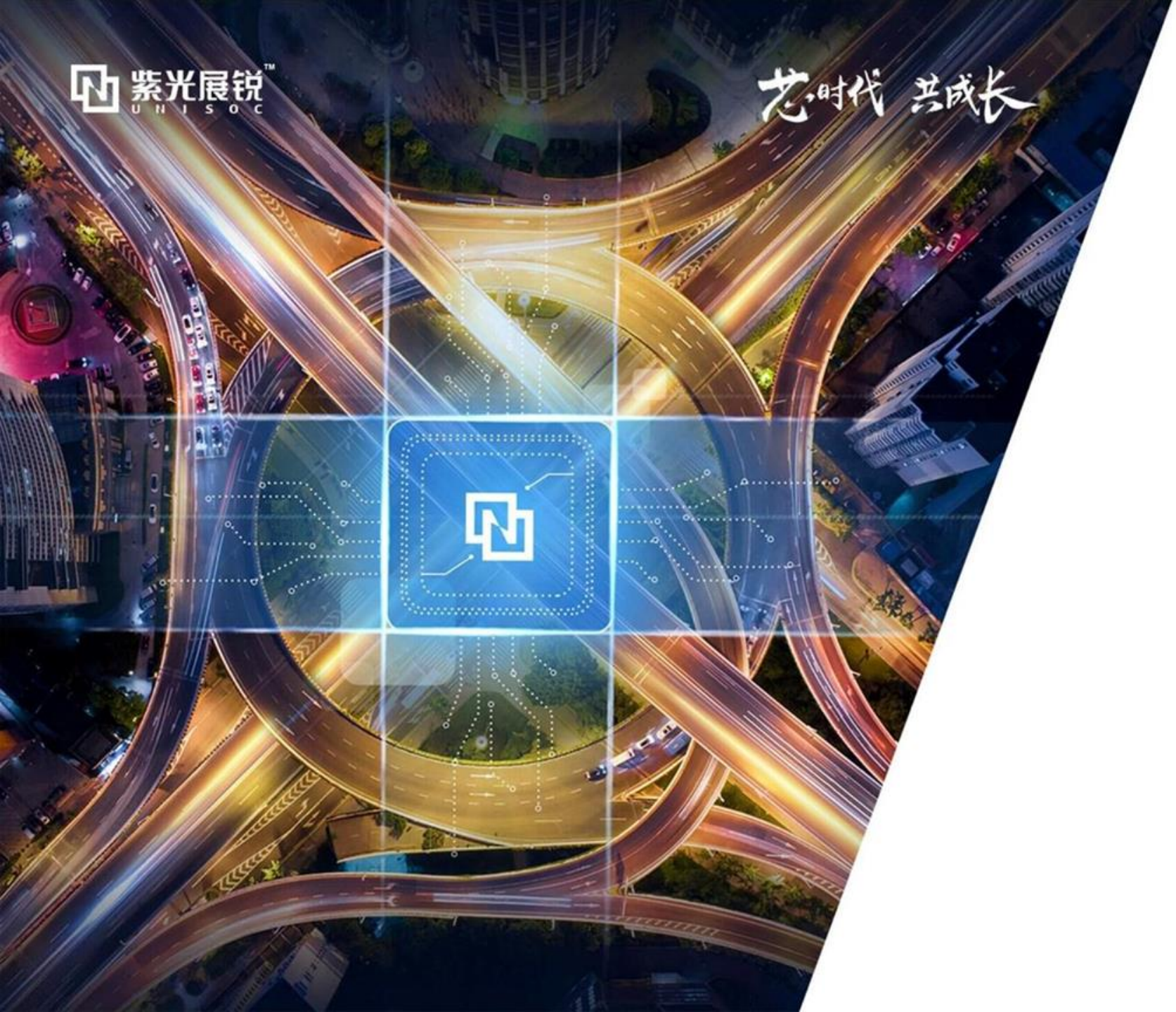


FBE 流程简介

修改历史 Revision History

版本号 Version	日期 Date	注释 Notes
V1.0	2019/12/09	初稿

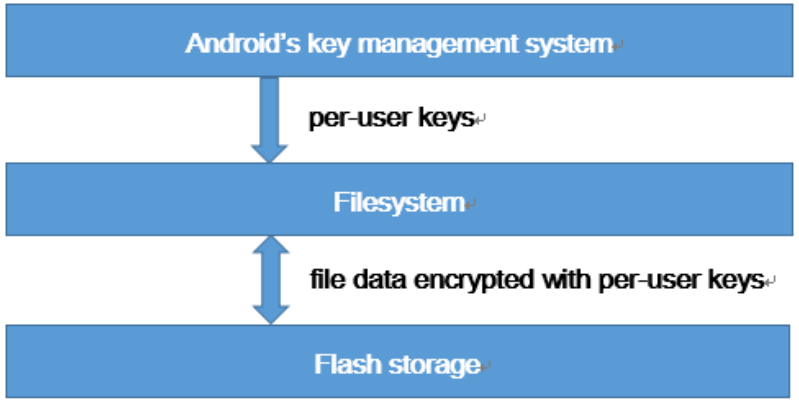
文档信息 Document Information

适用产品信息 Chip Platform	适用版本信息 OS Version	关键字 Keyword
SC9863A，SC9832E，SC7731E(1G)，SL8541E，UMS312，T7510	Android 9.0\Android 10.0	文件级加密 File-Based Encryption FBE

Contents

FBE（File-Based Encryption）

- **存储加密**
  - 存储加密是使用对称密钥对Android设备上所有用户数据（主要指data分区）进行编码的过程
  - 对于开启存储加密的设备，保存在磁盘上的数据始终是加密状态
    - ✓ 用户数据在写入磁盘之前加密
    - ✓ 读取操作在将数据返回给调用进程之前解密
- **Android存储加密方式**
  - 全盘加密（FDE）
  - 文件级加密（FBE）
  - Google要求搭载Android 10及更高版本的新设备使用FBE（Google CDD）
- **FBE**
  - 使用不同的密钥对不同的文件/目录进行加密，文件系统获取相应密钥后可以单独解密
  - 基于在文件系统层运行的Linux内核功能fscrypt，实际的加解密流程在文件系统I/O操作中
