OpenHarmony

开放原子开源基金会 OpenHarmony开发者大会 2023

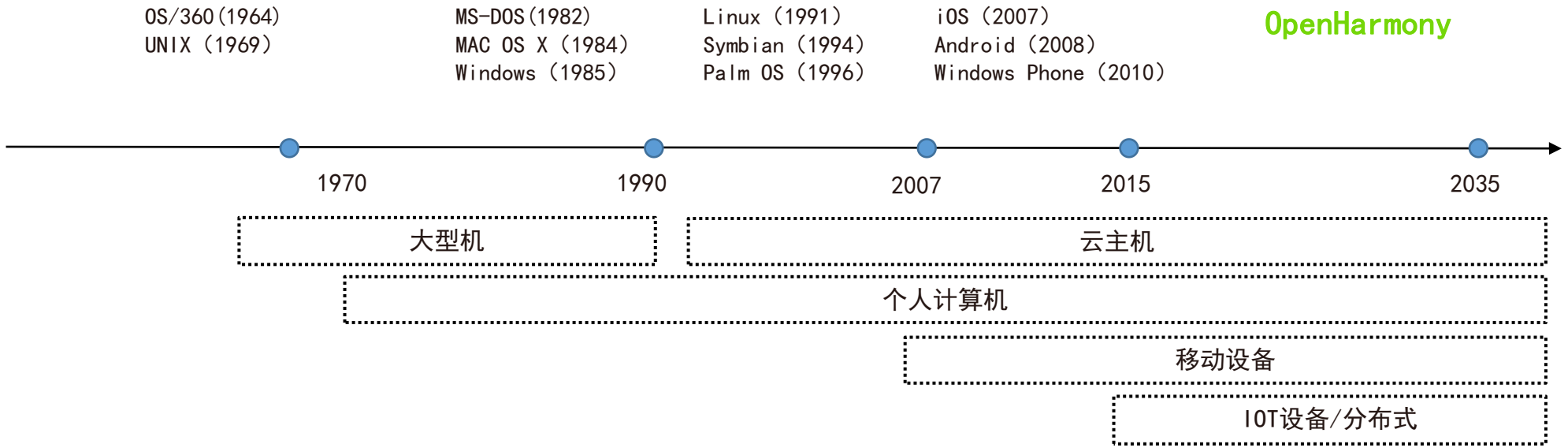
Openharmony安全和隐私保护技术演进

高红亮

职位 / 介绍 ：Openharmony安全架构师

目录 Contents

从OS的历史看OS安全的演进



	大型机	个人计算机	移动终端设备	IOT设备/分布式
安全特征	主要对资源非授权访问和机密文件窃取的安全攻击	以破坏系统为目的的病毒泛滥	用户机密与隐私数据价值大，成为攻击者逐利的目标	如何保证在不同安全等级设备上，实现对应数据的隐私保护
安全技术	主要通过账号隔离、访问控制	安全启动等完整性保护技术	数据隐私安全保护、权限管理等	分级权限管控、设备可信连接，以及不同等级数据跨设备传输安全性

