平头哥 RISC-V

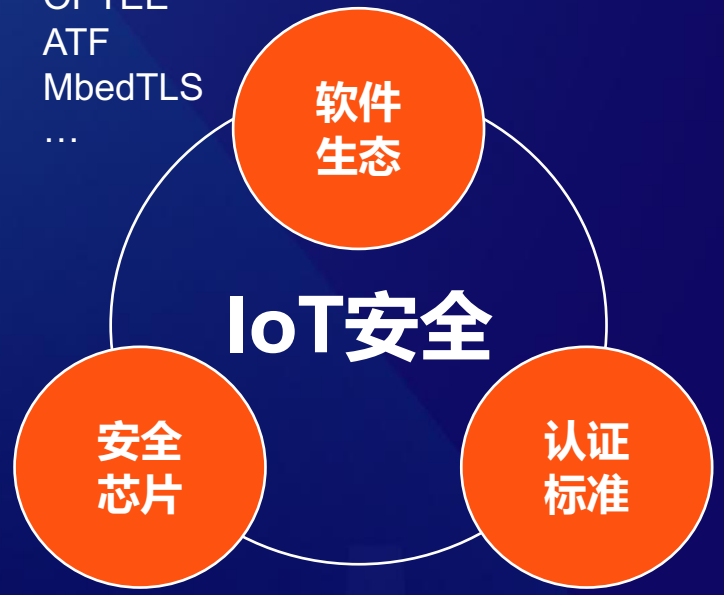
2023 RISC-V 中国峰会

RISC-V安全技术加速安全生态迁移和部署落地

崔晓夏/平头哥半导体有限公司

IoT安全领域的安全现状

- IoT安全生态基本以ARM软件为主流，例如：
  - TFM
  - OPTEE
  - ATF
  - MbedTLS
  - …



- 安全芯片基本以ARM处理器为主流，例如：
  - SE芯片
  - TEE芯片
  - TPM芯片
  - HSM芯片
  - …

- IoT领域的安全认证以ARM安全技术为标准，例如：
  - Global Platform TEE
  - Global Platform SESIP
  - PSA Certificate
  - …

RISC-V需要可复制地解决安全问题

定制化能力强　　扩展伸缩性强

玄铁RISC-V安全技术

详情请参考 https://xuantie.t-head.cn/soft-tools/security/4197784595837554688?spm=a2cl5.27298783.0.0.44939AVG9AVGHI