  - 目前只加密文件名和文件内容，文件系统元数据（目录结构、文件大小、权限和创建/修改时间等）不加密
    - ✓ 借助采用 XTS 模式的 AES-256 算法加密文件内容
    - ✓ 借助采用 CBC-CTS 模式的 AES-256 算法加密文件名



FBE 关键概念

- **加密目录**
  - 系统目录
    - ✓ 用于保存系统运行相关数据，由init进程执行mkdir创建
  - 用户目录
    - ✓ 凭据加密（CE）目录：默认存储位置，只有在用户解锁设备后才可用
    - ✓ 设备加密（DE）目录：直接启动模式期间以及用户解锁设备后均可用
    - ✓ 每个用户都有对应的CE和DE目录

FBE 关键概念

- **加密密钥**
  - 主密钥
    - ✓ 每个加密的目录树是由一个64 byte的主密钥来保护，主密钥并不直接参与实际的文件内容和文件名加密
    - ✓ 在读写加密目录前，用户空间必须首先将主密钥添加至内核密钥环（kernel keyring），密钥类型必须是”logon”，该类型的密钥保存在kernel的内存中而不能被用户空间回读
    - ✓ 用户空间进程vold（Volume Daemon）负责派生主密钥，并通过系统调用add_key() 将密钥传递给kernel keyring
  - 文件系统派生密钥
    - ✓ 用于实际数据加密时用的密钥通过主密钥和16 Byte随机数使用AES-128-ECB加密派生生成，长度为64 Byte
    - ✓ 这部分派生密钥逻辑在内核fscrypt中实现