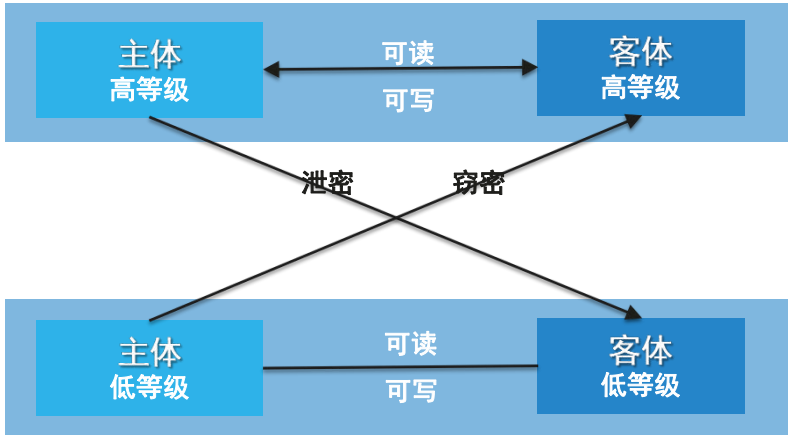
Openharmony安全模型：分级安全架构，重点加强应用分级权限能力构建

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。

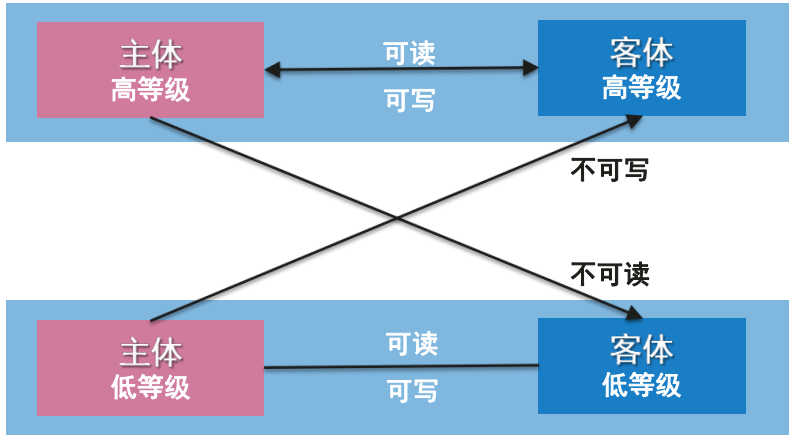


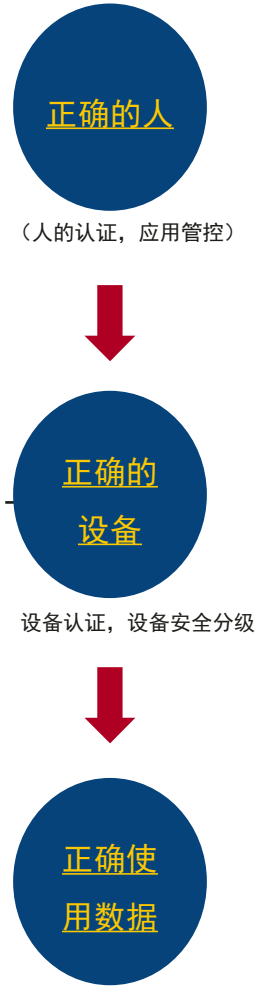
Biba模型核心规则

✓不下读-主体不能读取安全级别低于它的客体（数据）

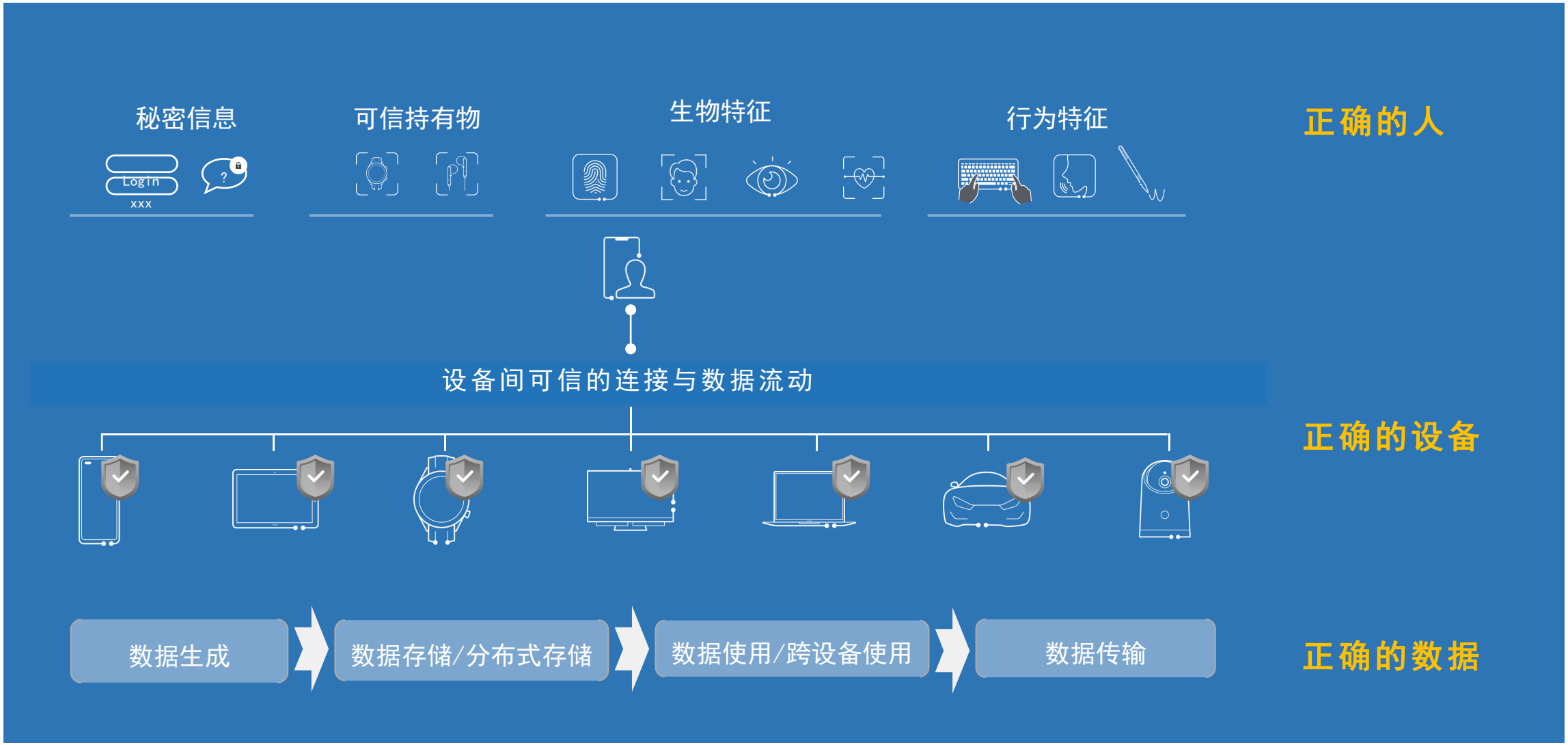
✓不上写-主体不能写入安全级别高于它的客体（数据）

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。





分布式安全：正确的人，通过正确的设备、访问正确的数据



目录 Contents

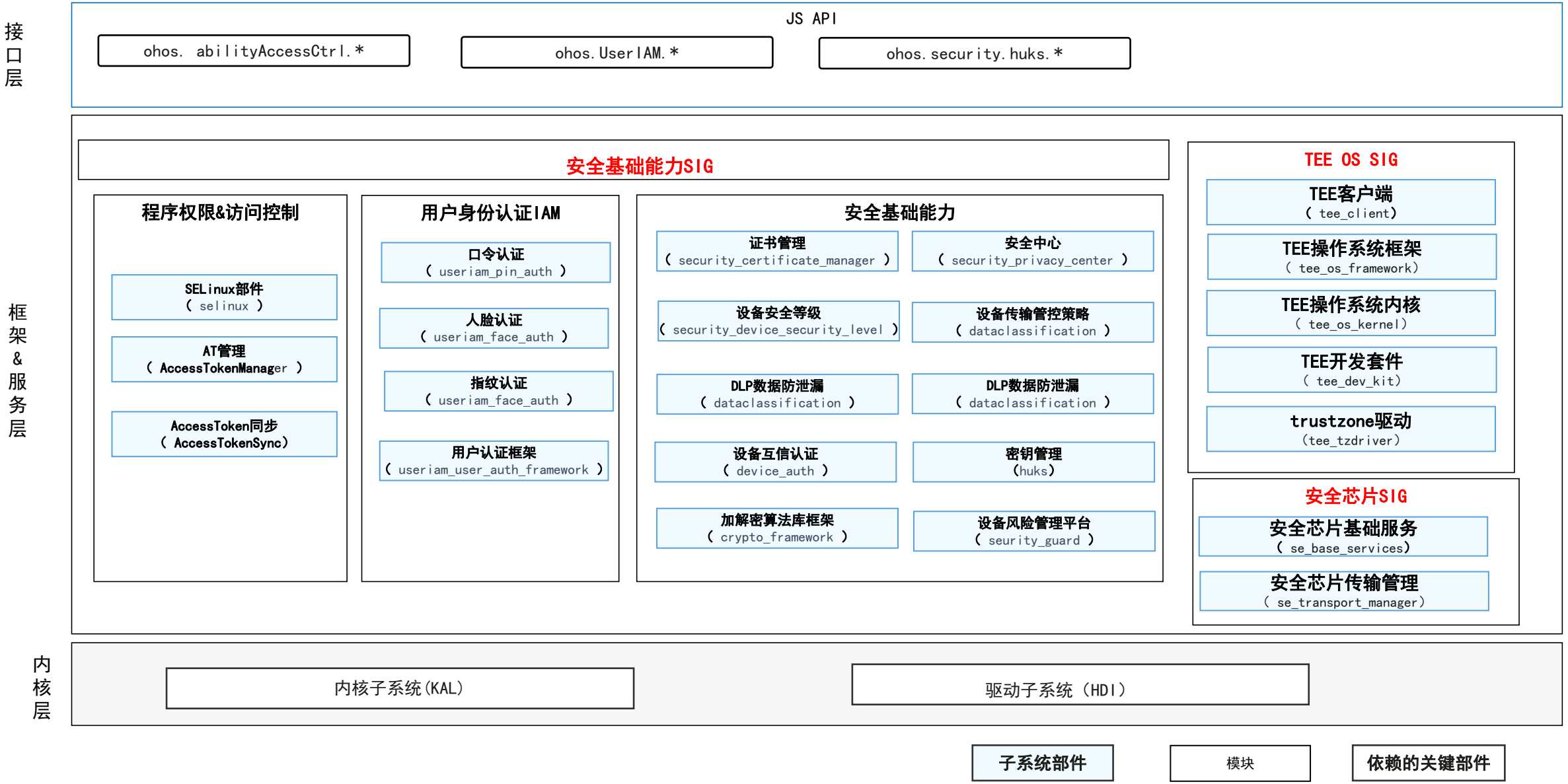
OpenHarmony安全能力进展及路标

社区化开发（LTS正式版）	OpenHarmony 2.0 开源首版本Canary版本	OpenHarmony 3.0 Release版发布	OpenHarmony 3.1 Release版发布	OpenHarmony 3.2 Release版本	OpenHarmony 4.0 Release版本
