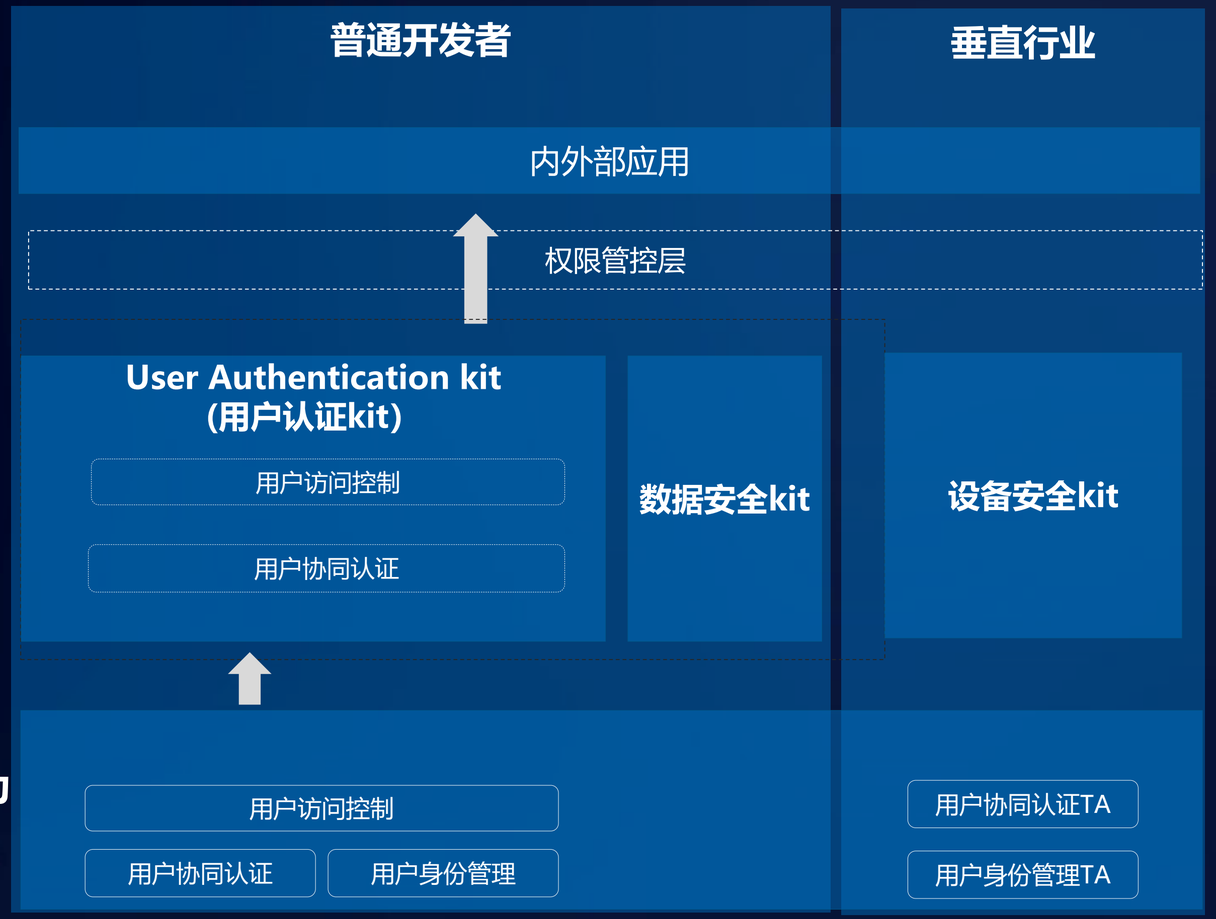
分布式采集与认证能力共享（便捷性）

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

分布式协同认证能力开放



- 面向开发者，以最小化学习/使用成本为原则，对内、对外开放安全能力
- 面向普通开发者和垂直行业开发者，分别提供不同的kit
- 目前仅对内部应用开放，未对三方应用开放；