FBE 关键概念

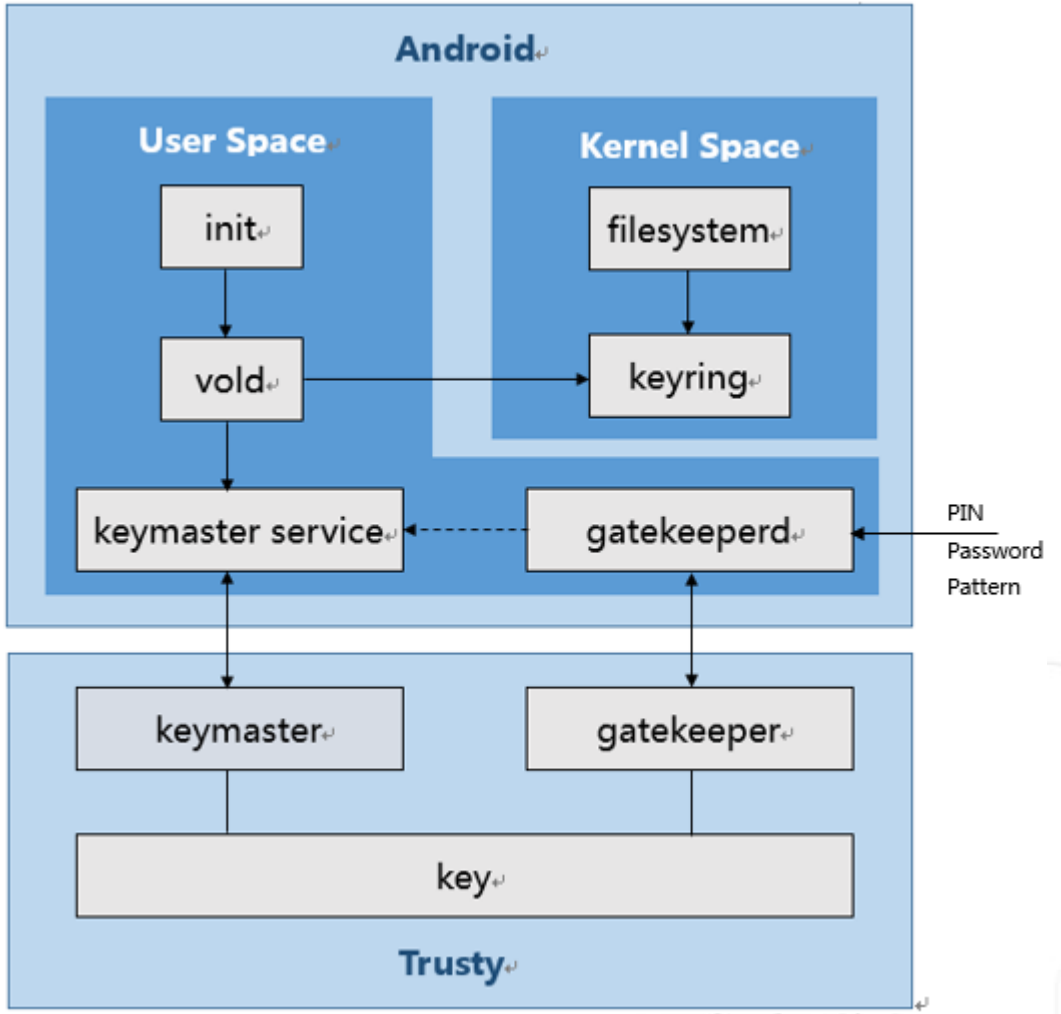
- **加密策略**
  - 加密策略包括文件名加密算法、文件内容加密算法和key_ref（对主密钥通过SHA512算法计算出的密钥索引，文件系统通过该索引从keyring中获取对应的主密钥）
  - 用户空间进程创建目录时，通过系统调用ioctl() 将加密策略传递给文件系统inode
  - 文件系统I/O操作时，根据inode判断该文件/目录是否需要加解密
  - 文件系统从keyring中获取主密钥，用于I/O流程中的加解密操作