轻量IoT产品开发 如智能家电控制类设备，行业控制类设备，弱交互类穿戴设备等	增强设备UI交互能力 社区带屏开发板发布	轻量带屏家电开发 安全能力：内存隔离，驱动隔离，权限管理，密钥管理，设备互信认证等	富设备OS基础能力 安全能力：密钥管理（常用算法），统一身份认证框架，访问控制，设备互信认证，系统安全增强等	富设备OS安全能力持续迭代 安全能力：密钥管理（增强），证书管理，身份认证（Pin&人脸），权限和访问控制，设备安全分级，数据分级，设备互信认证，TEE框架（SIG孵化中）等	富设备OS安全能力持续迭代 安全能力：身份认证（指纹），认证控件，安全控件，TEE内核（社区共建），代码签名&代码执行权限管控、安全芯片管理和服务框架（SIG仓孵化）等

轻设备（轻量系统，小型系统）安全能力Ready

富设备（标准系统）安全能力持续构建

Openharmony社区安全SIG技术栈全景图



目录 Contents

OpenHarmony安全基础能力介绍

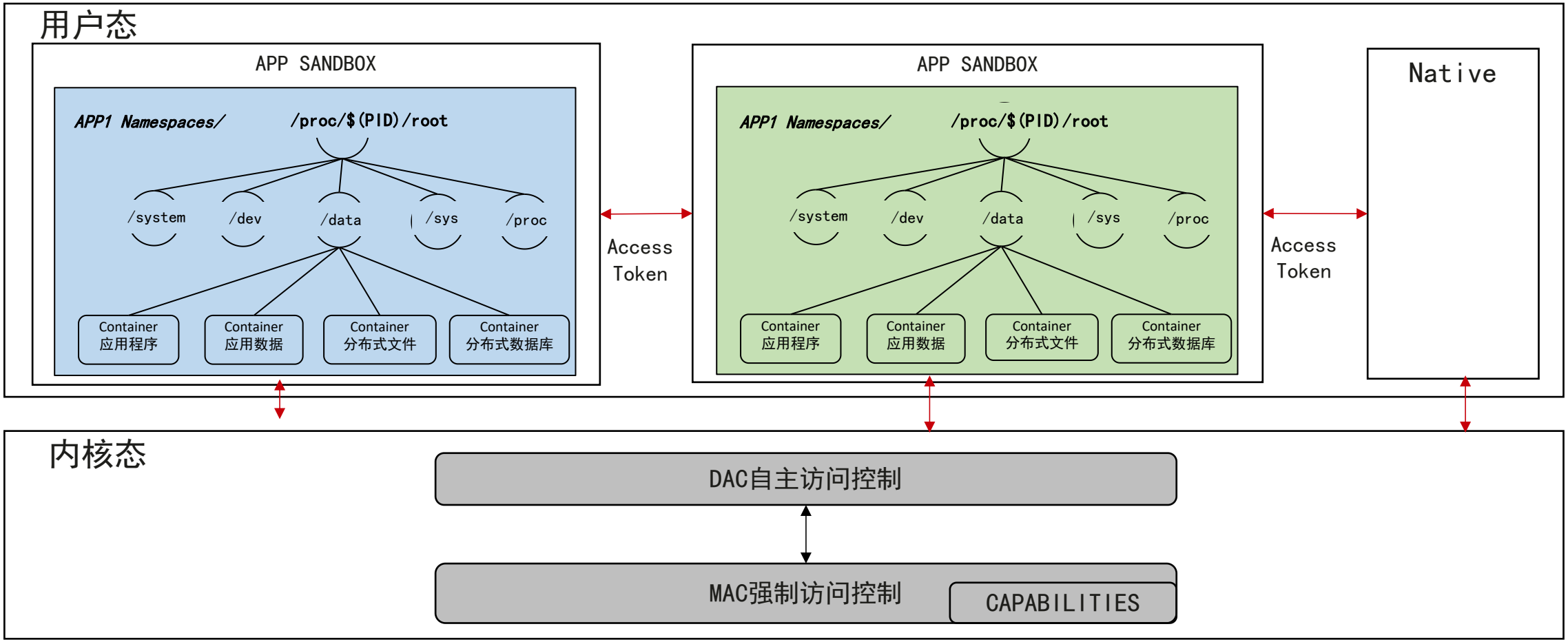
OS安全基础能力

为南向资源和北向应用提供基本的安全机密性、完整性安全保护基础能力

1. **隔离及访问控制：**对系统公共资源进行隔离，保持应用间独立、有序、可控的使用系统资源
2. **密码算法及密钥管理：**提供密钥生命周期（生成、交换、存储、使用、销毁、更替）安全保护能力
3. **设备互信认证：**实现设备可信关系建立、可信关系认证，以达到组成可信超级虚拟终端的目的
4. **数据分级保护：**在数据生成、存储、使用、传输、销毁等全生命周期提供分类分级的隐私安全保护
5. **可信执行环境：**提供一个可信的隔离运行环境，即使系统被攻破，也能保护高安全级别数据的完整性和机密性
6. **安全芯片管理框架：**提供统一的安全芯片管理框架机制，降低芯片接入成本，提高总体生态设备安全性。