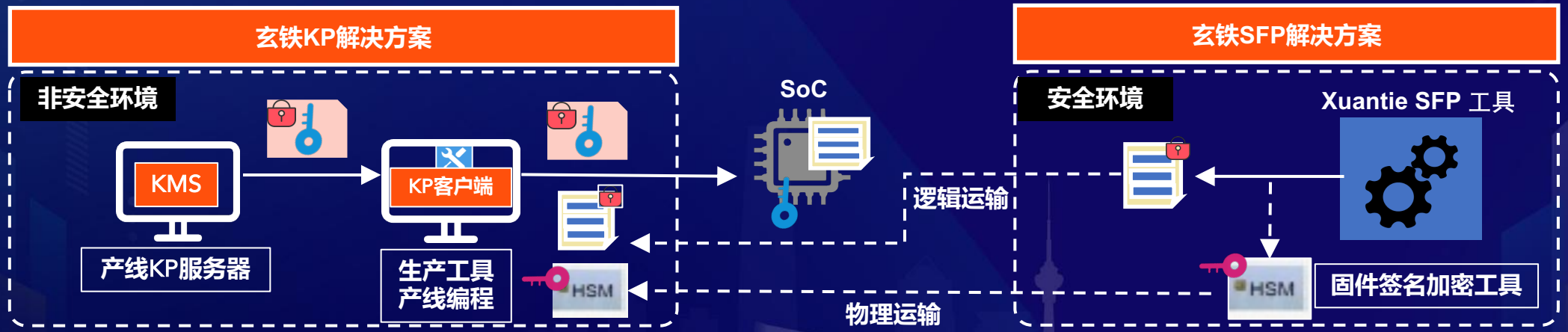
同构跨平台玄铁TEE解决方案

Global Platform®

- 全球首个RISC-V TEE安全平台
- 国际Global Platform安全认证进行中

玄铁安全生产解决方案

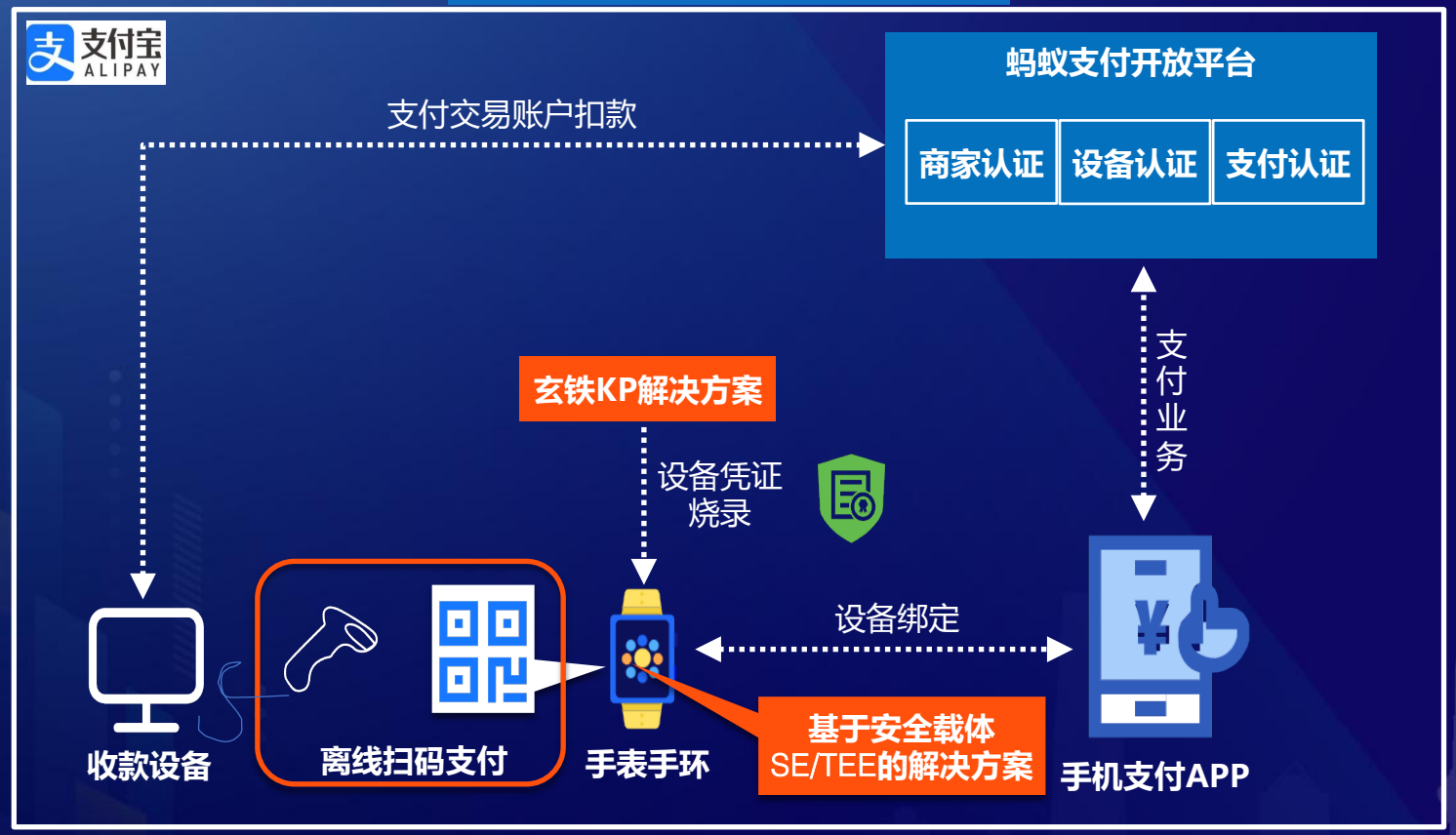
解决方案	带来的好处	功能
玄铁KP解决方案	1. 解决产品安全密钥在非安全环境下的生产问题 2. 快速被集成至客户生产环境，减少生产时间周期	• 支持不同安全等级的密钥生成、传输、存储、注入等 • 支持产品安全个性化生产 • 使用C/S模式，客户端支持多种方式被集成
玄铁SFP解决方案	1. 解决可信固件在非安全环境下的生产问题 2. 准确管控可信固件的生产数量	• 支持第三方的软IP（语音算法、识别算法、AI算法等） • 可防止可信固件被克隆和破解 • 可满足可信固件不同存储形态的安全性