FBE 主密钥派生流程

- FBE主密钥以加密形式存储，通过另一个存放在Trusty中的密钥进行加密

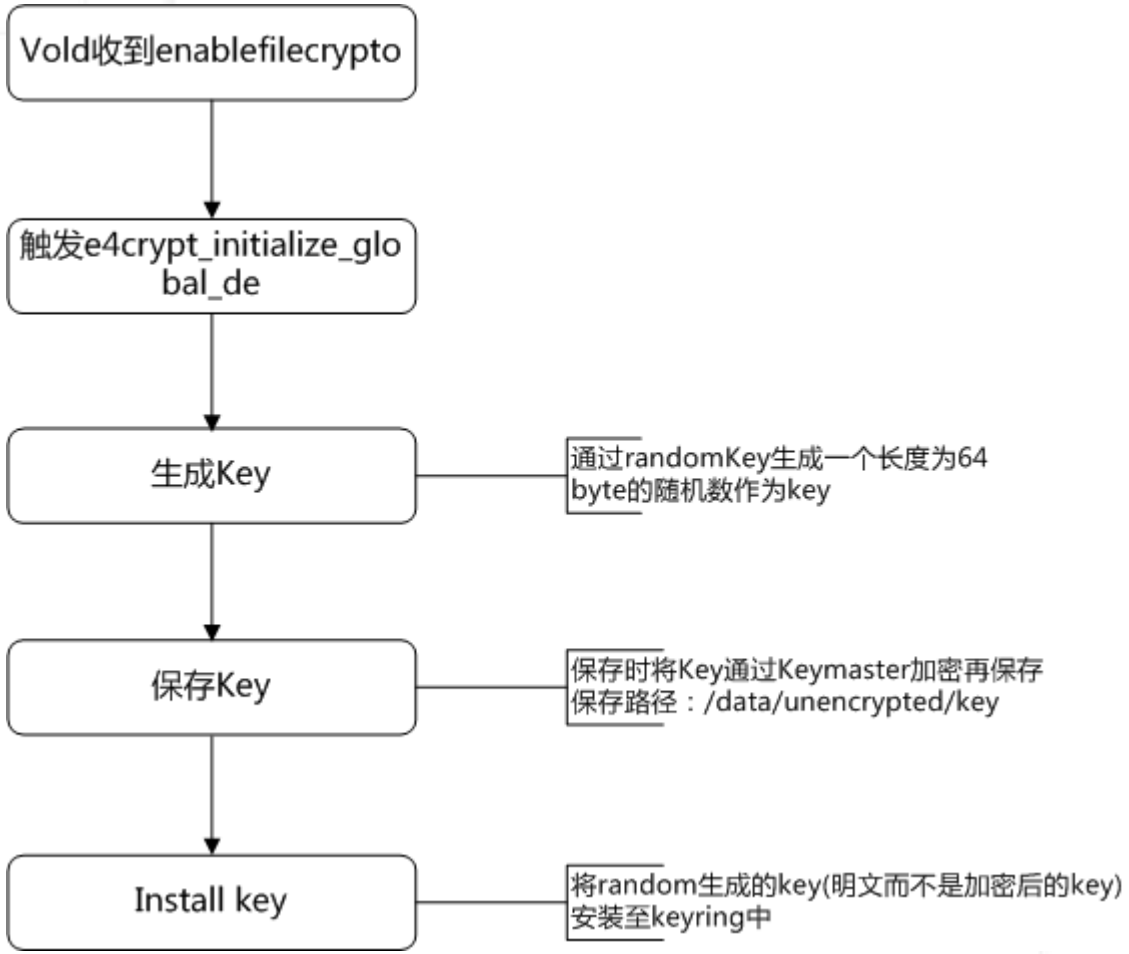
- 开机流程
  - 开机流程中，init进程调用vold
  - vold与Keymaster/Keystore交互，派生系统密钥（device_key）和用户DE密钥（user_de_key）
  - vold将相应密钥传递给kernel keyring后，系统目录和用户DE目录可访问