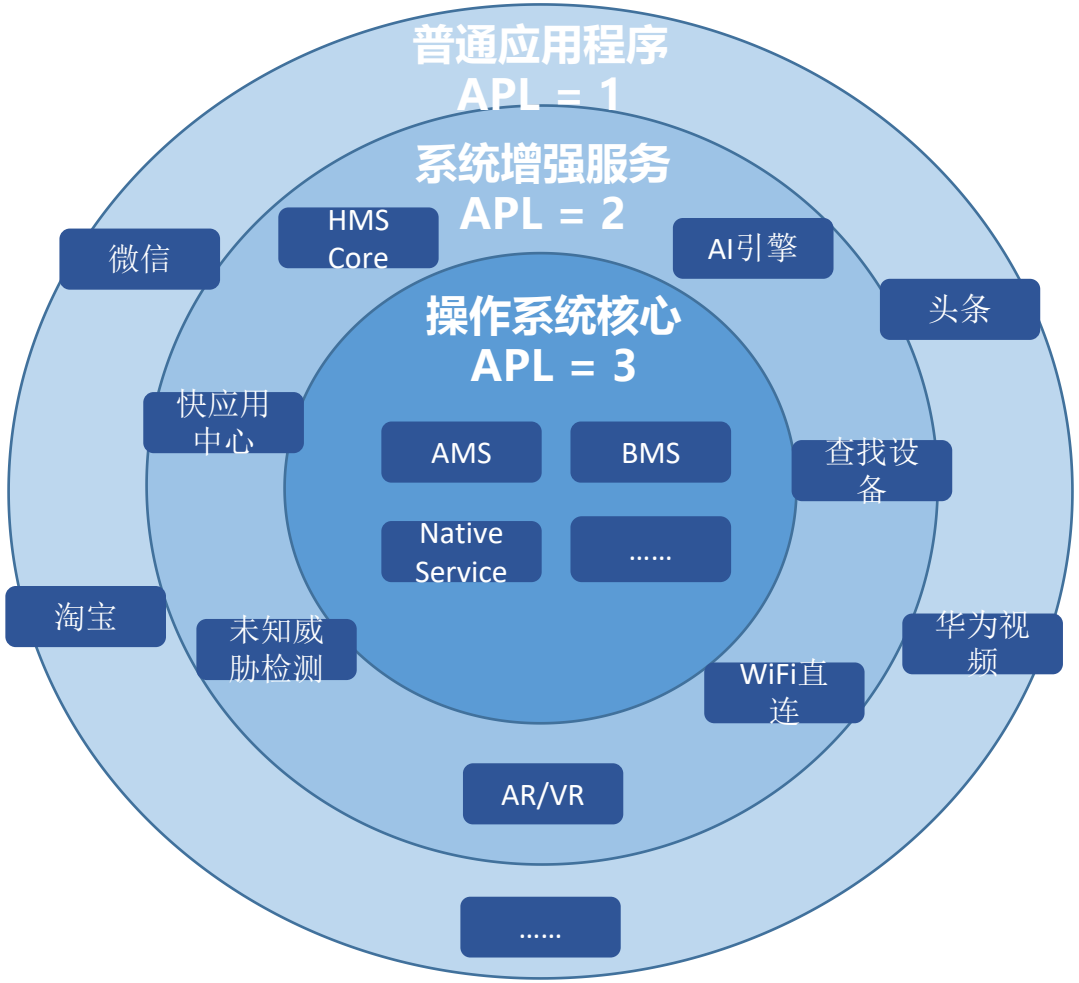
隔离与访问控制架构：应用沙盒到分级的权限访问控制

- 应用程序沙盒化管理，应用沙箱间通过namespace机制隔离，系统服务和应用间数据通过UGO机制隔离采用
- 分级的“洋葱”模型管控应用权限访问控制
- 基于DAC/MAC的主客体访问控制框架



基于AT Token的程序分级“洋葱”访问控制模型

基于洋葱模型，按照APL维度，严格定义三层等级：OS核心APL3，系统增强服务APL2，应用程序APL1，实现严格的分层保护，外部的应用如果需要访问内部的权限，默认无法访问。通过严格的分层权限保护模型，可以有效抵御恶意攻击，确保系统安全可靠



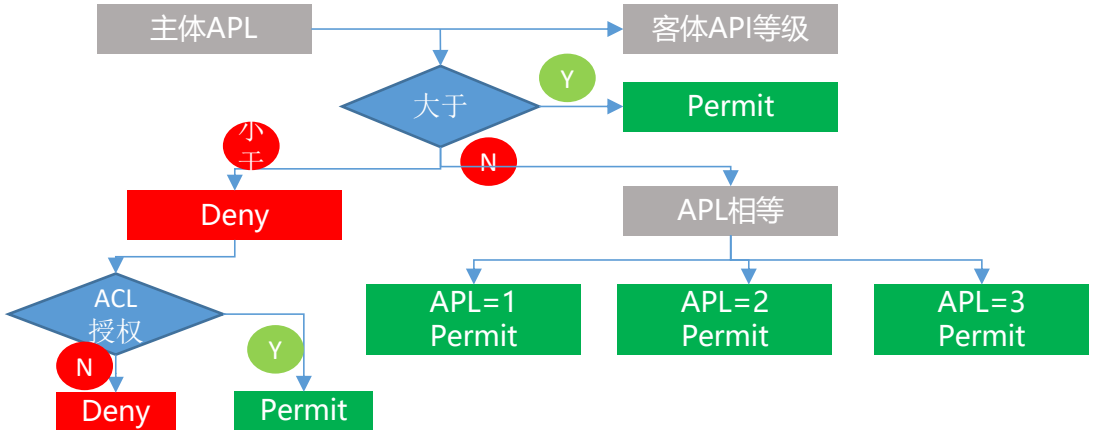
权限分配原则

- **操作系统核心能力APL=3：**
  1、属于最小系统，无此能力系统无法正常运转，如AMS、BMS、DMS、软总线
  2、作为整个应用程序的TCB，拥有较高特权，要求TCB最小化
  3、禁止应用、业务类程序申请
  4、可访问所有API接口，不对API权限进行限制
  5、减少攻击面，禁止应用申请联网能力

