HUAWEI

< HDC.Together >

HUAWEI DEVELOPER CONFERENCE 2021

如何开发安全的OpenHarmony兼容设备？

1 OpenHarmony的安全设计理念

2 基于OpenHarmony设备生命周期的安全开发

安全设计理念：正确的人，通过正确的设备、访问正确的数据

正确的人

- 在分布式设备上安全、便捷地认证人的身份

正确的设备

- 正确的安全级别的设备
- 正确的设备合法性授权

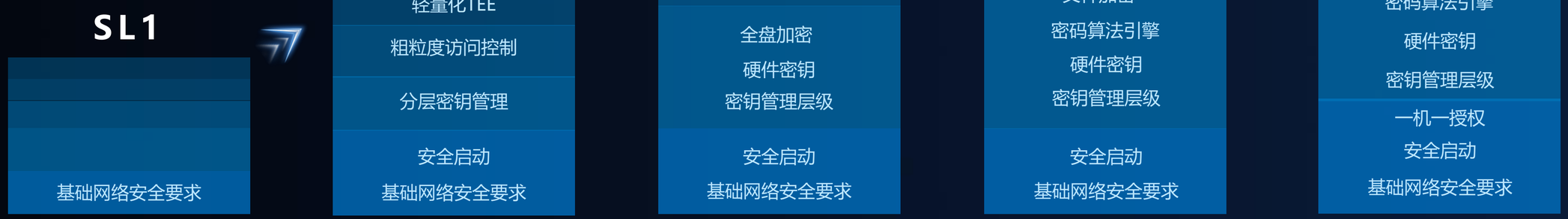
正确的数据

- 数据分类分级，确保数据在1+8+N上获得对应等级的保护

正确的设备安全分级：运行环境安全

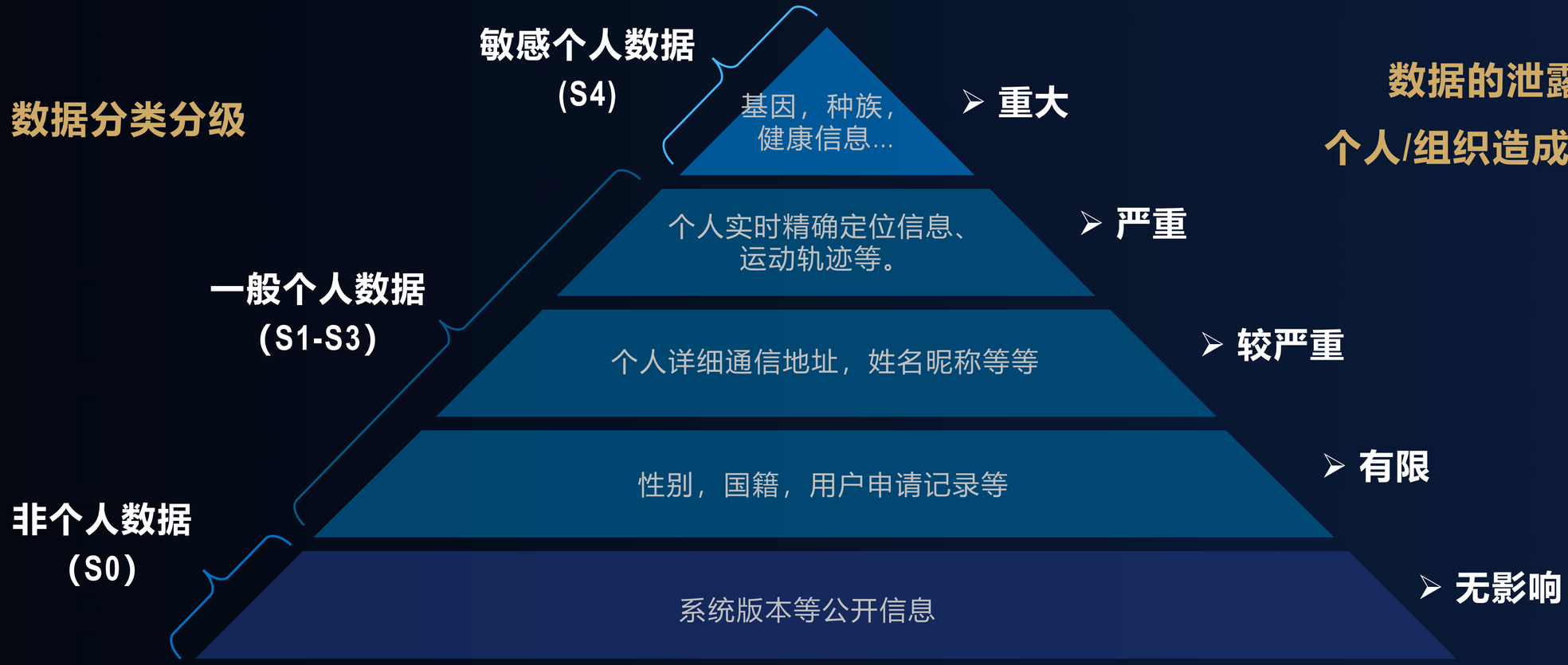
划分设备安全等级

对应安全能力要求



基础保护 **受控保护** **结构化保护** **安全域保护** **验证安全设计**

正确的数据分级分类：基于法律法规 对数据分类分级



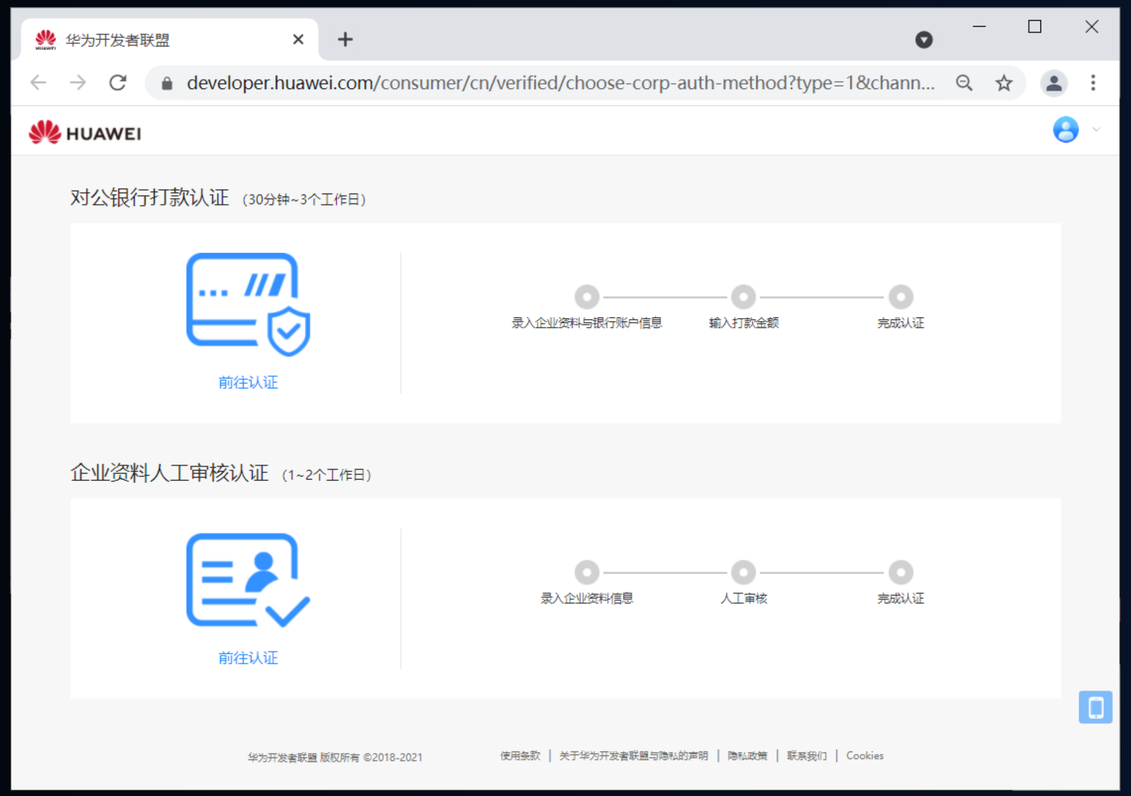
1 OpenHarmony的安全设计理念

2 基于OpenHarmony设备生命周期的安全开发

开发者OpenHarmony设备开发、发布及生命周期管理的安全

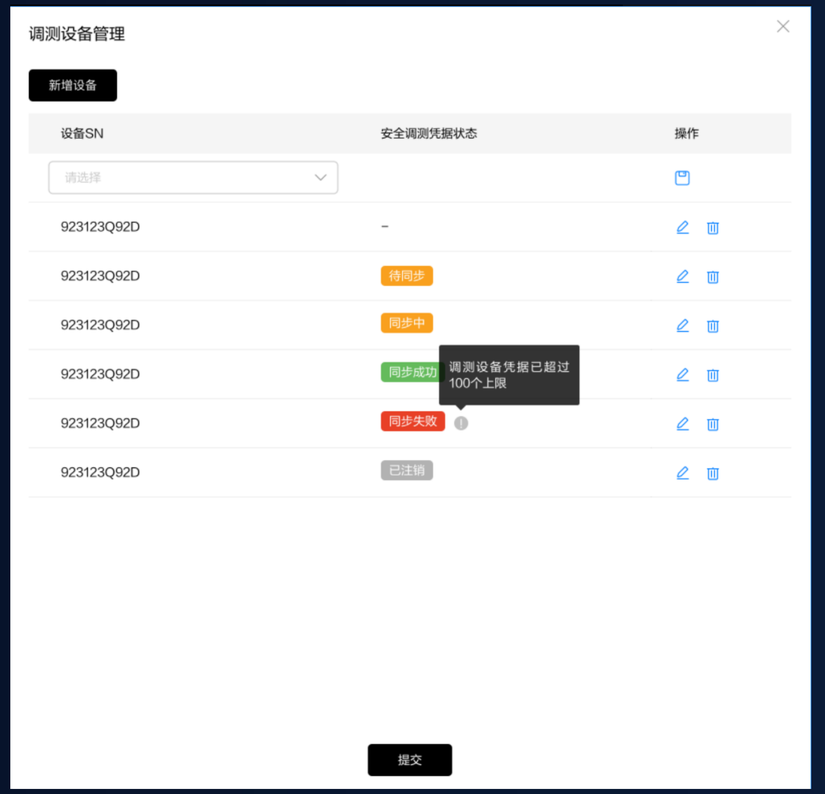
准备阶段：注册审核企业开发资质&登记开发调测设备授权