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

分布式终端OS安全设计目标及认证等级情况

HUAWEI

设计目标
（参考桔皮书）

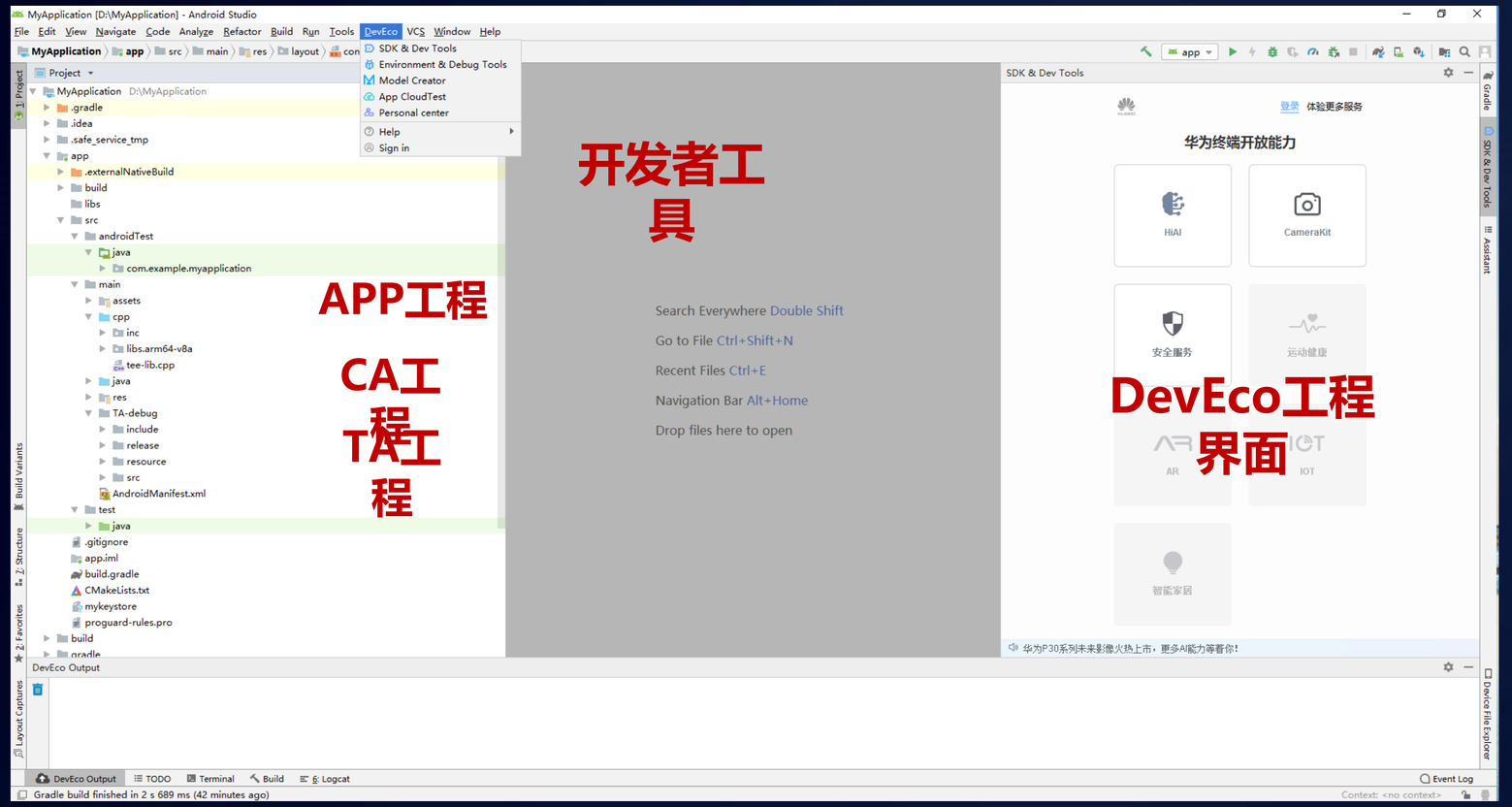
OS：以整体达到B1级为目标
数据安全：以达到B2级要求为目标
关键数据：以B3级要求为目标
核心子系统：以A1要求为目标

