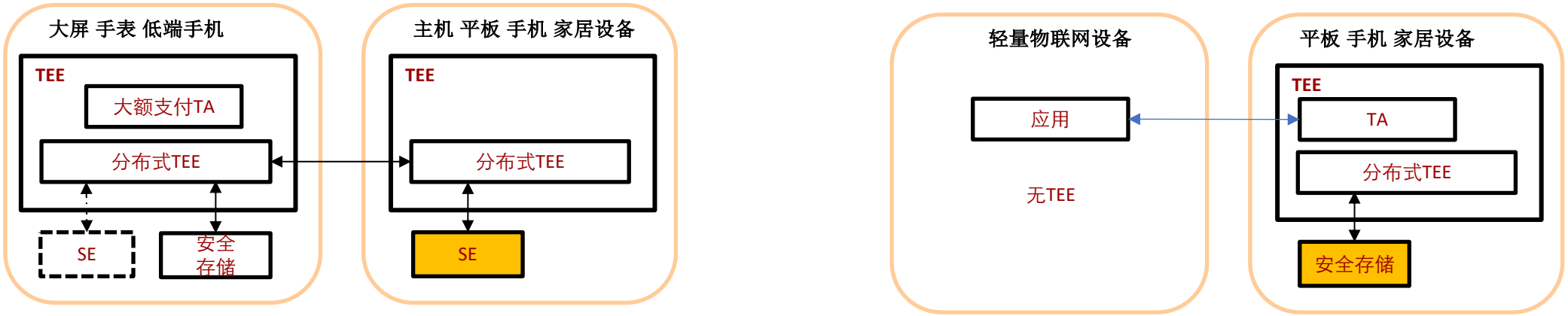
OpenHarmony Web3 TSG
分布式软总线可信互联方案

开放原子开源基金会
OPENATOM FOUNDATION

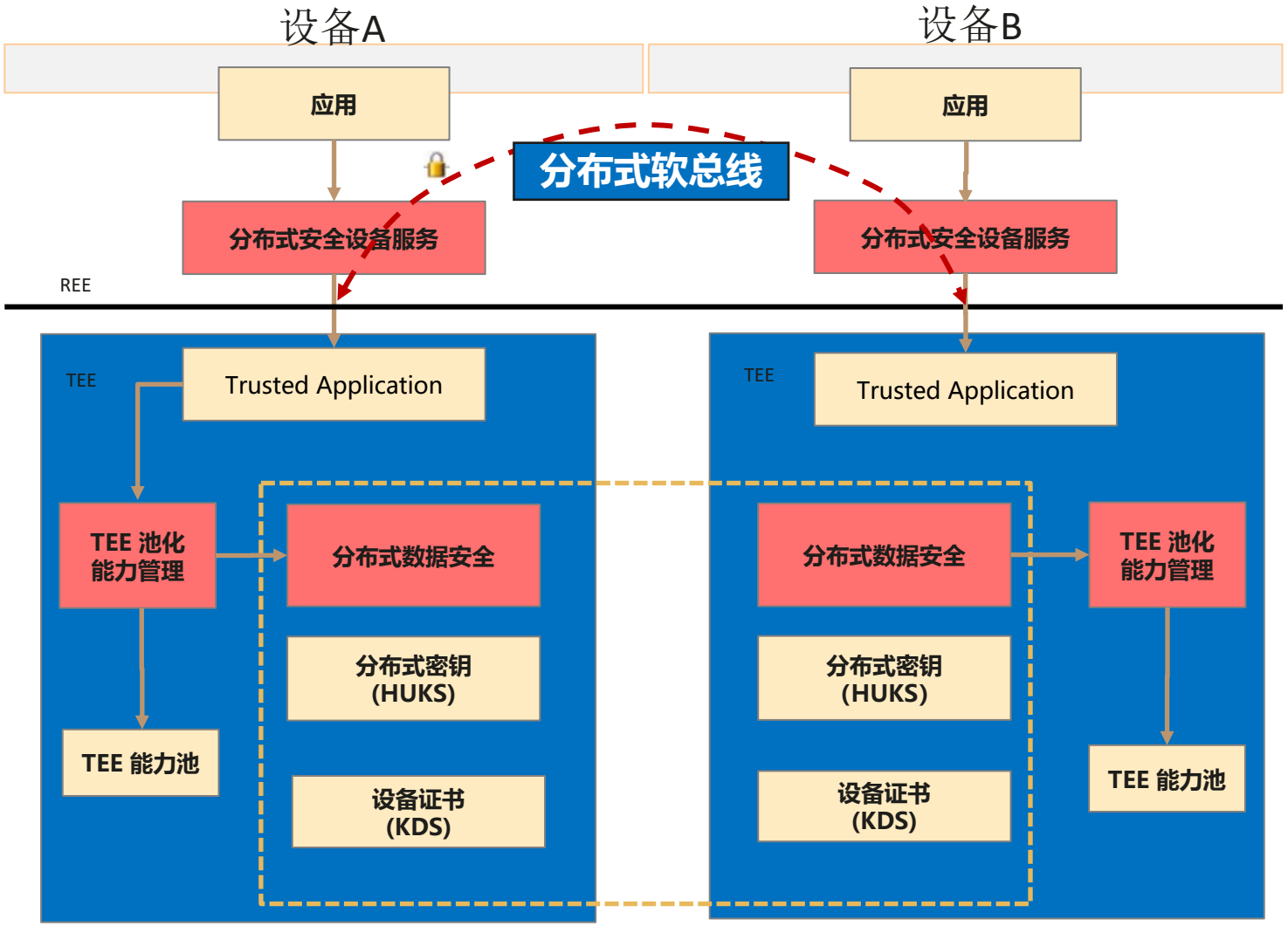
分布式TEE业务场景

端端互助：中控大屏无SE器件，如需大额支付功能时，可借用主机的SE能力进行金融支付；

强帮弱：者对于没有TEE的设备，可以利用强设备中的TEE安全能力，进行安全存储，提升数据安全性；



分布式TEE整体示意图



分布式软总线：OpenHarmony基础能力，提供设备发现、链接、组网、传输的基本能力，为分布式TEE提供底层通信能力。