审核企业资质



审核企业资料1~5个工作日

注册登记调测设备



只有注册的设备能作为开发调测设备使用

合作伙伴管理平台 http://devicepartner.Huawei.com

开发阶段：代码安全检查

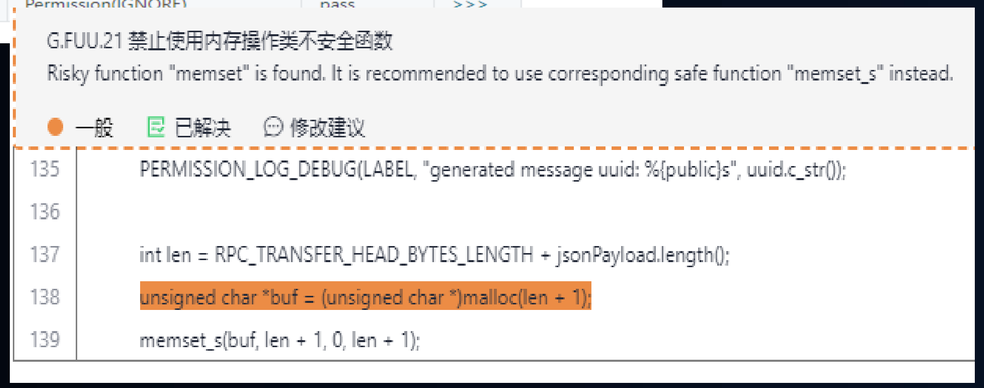
静态：开源社区全量代码例行静态扫描

openharmony_ci 成员 2 小时前

代码门禁未通过
静态检查:

#	check type	result	report
1	codeCheck	failed	>>>
2	CodingStyleCheck_CPP(IGNORE)	warning	>>>
3	CodingStyleCheck_C(IGNORE)	warning	>>>
4	Cmetrics(IGNORE)	pass	>>>
5	Codemars_C(IGNORE)	pass	>>>
6	开源扫描(IGNORE)	interception	>>>
7	Buildmc(IGNORE)	pass	>>>
8	Permission(IGNORE)	pass	>>>

编译构建过程，自动完成安全编码扫描



G.FUU.21 禁止使用内存操作类不安全函数
Risky function "memset" is found. It is recommended to use corresponding safe function "memset_s" instead.