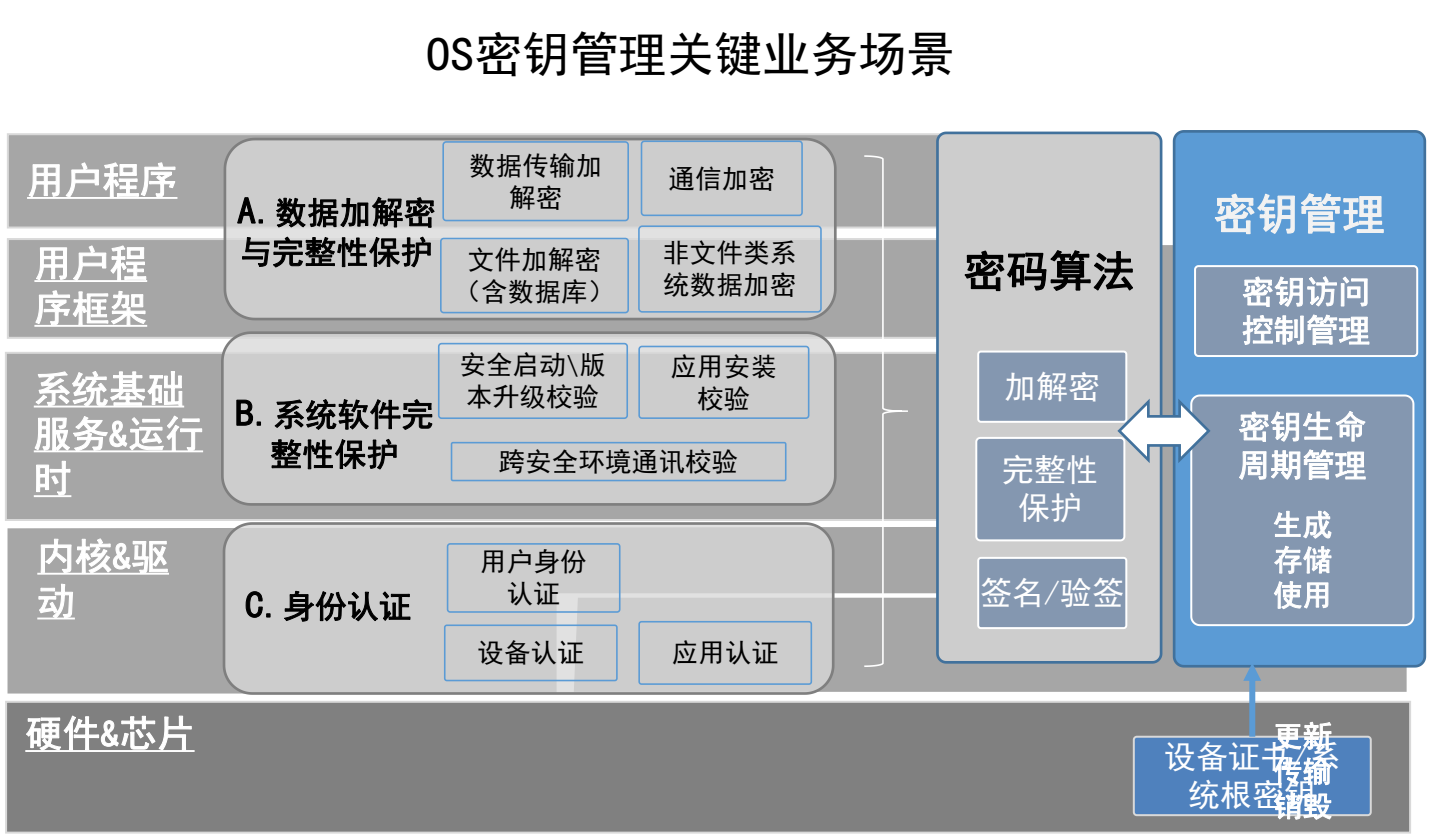
- **系统增强服务APL=2：**
  1、在操作系统核心能力基础上，仅操作系统能提供的增强服务，如情景感知、查找设备
  2、开放部分特权给HMS，经过HMS封装后HMS更好的为普通应用服务
  3、不对外开放的增强服务，如语音助手应用拉起能力，服务中心安装能力等。

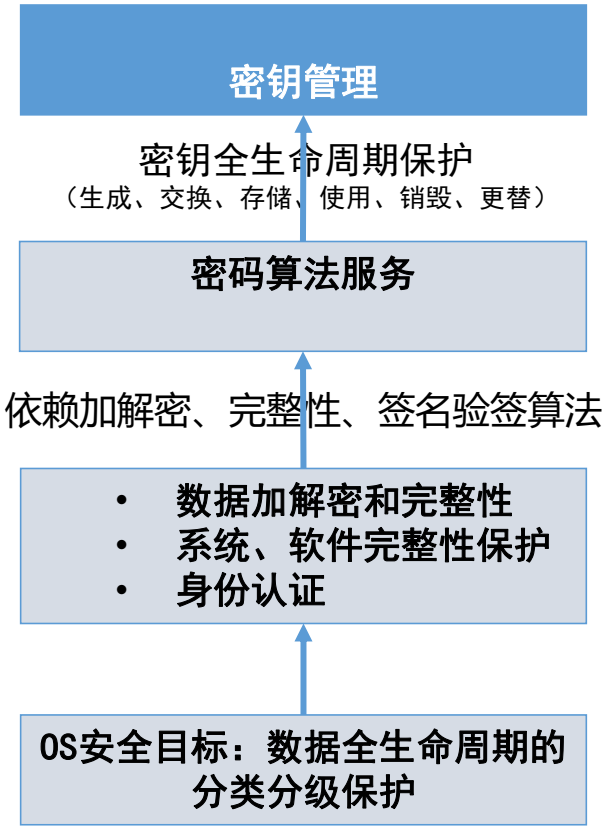
- **普通应用程序APL=1：**
  1、一切应用程序都是APL=1
  2、禁止应用程序申请高等级特权
  3、如果需要特殊权限，以API的权限申请解决