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
EMVCo	inSE芯片	2018
国密认证	芯片	2019
MDPP	OS	2019
中国CC（EAL4+）	OS	2020

面向开发者的TEE OS能力开放

HUAWEI



面向开发者提供业务开发服务

SDK　手册文档　参考设计　DevEco 工具

面向应用运营者提供业务上线服务

证书服务　生命周期管理　标准框架

开发者联盟获取材料 → 注册开发者账号 → 集成开发环境 → 业务审核上架

正确的使用数据

正确使用数据：定义数据隐私级别 确保数据流通安全可信

HUAWEI

GDPR

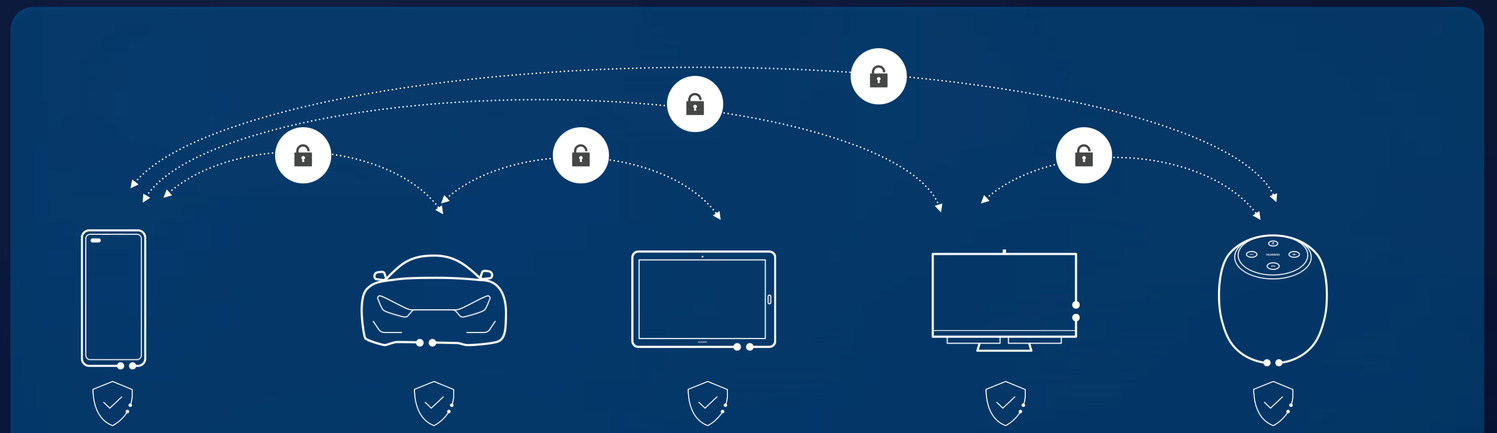
HIPPA

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



数据产生

- 根据分级打上标签

数据存储