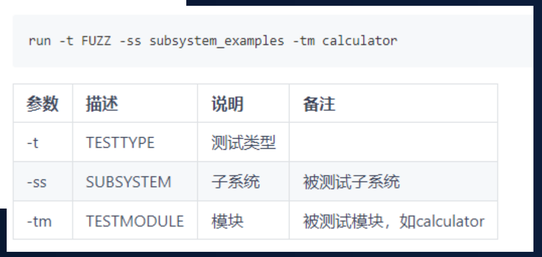
一般 已解决 修改建议

```
135     PERMISSION_LOG_DEBUG(LABEL, "generated message uuid: %{public}s", uuid.c_str());
136
137     int len = RPC_TRANSFER_HEAD_BYTES_LENGTH + jsonPayload.length();
138     unsigned char *buf = (unsigned char *)malloc(len + 1);
139     memset_s(buf, len + 1, 0, len + 1);
```

动态：高风险模块提供Fuzz测试支撑

测试框架Fuzzing安全测试指导

- Fuzzing简介
- Fuzzing测试关注的风险接口
- 使用测试框架DTFuzz
  - 配置启动测试框架
  - 单个Fuzz用例初始化
  - Fuzz用例编写
  - Fuzz用例编译
  - Fuzz用例执行
- 测试结果与日志



```
run -t FUZZ -ss subsystem_examples -tm calculator
```

参数	描述	说明	备注
-t	TESTTYPE	测试类型	
-ss	SUBSYSTEM	子系统	被测试子系统
-tm	TESTMODULE	模块	被测试模块，如calculator