权限访问控制原则



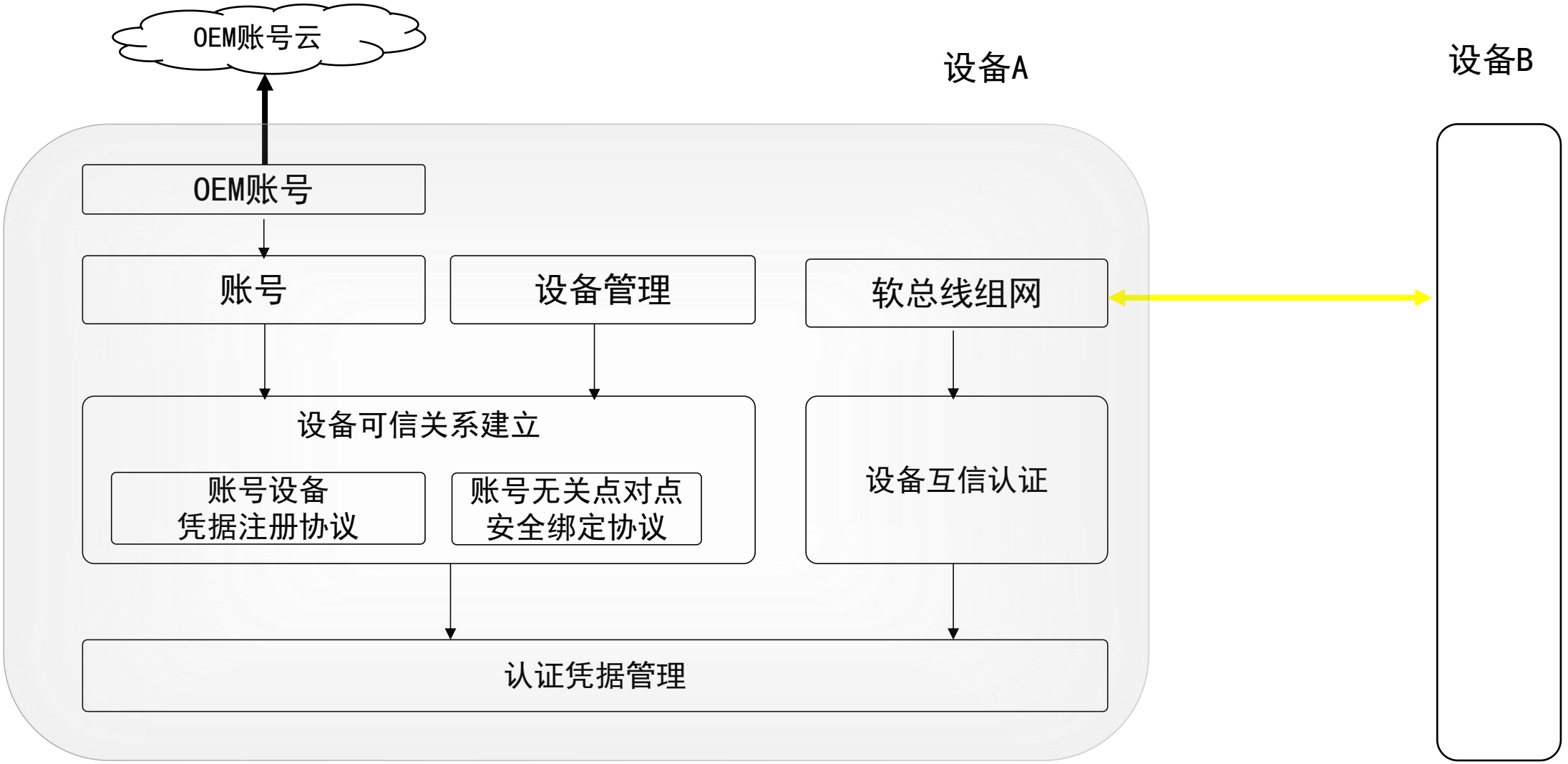
密钥管理：提供密钥生命周期安全保护能力





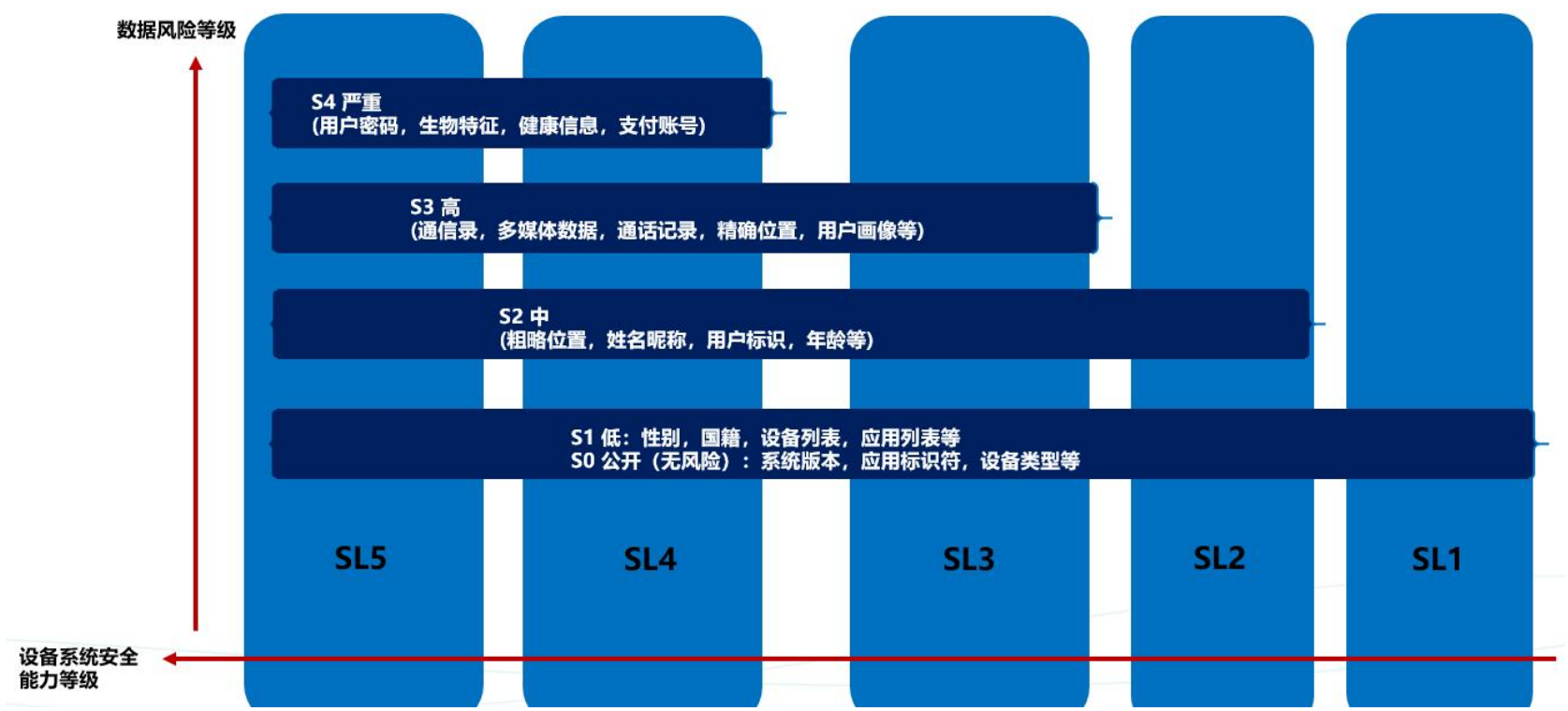
已经完成密钥管理基础框架，以及常用算法交付。部分非常用算法、密钥访问控制增强能力还在持续构建中