- 用户解锁流程
  - 用户输入PIN/Password/Pattern，经过Gatekeeper身份认证后，生成身份验证令牌（AuthToken）
  - vold负责与Keymaster/Keystore交互，派生用户CE密钥时需要传入AuthToken
  - vold将相应密钥传递给kernel keyring后，用户CE目录可访问



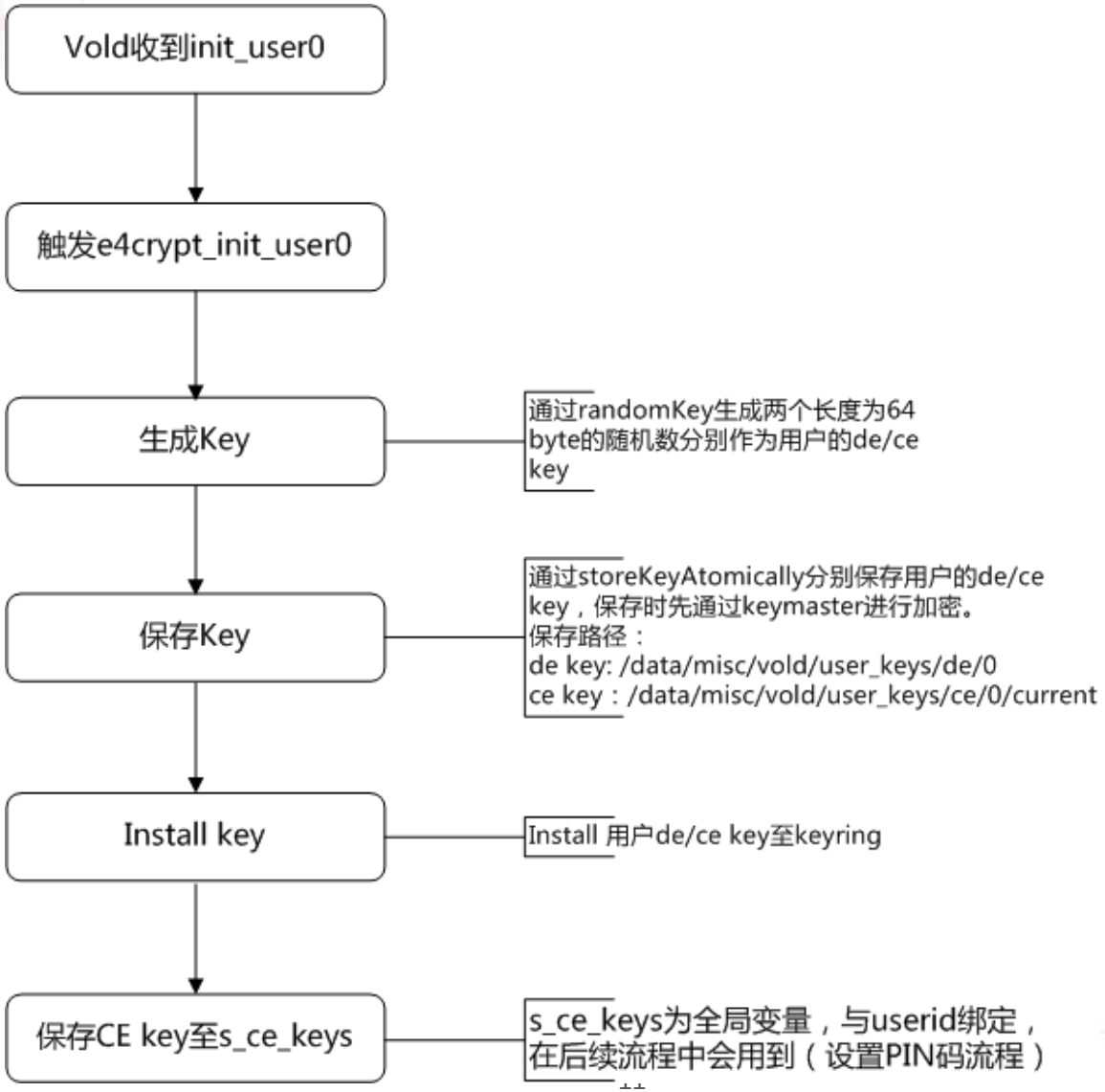
FBE 主密钥派生流程

- 首次开机创建系统目录密钥（device_key）



