openEuler环境下基于openHiTLS构建多场景密码产品体系

目录

openHiTLS在移动端产品的应用

移动签名

身份认证
数据签名
文档签名

移动签署

电子签章
印章申请
印章管理

身份核验

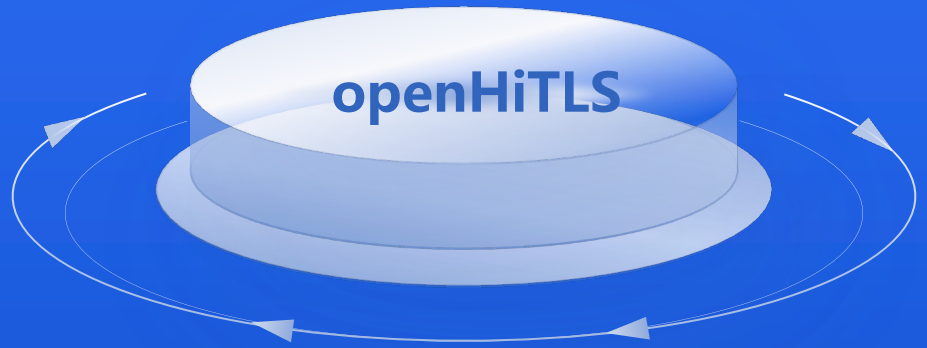
活体检测
人脸识别
OCR识别

手写签名

拍照证据
手写证书
录音证据

身份核验组件 | 键盘组件 | openHiTLS | OCR组件 | 手写组件

openHiTLS在客户端产品的应用



数字证书

证书解析
证书验证

数据签名

签名数据编解码
国密签名消息语法

数据加密

加密数据编解码
国密加密消息语法

电子签章

签章数据编解码
国密签章语法

安全通信

TLS协议
国密TCLP协议

基于openEuler和openHiTLS底座构建服务器密码产品平台

openHiTLS作为密码底座

- 屏蔽不同软硬件密码的差异
- 提供完善的密码应用接口

openEuler作为操作系统底座

- 磁盘、网络等各项指标均明显高于CentOS
- 在生态软件兼容性方面，相比其他操作系统更完善

基于openHiTLS构建V2X终端安全协议栈

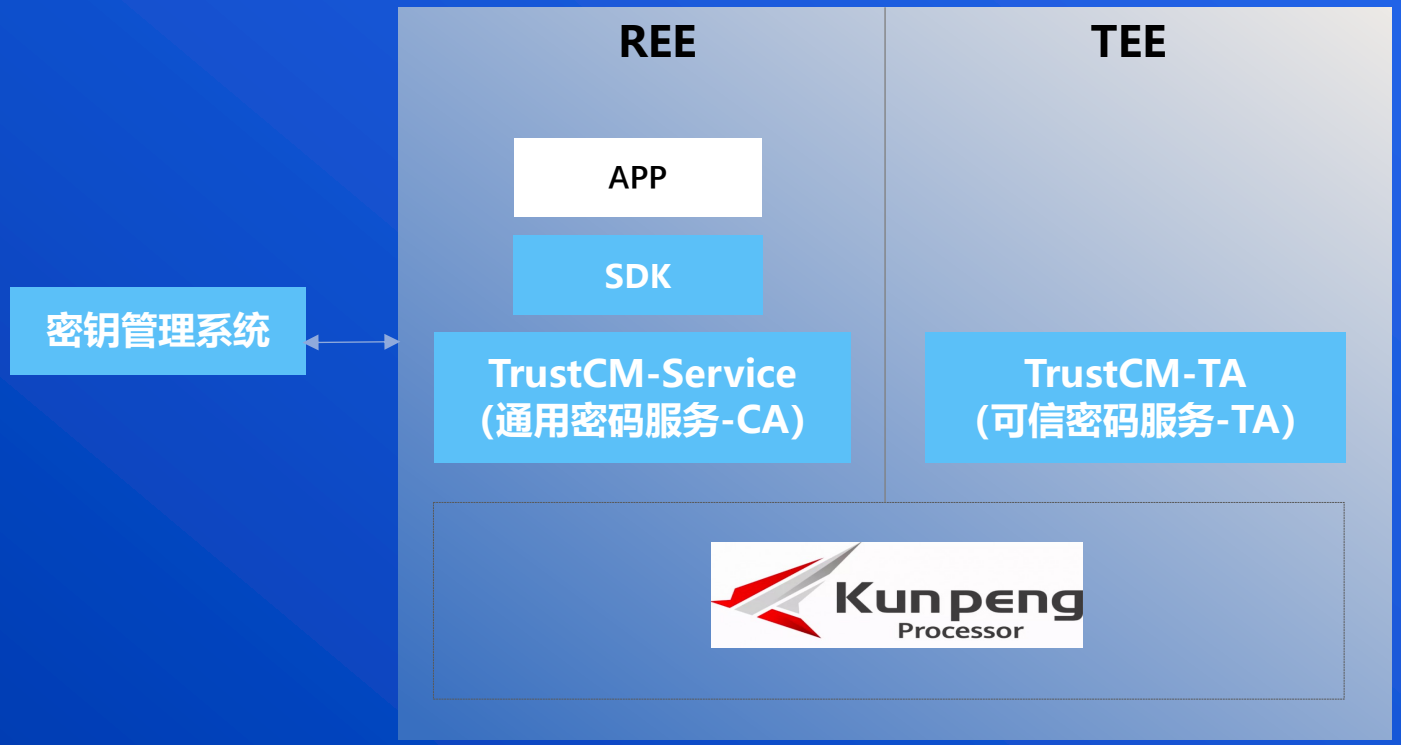
消息签名和验证

消息加密和解密

假名证书密钥衍生

- 提供安全通信能力，保障V2X安全通信安全
- 提供的全栈的密码算法和数字证书的支持
- 为密码应用提供统一的密码运算接口，实现了业务模块和密码芯片的解耦
- 支持多平台，能够更快速的移植到车载和路侧设备