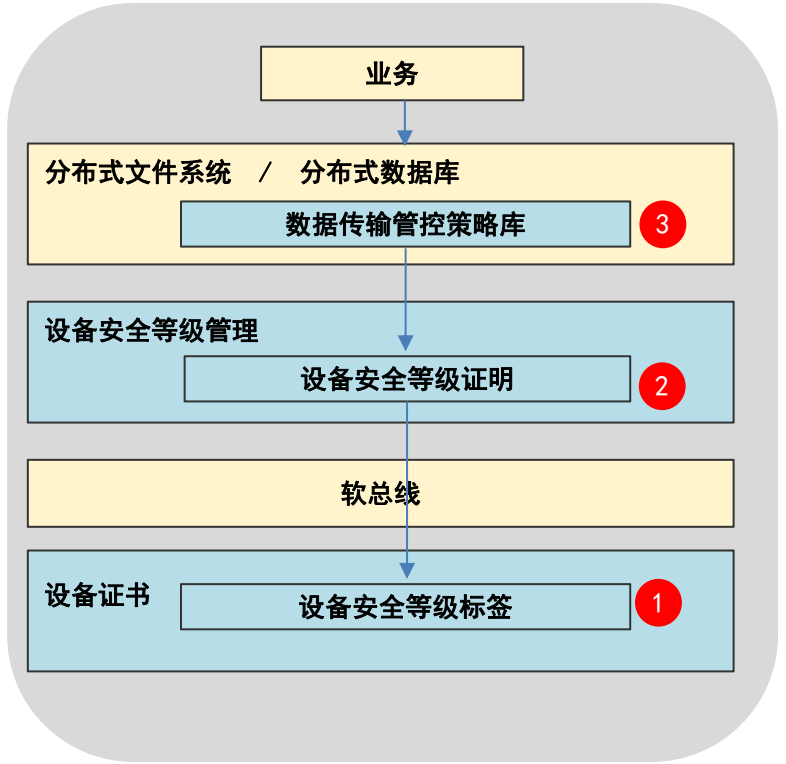
设备互信认证：设备可信连接，组成超级虚拟终端



分布式数据传输：基于设备和数据分级的数据传输管控

分布式数据传输挑战：数据跨设备传输需要保证不同等级设备对数据提供对应安全强度的保护，以保证只有正确的设备可以接受‘正确的数据’