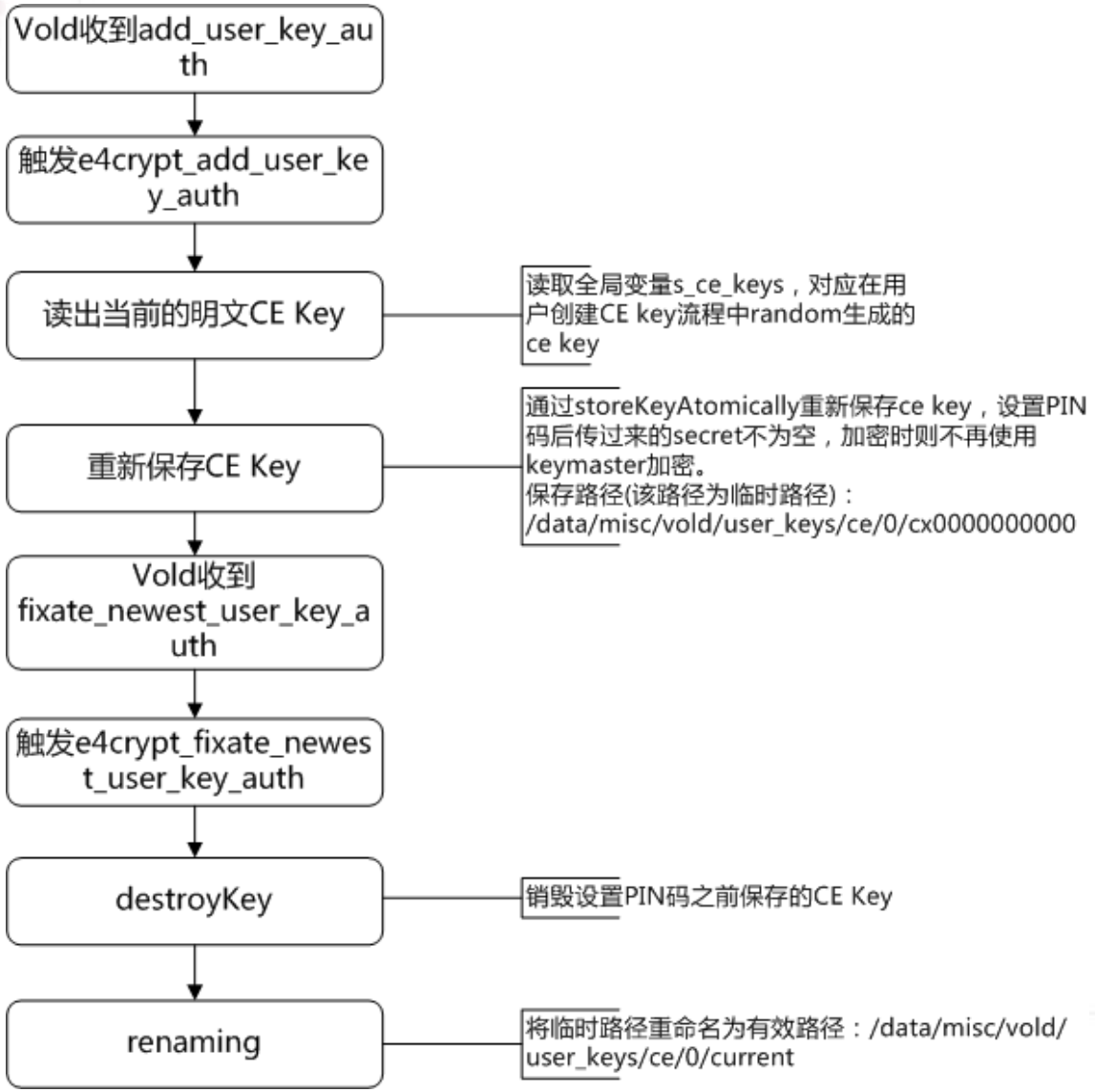
FBE 主密钥派生流程

- 首次开机创建用户CE/DE目录密钥



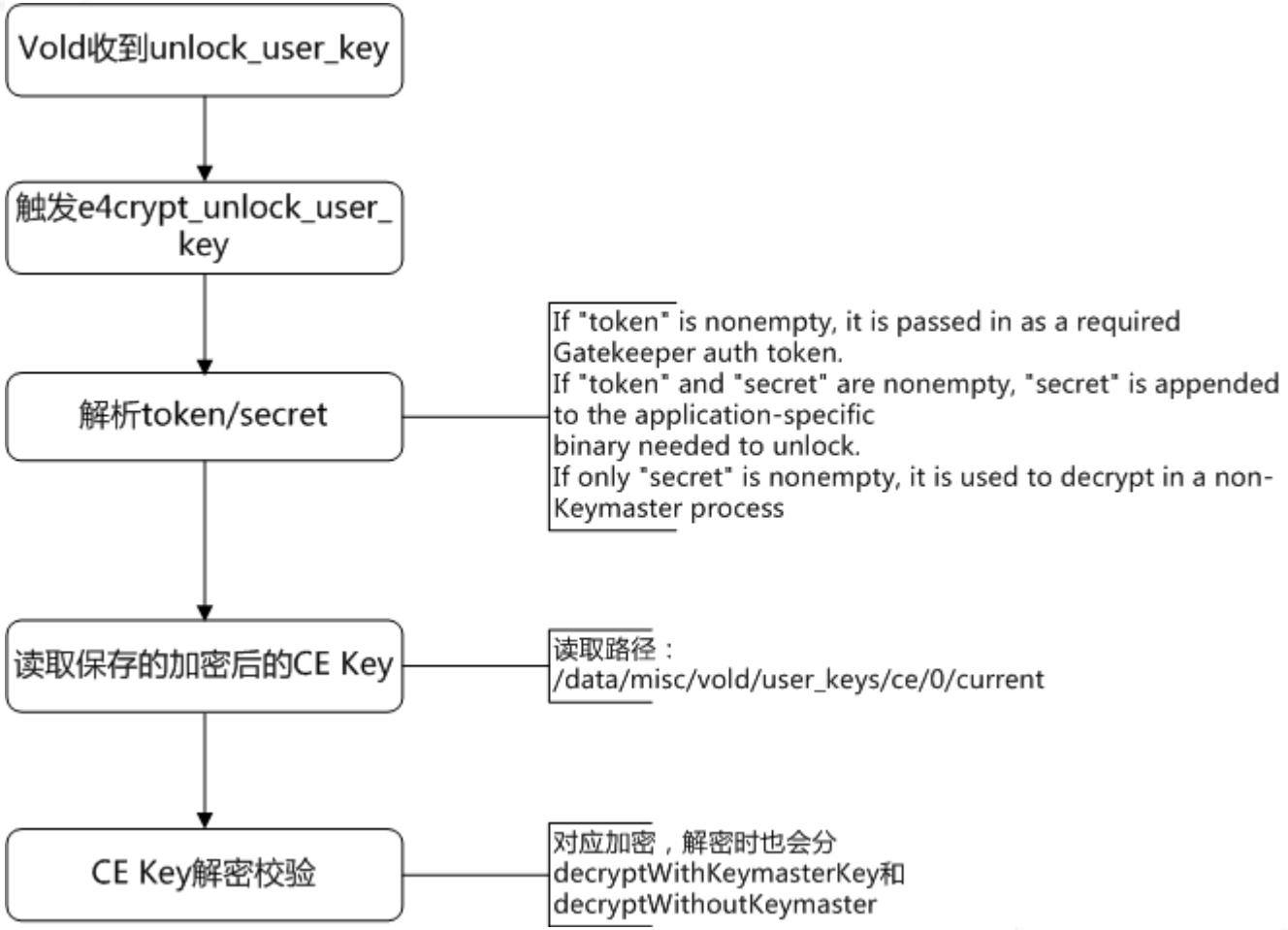
FBE 主密钥派生流程

- 设置PIN/Password/Pattern更新用户CE目录密钥



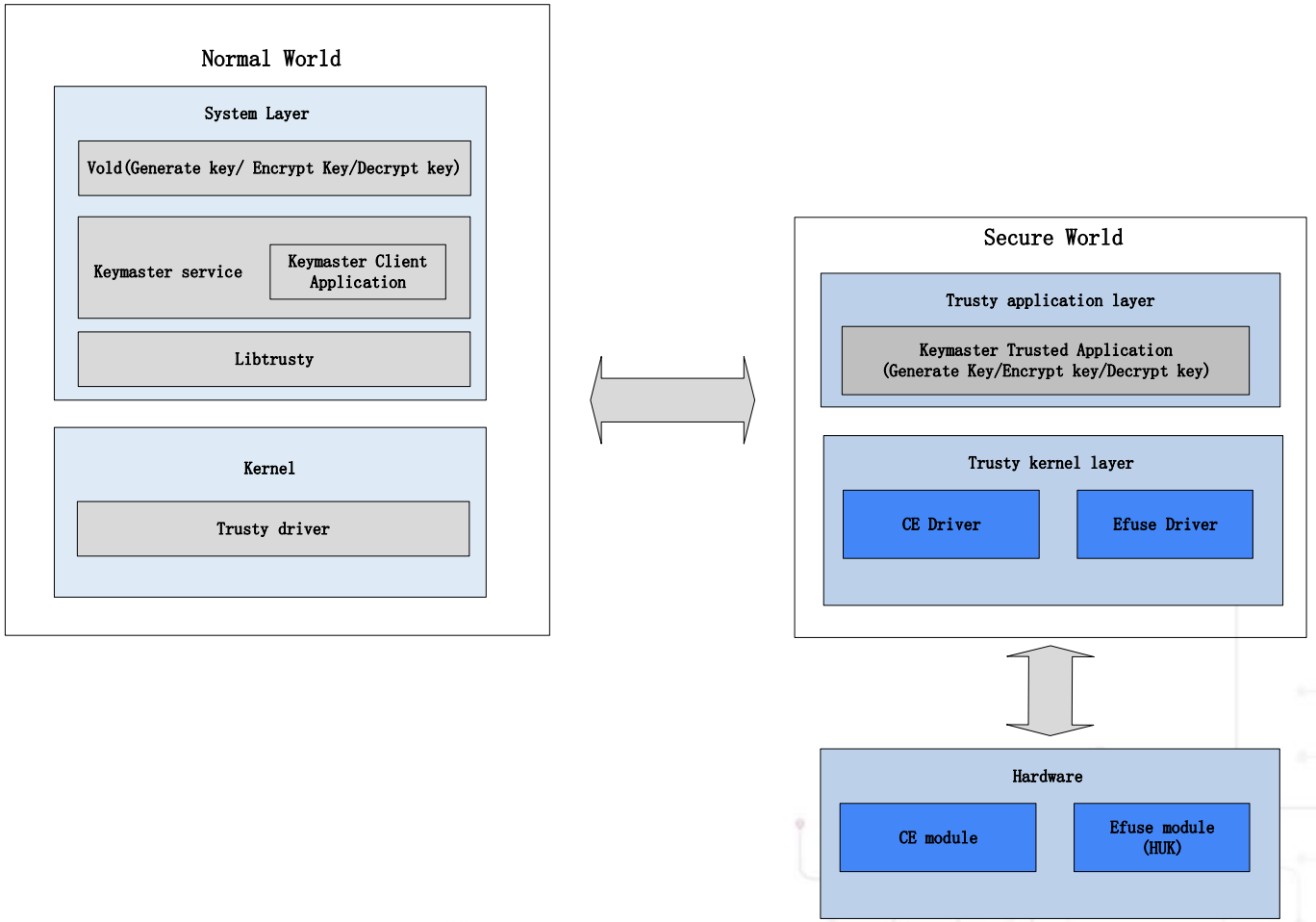
FBE 主密钥派生流程

- 用户解锁派生CE目录密钥



TEE Keymaster 密钥管理流程

- vold通过Binder机制与Keymaster Service建立通信连接，调用Keymaster Client Application响应vold模块的Generate key/Encrypt key/Decrypt key请求
- 进一步通过Kernel Trusty Driver转发Keymaster client Appliction请求至Secure world
- Secure world的Keymaster Trusted Application调用CE,efuse等功能完成实际的Generate key/Encrypt key/Decrypt key运算