详情请参考 https://xuantie.t-head.cn/product?id=4183663875847163904

可穿戴支付典型应用场景

可穿戴设备支付场景



全链路高安全解决方案

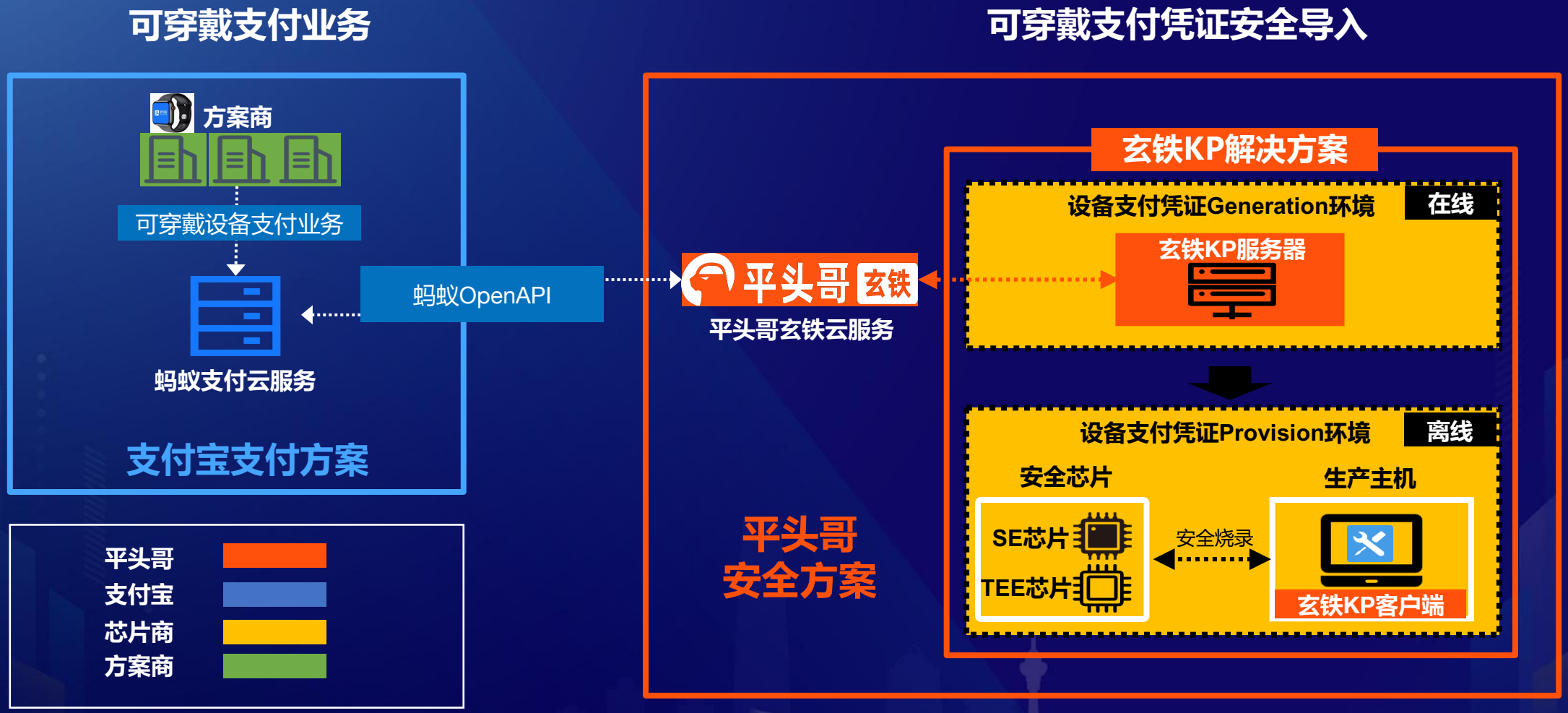
平头哥

- TEE/SE技术
- 玄铁KP解决方案
- 硬可信链技术

- 软件IP安全保护
- 支付资产注入安全
- 隐私数据存储安全

详情请参考 https://xuantie.t-head.cn/product?id=4117672381135261696

可穿戴支付设备安全生产



行业生态效应

支付宝 ALIPAY

聚焦支付业务场景

平头哥

聚焦安全解决方案

可穿戴行业量产落地

芯片原厂	10+
方案商	35+

玄铁 RISC-V 技术

- 华润微
- 宏思
- 华大电子
- 国民技术
- 杭州国芯
- 中科蓝讯

安全芯片厂商开始从ARM转向RISC-V

普惠

标准认证

标准化

蚂蚁企业团标

支持支付业务的可穿戴设备安全规范

- 蚂蚁安全标准组审核通过
- 蚂蚁企标对外发布中

中国信通院团标

面向支付业务的终端安全标准

- 蚂蚁科技
- 支付宝
- 信大捷安
- 平头哥
- 百度
- 信通院
- 中国联通

IEEE标准

Standard for Security specifications for Wearable devices supporting payment service Criteria

- IEEE标准分委会审核通过
- NesCom立项审批中

生态

安全

RISC-V生态渴望拥有你的安全

■ 安全技术

- 安全处理器升级和演进
- 安全算法PQC的支持
- RISC-V TEE技术满足国际行业标准安全认证

■ 应用领域

- 兼容现有领域产品的安全标准和完善专有领域的安全产品认证
- 实现不同领域之间的方案可复制

■ 软件生态

- 支持主流的开源安全软件
- 统一抽象密码学算法、TEE等软件接口定义(RVI-CSI， AP-TEE)

Find More

Xuantie @
GitHub