预计开放Fuzz测试用例100+

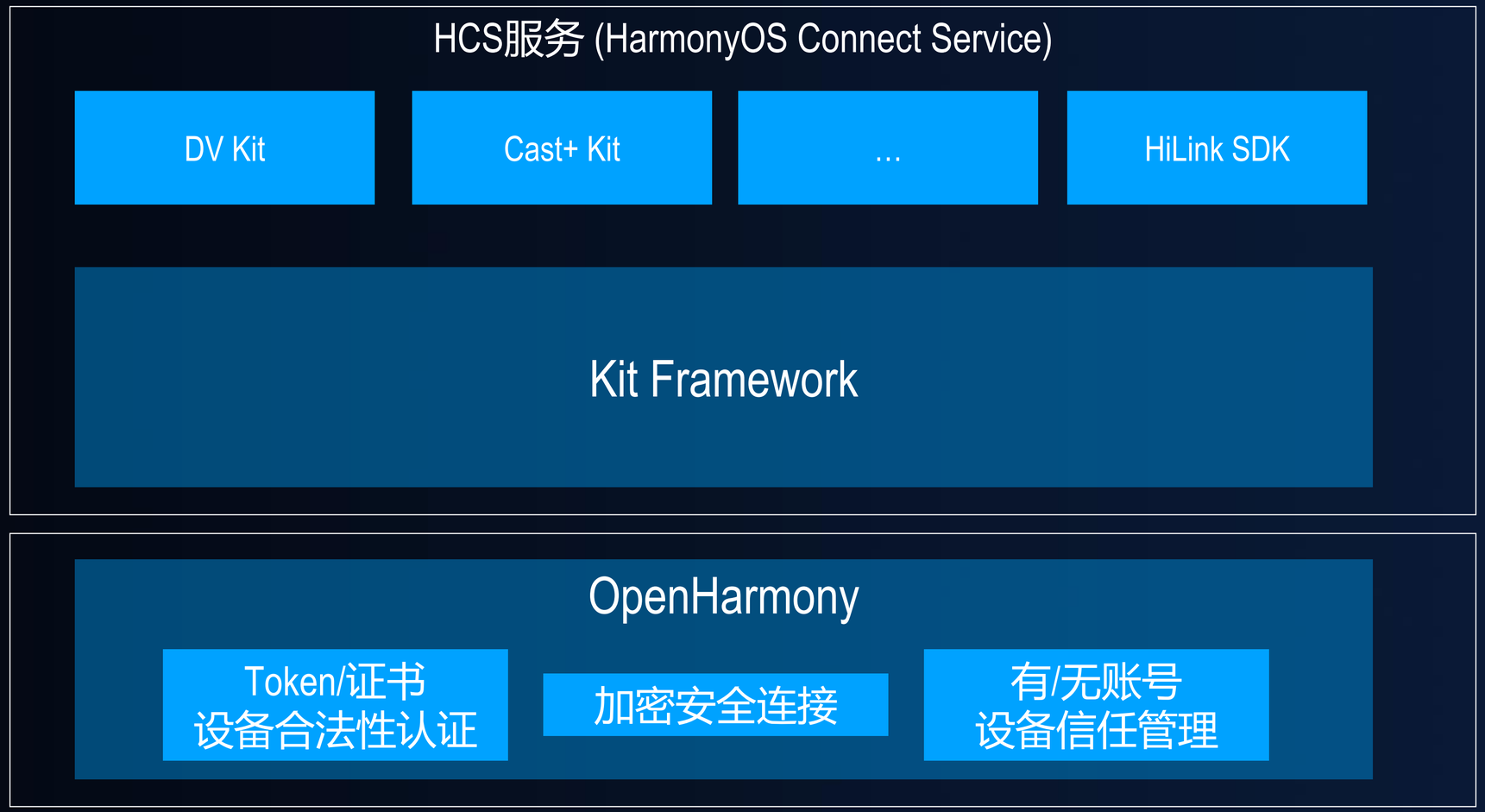
音视频、图片解码处理

分布式交互中蓝牙、WIFI等数据协议处理

设备内跨信任域数据访问，用户态访问内核

开发建议：针对处理外部数据的C/C++高风险模块开展白盒Fuzz，消减内存访问越界等安全编码问题

开发阶段：设备集成Kit的安全



HCS Service→ 嵌入并使能设备业务安全

开发阶段：集成设备合法性授权开发

集成方式1：设备Token开发与集成：

- 用于对安全要求一般的设备合法性授权场景
- 在合作伙伴管理平台申请Token
- 预留专属Token存储区（1K）；要求：不可擦除，专属访问接口，防止非法访问和篡改