“鲲密”密码算力平台

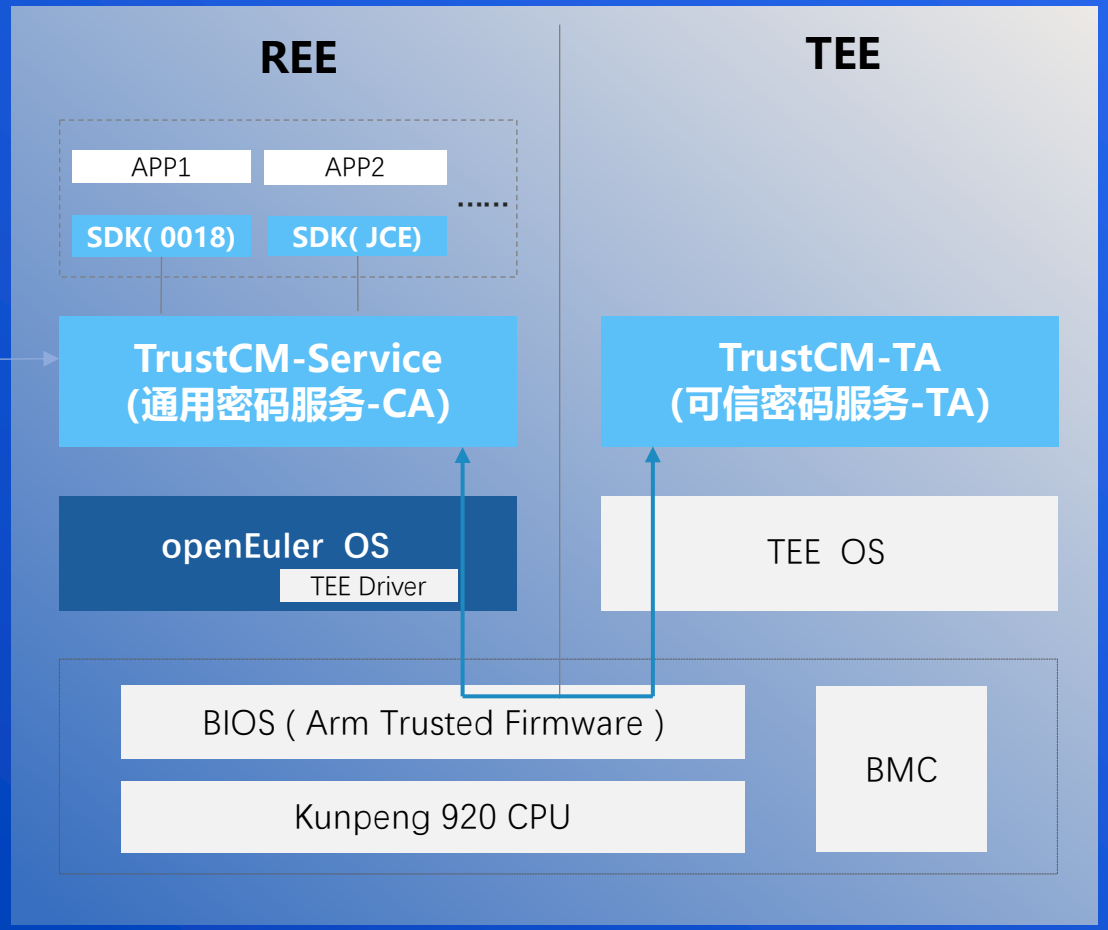


创新的密码算力供给模式

内生　分布式　敏捷　高效

- 基于鲲鹏CPU构建的可信执行环境TEE，实现二级密码模块及密码算力系统。
- 系统包括：可信密码服务、通用密码服务、应用适配SDK、密钥管理系统

openEuler支撑“鲲密”密码算力平台的多元化密码应用需求



基于芯片实现硬件层面的强制隔离计算

- 密钥作为运算机密数据下载于TA中
- 涉及密钥运算全部在TA中完成
- 满足GB/T 37092二级安全要求

匹配应用多元需求的柔性密码供给交付

- REE侧实现对密钥管理、密码服务的封装
- 对应用提供各种标准合规的SDK、API接口
- 支持宿主机和虚拟化等多种环境

基于“鲲密”和openHiTLS实现软件定义SSL卸载

外挂密码设备，传统SSL流量卸载

Nginx+SSL引擎，软件定义SSL卸载

openHiTLS是一款极全特性、极高性能、极高信任的密码套件

能够满足多场景的安全需求

身份认证

安全通信

数据安全

隐私计算

THANKS

THANKS

THANKS