- 根据分级加密
- 只在满足安全等级的设备上存储

数据传输

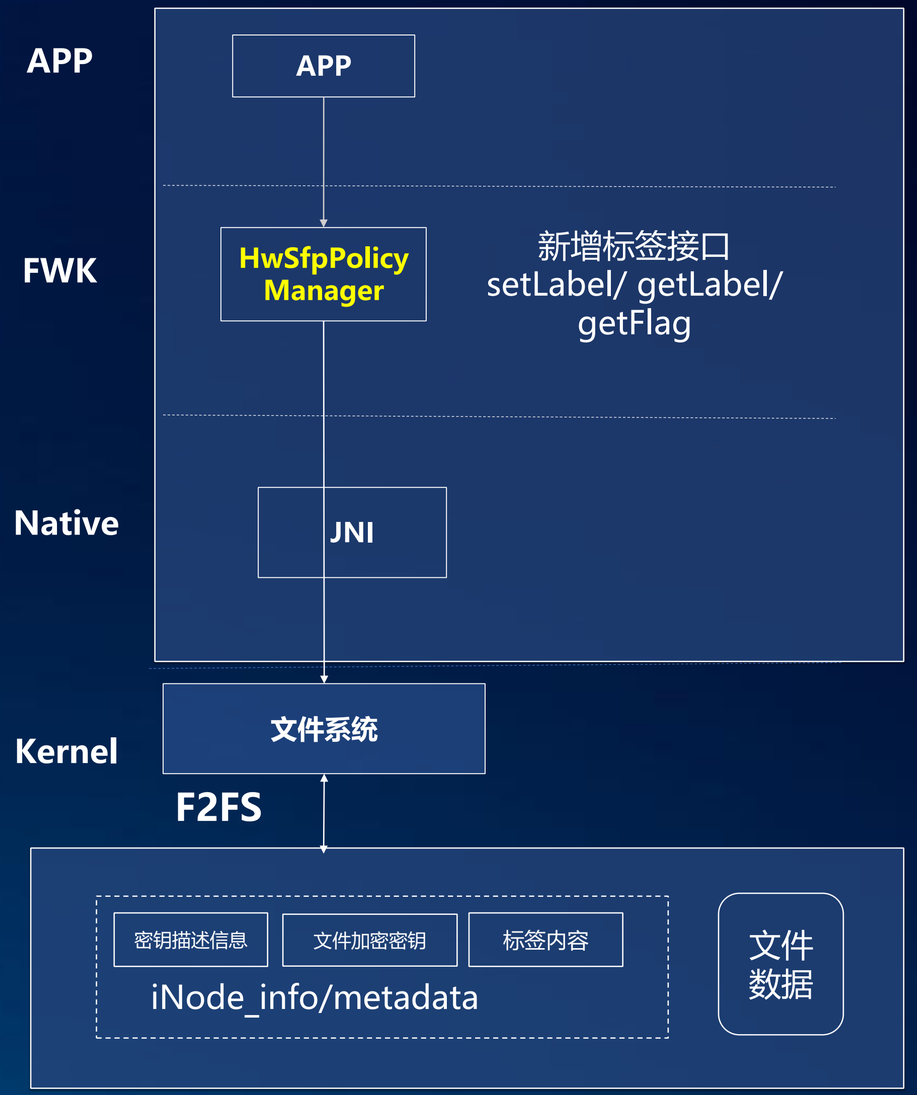
- 数据加密传输，敏感数据端端加密

数据使用

- 使用数据时需要获得相应等级的访问权限

数据分类分级加密保护标签方案

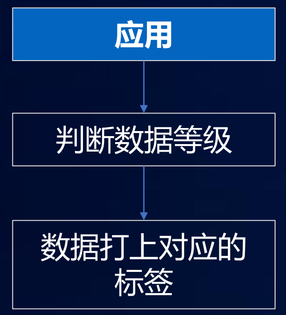
特性	文件打数据风险标签
特性描述	提供接口供应用设置数据的风险等级，标签系统自动适配加密保护方案
应用场景	为文件，数据库（将数据库文件按照文件保护）根据其风险等级提供保护
价值	降低应用使用门槛，减少异构设备上数据保护适配工作量，普及数据分级安全保护。
竞争力	差异化竞争力，安卓首发



分布式系统设备上风险等级和加密等级的对应关系

风险等级	严重（S4）	高(S3)		中(S2)	低(S1)	公开(S0)
保护策略	锁屏下不可写	锁屏下不可写	锁屏下可写	第一次解锁前不可写	上电即可写	上电即可写