设备厂商实现Token相关接口：

接口名	接口原型	接口说明
读取token	int ReadToken(char *token, unsigned int len);	0：返回成功，表示是否是更新区域的token，1：返回成功，表示是否是返回预制token；-1：返回失败；-2：厂家无预制token错误；
更新token	int WriteToken(const char *token, unsigned int len);	存储token数据，如果成功返回0，错误返回-1；
获取AcKey	int GetAcKey(char *acKey, unsigned int len)	获取AcKey数据，如果成功返回0，错误返回-1；AcKey是华为与CP伙伴之间的共享秘钥。每个CP伙伴唯一
产品型号	int GetProdId(char productId[], size_t len)	prodId 5bytes的值，如果成功返回0，错误返回-1；OEM厂商从Partner网站认证的时候华为分配。
产品密钥（可选）	int GetProdKey(char prodKey[], size_t len)	prodKey是内存buffer，函数实现需要返回CP伙伴从华为合作伙伴服务中心中获取到的该型号产品所对应的ProdKey实际字符串内容（base64编码，含字符串终结符）；如果成功返回0，错误返回-1；

集成方式2：PKI 设备证书开发与集成：

- 对于安全性要求高的设备的设备合法性授权场景
- 若设备有Trustzone或华为定义的安全芯片，可采用PKI证书的验证机制
- 要求Trustzone中有超过10KB的存储空间

接口名	接口原型	接口说明
读取key	int GetKeypair(char keypair[], size_t len);	HUKS调用
存储key	int WriteKeypair(char keypair [], size_t len);	HUKS调用
读取证书	int GetCertificate(char certificate[], size_t len);	HUKS调用
存储证书	int WriteCertificate(char certificate[], size_t len);	HUKS调用

开发阶段：设备安全检测，设备开发集成更高效安全

DevEco Testing

开发者

一键扫描

HarmonyOS

= 报告 + 修复建议

问题闭环，安全提升

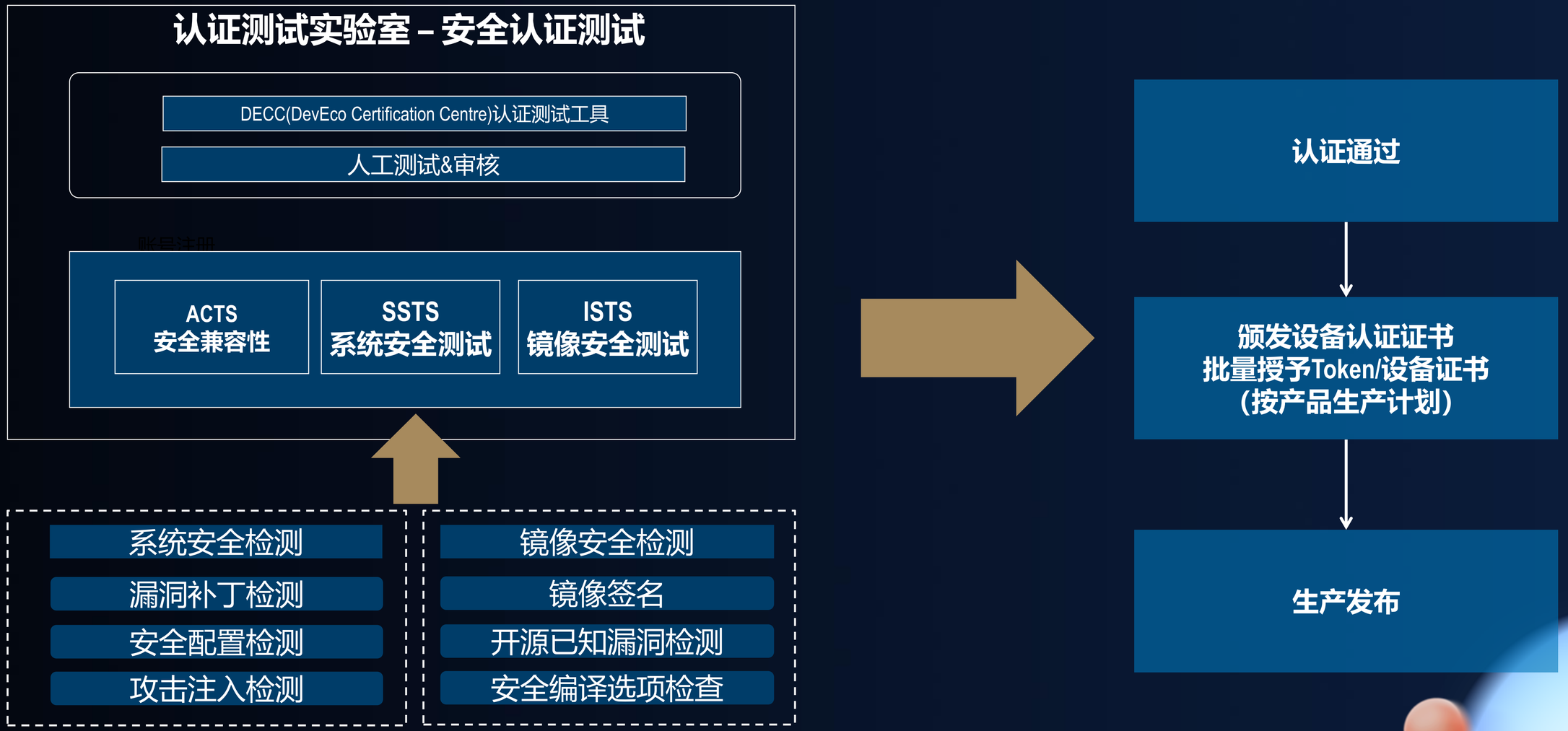
安全漏洞	安全配置	接口攻击注入	鸿蒙预认证(待上线)
•SPT安全级别 •已知漏洞扫描	•文件权限扫描 •预置敏感文件检测(Su等) •Selinux权限检测…	•SA系统服务 •内核接口 •网络接口…	•安全编译选项