1 设备安全等级标签

- 根据设备安全等级规范，设备出厂时具有设备安全等级标签

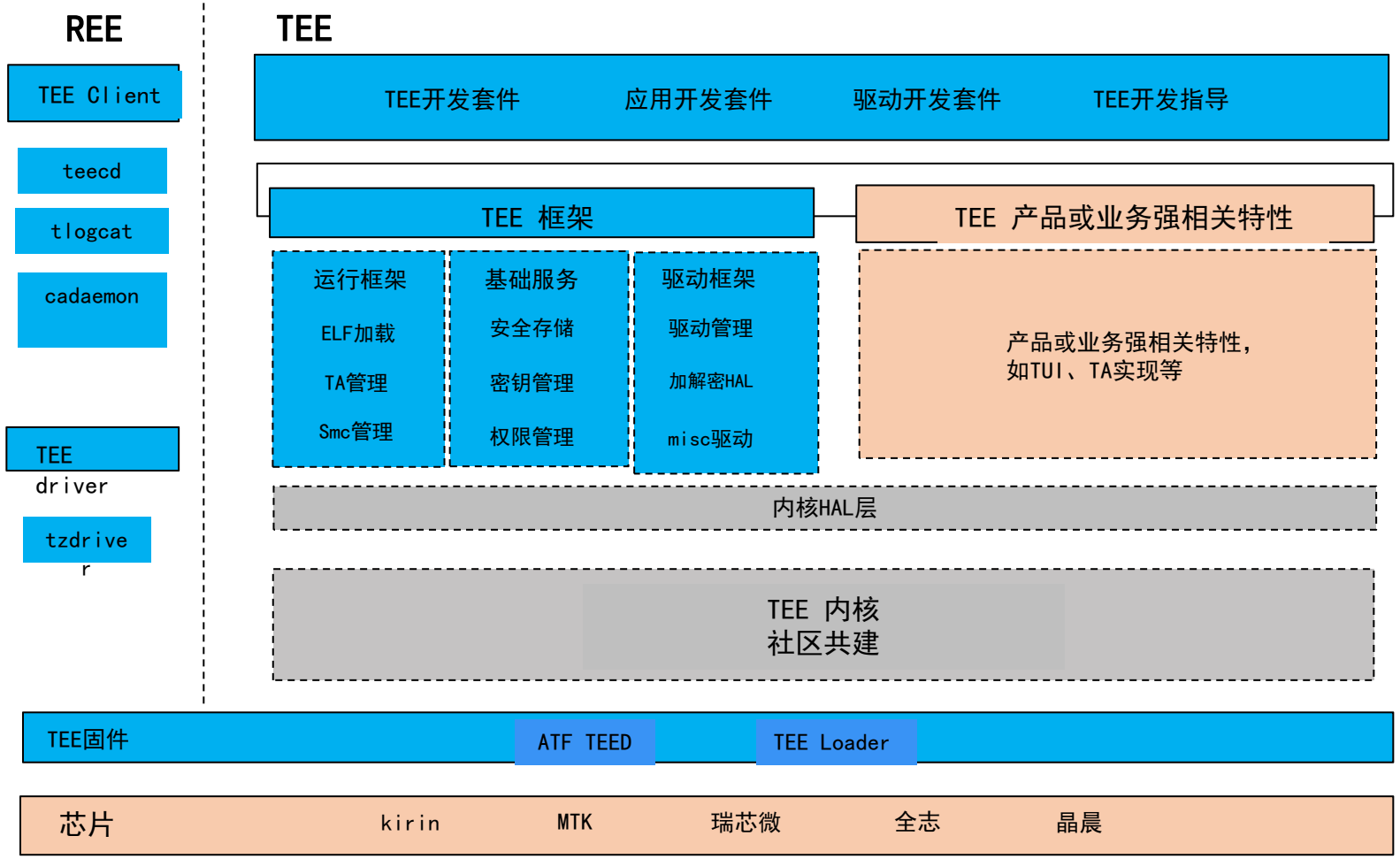
2 设备安全等级证明

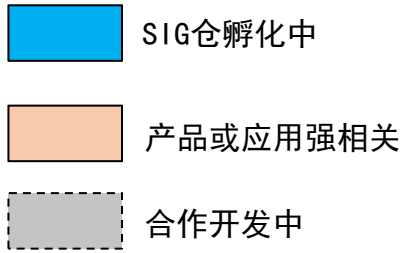
- 组网内设备间交互证明自己的设备安全等级

3 数据传输管控统一策略库

- 基于数据分级、设备安全分级，制定统一传输管控原则，并基于原则实现管控策略

可信执行环境：TEE整体架构&社区构建进展



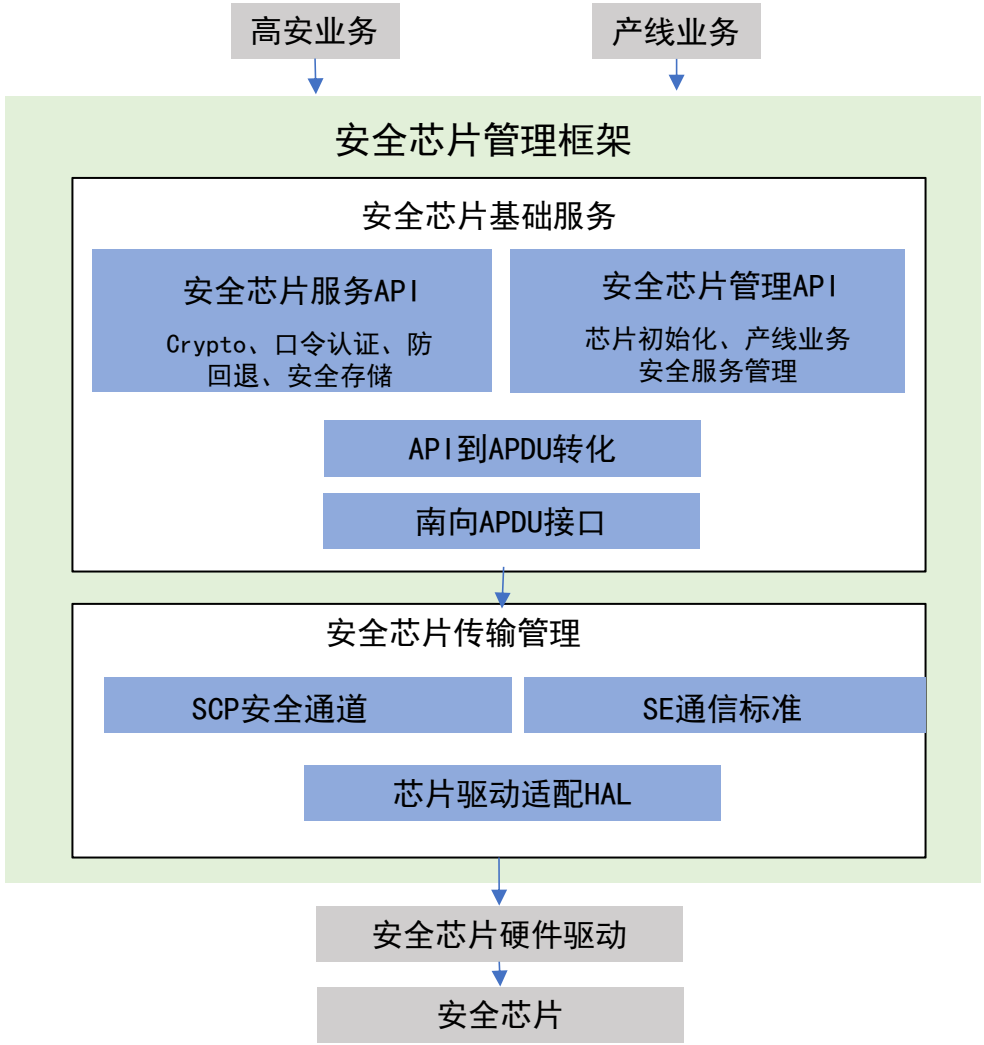


可信执行环境安全底座：

- 实现统一的TEE 框架、TEE工具、TEE client等生态接口能力，避免出现TEE生态碎片化问题；
- 社区后续制定标准规范，统一Openharmony标准。

可信执行环境框架能力在持续构建中，TEE框架、TEE工具、TEE client能力在TEE SIG仓孵化中，TEE 内核正在共建

安全芯片管理架构



OpenHarmony 安全芯片能力：

✓ **提供统一安全芯片管理框架，统一API及APDU规范**

- 基于统一的安全芯片管理框架，便于业务快速接入
- 支持安全芯片厂商快速接入安全芯片管理框架

✓ **为高敏感核心业务提供芯片级的高安全能力（待构建）**

- 标准化口令认证
- 密钥管理、安全存储、防回退等系统安全服务能力

OpenHarmony 社区交付件：

➢ **北向业务生态和南向芯片生态标准规范（待购建）**

- 《OpenHarmony SE 管理框架通用规范》
- 《OpenHarmony SE 高安服务 API 规范》
- 《OpenHarmony SE 高安服务 APDU 规范》
- 《OpenHarmony SE Applet 功能规格及测试用例》

➢ **管理框架及开源实现（持续构建）**

- 向北向业务提供安全芯片基础服务
- 提供安全芯片传输管理
- 向南向芯片厂商提供硬件驱动适配层HAL的相关实现

安全芯片管理框架能力在持续构建中，框架能力暂未开源，计划先在安全芯片SIG仓孵化

OpenHarmony

THANK YOU

扫描二维码 关注官方公众号

【官网网址】www.openharmony.cn