文件分级能力接口描述



功能	接口原型	描述

设置文件风险等级	int HwSfpPolicyManager.setLabel (Context context, String filePath, String labelName, String labelValue，int flag)	设置文件风险等级标签，如果设置成功则返回0，失败则返回错误码；
		context：上下文对象
		filePath：需要设置风险等级的文件路径+文件名称
		labelName：分类分级标签名，为SecurityLevel
		labelValue：分类分级值，为S4-S0
		flag：0x0000 本地使用，锁屏不可写，支持S4-S0入参
		0x0001 本地使用，锁屏可写，仅支持S3入参
		`// Set the SECE file to the corresponding label level: S3 and the flag is FLAG_FILE_PROTECTION_COMPLETE_UNLESS_OPEN.`
		`int errorCode = policyManager.setLabel(context, filePath,`
		`HwSfpPolicyManager.LABEL_NAME_SECURITY_LEVEL, HwSfpPolicyManager.LABEL_VALUE_S3,`
		`HwSfpPolicyManager.FLAG_FILE_PROTECTION_COMPLETE_UNLESS_OPEN);`

获取文件风险等级	String HwSfpPolicyManager.getLabel (Context context, String filePath, String labelName)	获取文件风险等级标签，输入文件绝对路径+文件名称，可查询文件的风险等级。
		`// Get the file's corresponding label level.`
		`String label = policyManager.getLabel(context, filePath,`
		`HwSfpPolicyManager.LABEL_NAME_SECURITY_LEVEL);`

获取文件风险等级附属的细分属性信息	int HwSfpPolicyManager.getFlag (Context context, String filePath, String labelName)	文件风险等级附属的细分属性信息，为0或1，如果没有设置风险等级，返回-1
		`// Get the ancillary information of security label for a file.`
		`int flag = policyManager.getFlag(context, filePath,`
		`HwSfpPolicyManager.LABEL_NAME_SECURITY_LEVEL);`

三方设计与开发工作量：
约1人周

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

HUAWEI

手机
分布式应用

TV
分布式应用

手表
分布式应用

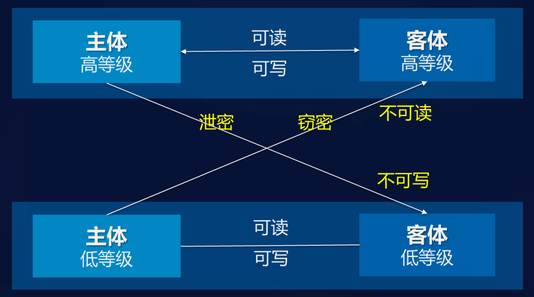
分布式能力基础套件

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



- HarmonyOS安全设计理念
- 如何利用HarmonyOS安全能力保护你的数据
- **利用HarmonyOS安全使能生态伙伴**
- 总结

OS安全能力开放：使能生态合作伙伴开发安全的应用与设备

HUAWEI

一般开发者

支付购物、金融理财、社交通信等开发者

特定行业

安全生态伙伴：手机车钥匙、ePOS

高安行业：银行（手机盾）、银联（手机POS）、公安等

HMS Core

HMS安全能力向**应用生态**开放

Wallet Kit | Account Kit | DRM Kit | Fido Kit

Safety Detect Kit | Data Sec Kit

HMS Engine

安全能力全集，直接通过Engine开放给**OEM/应用生态**合作伙伴

Authentication Engine（正确的人）

Data Security Engine（正确的数据）

Device Security Engine（正确的设备）

端侧安全基础能力平台

- HarmonyOS安全设计理念
- 如何利用HarmonyOS安全能力保护你的数据
- 利用HarmonyOS安全使能生态伙伴
- **总结**

基于拜占庭入侵容忍技术构建具有韧性的安全系统

HUAWEI

欢迎关注HarmonyOS开发者微信公众号