✓ 系统一键扫描，护航产品安全，提升认证通过率。

https://devecotesting.huawei.com/

https://devecotesting.rnd.huawei.com/help?jobType=security

认证发布阶段： 安全认证测试 & 设备批量生产



运行阶段：设备可信连接，组成安全的超级虚拟终端

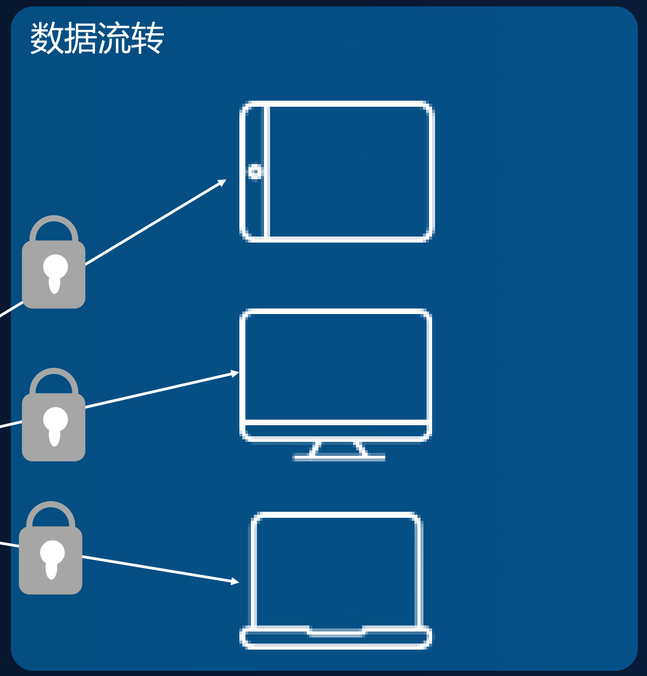
设备被正确的人绑定

安全的交换公钥凭据

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

设备间流转的数据仅正确的人可访问



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

开发指导：https://developer.harmonyos.com/cn/docs/

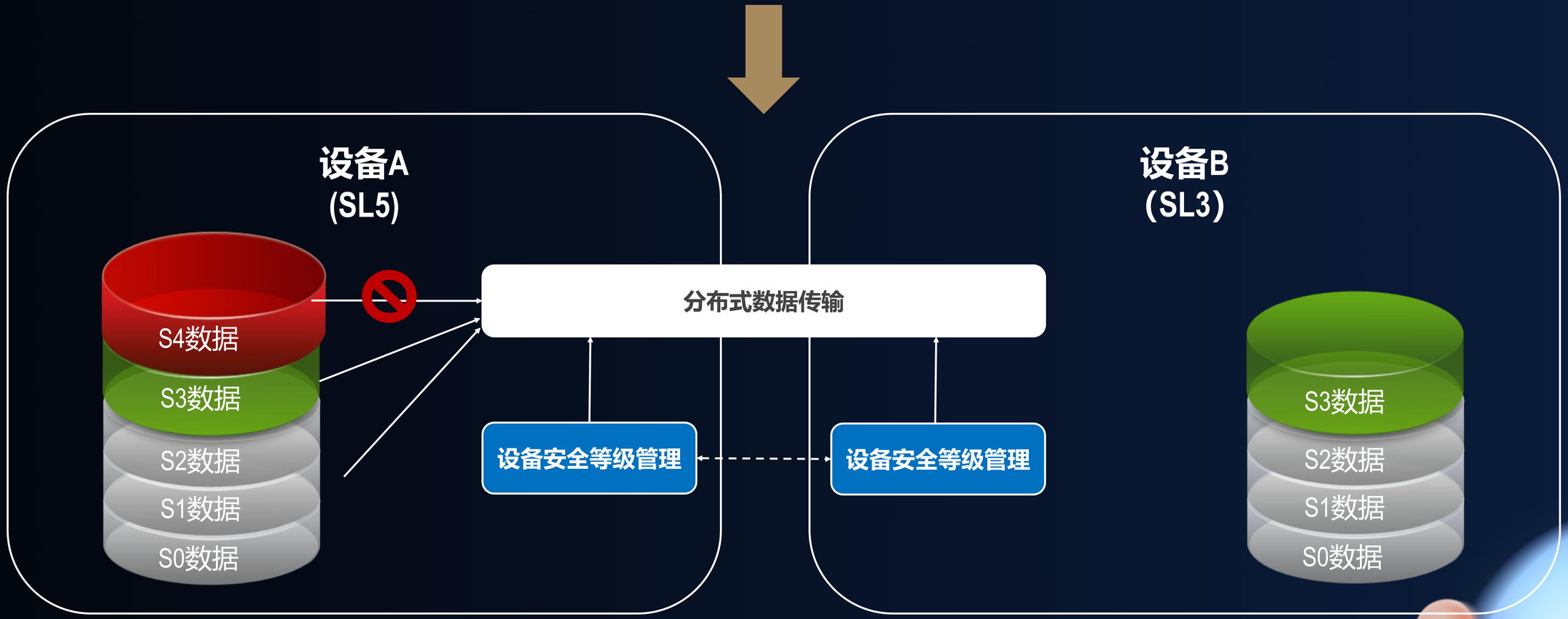
运行阶段：正确的数据获得正确的设备安全等级保护

数据生命周期

产生	存储	使用	传输
数据产生时根据标准进行分类并打上S0-S4标识	数据只能在满足其安全等级要求的设备上存储	满足安全等级要求的设备获得授权后才能访问	数据传输时端端加密