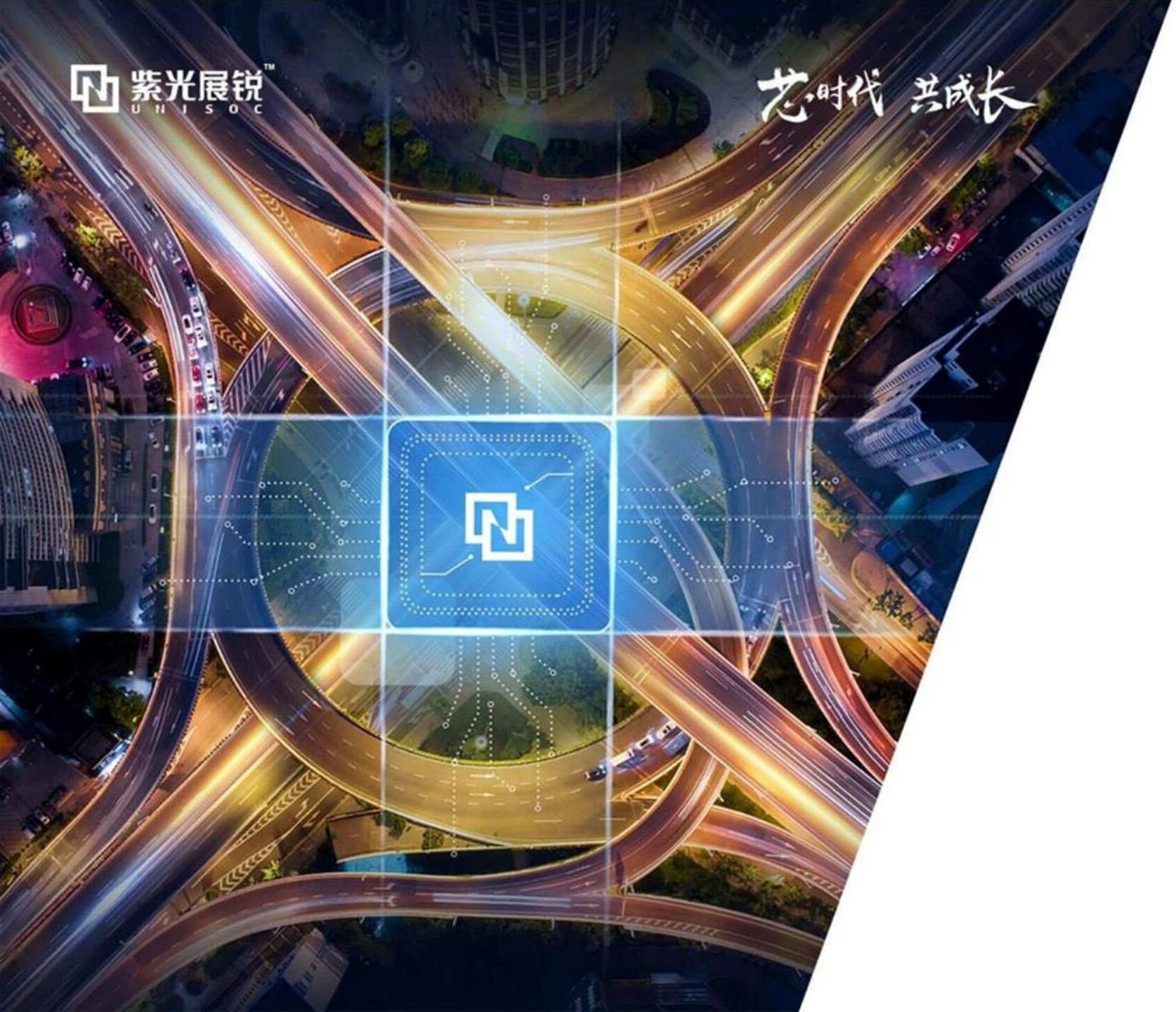
TEE Keymaster 密钥管理注意事项

- Generate Key/Encrypt Key/Decrypt key 操作使用root of trusty 来自于芯片Efuse模块内部（HUK）
- HUK具有唯一性
- 要正常响应来自于Generate Key/Encrypt Key/Decrypt key 的请求，Keymaster sevice、Keymasater Client application, Kernel, TOS及Keymaster Trusted Applicaton须能够正常工作加密

防御模式分析

- 基于安全防御模式角度分析，目前文件系统fscrypt加密只防御针对文件名称和文件内容的离线攻击，不保护诸如文件大小、权限、时间戳和扩展属性之类的数据

- 针对计时攻击和在线攻击，按照Google的官方说明，虽然这两种攻击模式在一些场景下更需要防御，但是由于需要整体协调用户空间、kernel Crypto API、内存管理和文件系统，针对这两种模式攻击的防御方案暂不支持



THANKS

WWW.UNISOC.COM
紫 光 展 锐 科 技