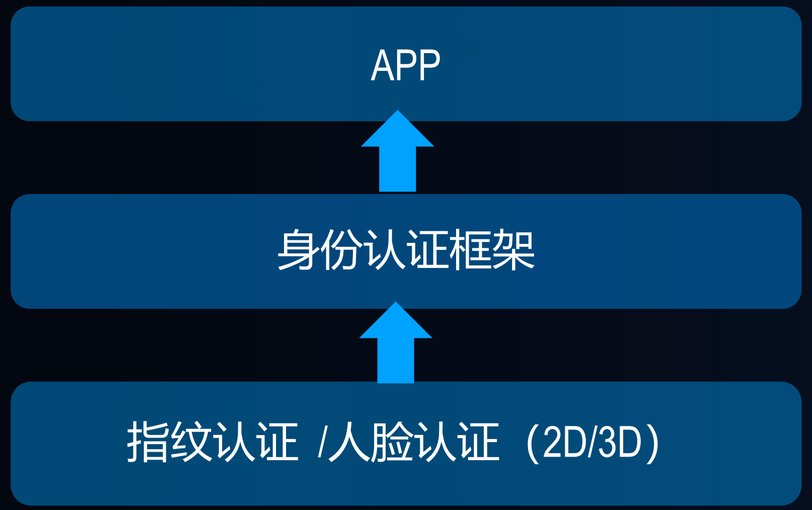
运行阶段：基于分级保护实现访问控制 正确数据流转

设备安全级别	SL5	SL4	SL3	SL2	SL1
数据等级	S0~S4	S0~S4	S0~S3	S0~S2	S0~S1



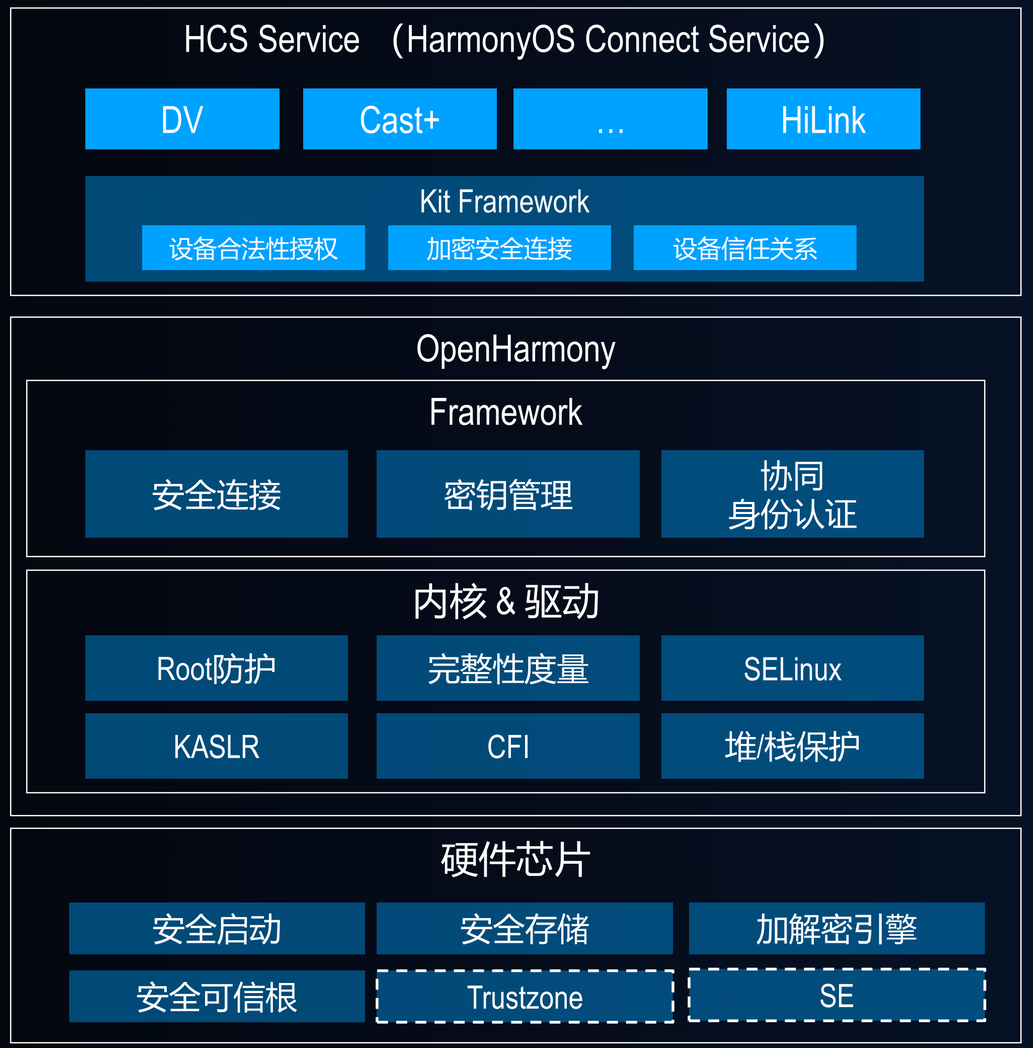
运行阶段：多类型身份认证，认证更便捷更安全

单终端：身份认证



超级终端：分布式协同认证

运行阶段：OpenHarmony嵌入安全功能



HCS Service→ 使能设备业务安全

- Kit Framework 接入时认证设备的合法性
- 只有合法的设备才能获取对应的Kit授权
- Kit结合Kit Framework建立安全的连接和信任关系

OpenHarmony→ 平台基础安全嵌入OS

- OpenHarmony OS内嵌系统的安全能力，具有非常好的内核安全防护能力
- 同时嵌入了HiChain、HUKS密钥管理、Token/设备证书的安全能力

硬件&芯片 → 提供可集成的安全硬件

- 芯片选型应具备硬件安全能力的芯片，如：安全启动、TEE可信安全环境等；
- 若主芯片不具备硬件安全能力，可选择集成华为安全套件的安全芯片

运维阶段：安全补丁 & 漏洞

安全补丁升级及或合作伙伴服务协议

HarmonyOS许可与分发协议

发布之日起两年内的设备型号90天内升级率需达到5%以上，新版本需带60天内的安全补丁

HarmonyOS合作伙伴服务协议

- **紧急安全补丁：发布之日起30天内向最终用户推送**
- **普通安全补丁：按照双方协议一致的时间给用户推送**

华为终端安全漏洞奖励计划

device.harmonyos.com/cn/docs/security/

级别	漏洞样例	奖金级别（人民币）
严重	通过分布式网络在远端设备特权进程执行任意代码； 通过分布式网络造成远端设备永久拒绝服务；	最高 1,000,000元
高	通过分布式网络在远端设备普通进程执行任意代码； 通过分布式网络获取远端设备受保护的数据（特权进程才能访问的数据）。	最高500,000元
中	通过分布式网络越权调用远端设备敏感接口； 通过分布式网络造成远端设备临时拒绝服务，导致设备挂起或者重新启动； 绕过部分用户交互开启或关闭通常由用户才能发起的功能； 分布式组网条件下绕过将应用数据与其他应用隔离开来的安全机制。	最高130,000元
低	通过分布式网络造成远端设备特权进程拒绝服务（不会导致设备重启，仅导致进程重启）。	最高13,000元

以上场景需满足如下条件之一：
1、从低级别设备攻击到高级别设备的场景；
2、从UID >10000进程攻击其他同安全级别设备。

*奖励计划具体以华为网站公布为准

*以上协议和漏洞奖励计划，仅针对华为自研的设备， 漏洞修复后会定期发布在OpenHarmony上修复

<HDC.Together>
华为开发者大会2021

扫码参加1024程序员节

<解锁HarmonyOS核心技能，赢取限量好礼>

开发者训练营

Codelabs 挑战赛

HarmonyOS技术征文

HarmonyOS开发者创新大赛

扫码了解1024更多信息

报名参加HarmonyOS开发者创新大赛

谢谢

欢迎访问HarmonyOS开发者官网

欢迎关注HarmonyOS开发者微信公众号