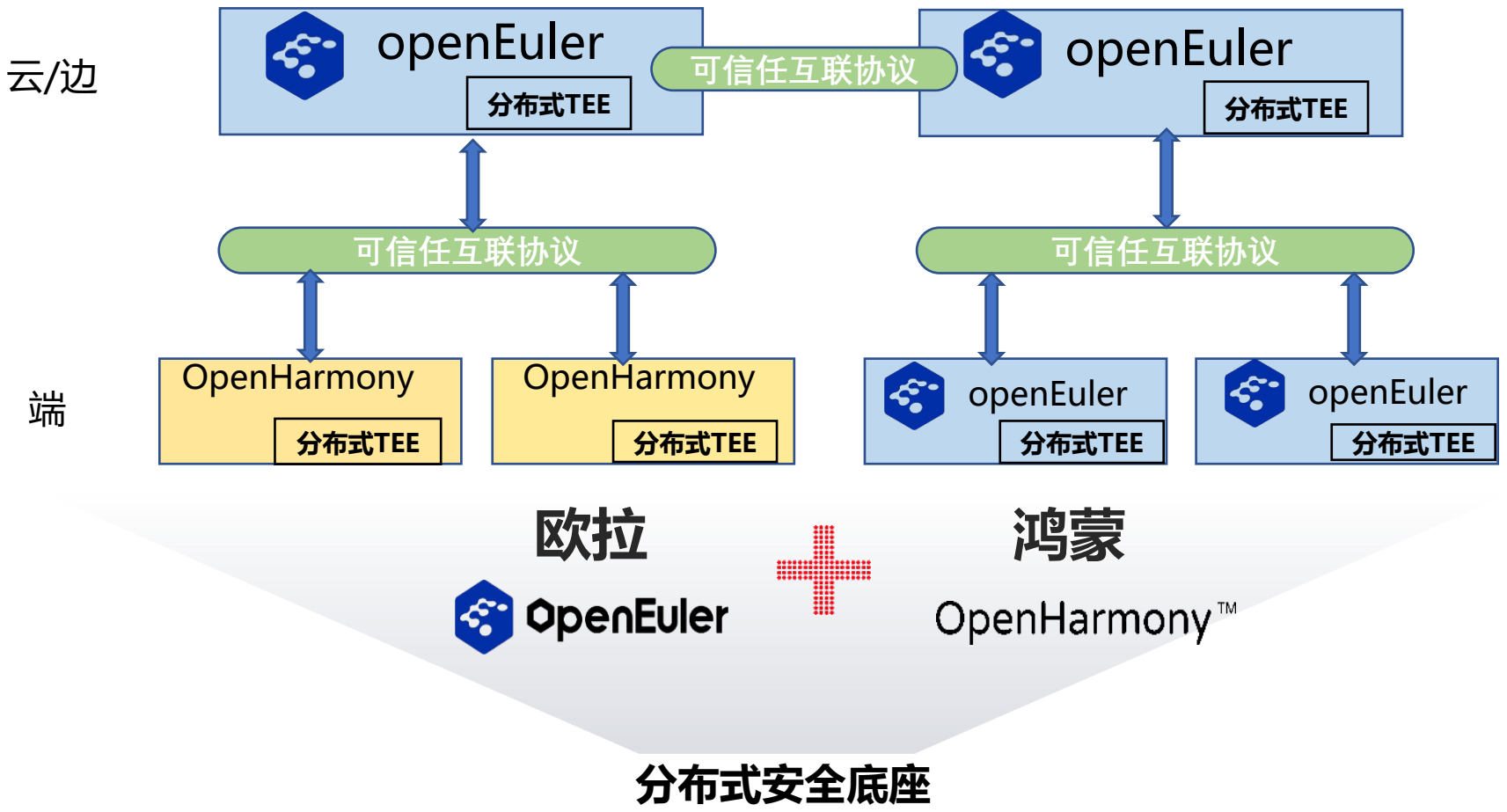
加密+认证=可信互联

分布式数据安全：出TEE数据全部加密，通过底层通信能力，将两个设备的TEE互联。

分布式认证：连接前，对两边的身份进行认证

当前采用集中式方案，希望通过分布式方案进行互联

未来基于可信任互联协议，将分布式TEE扩展到全场景



挑　战

- 集中式PKI管理成本高，不适合大规模使用
- 集中式的认证，不利于跨信任域场景

需要利用分布式方法，解决相关挑战。

根据我的理解，尝试梳理一下过程，请wenjing老师指正

场景：手机向平板用户证明是华为的TEE

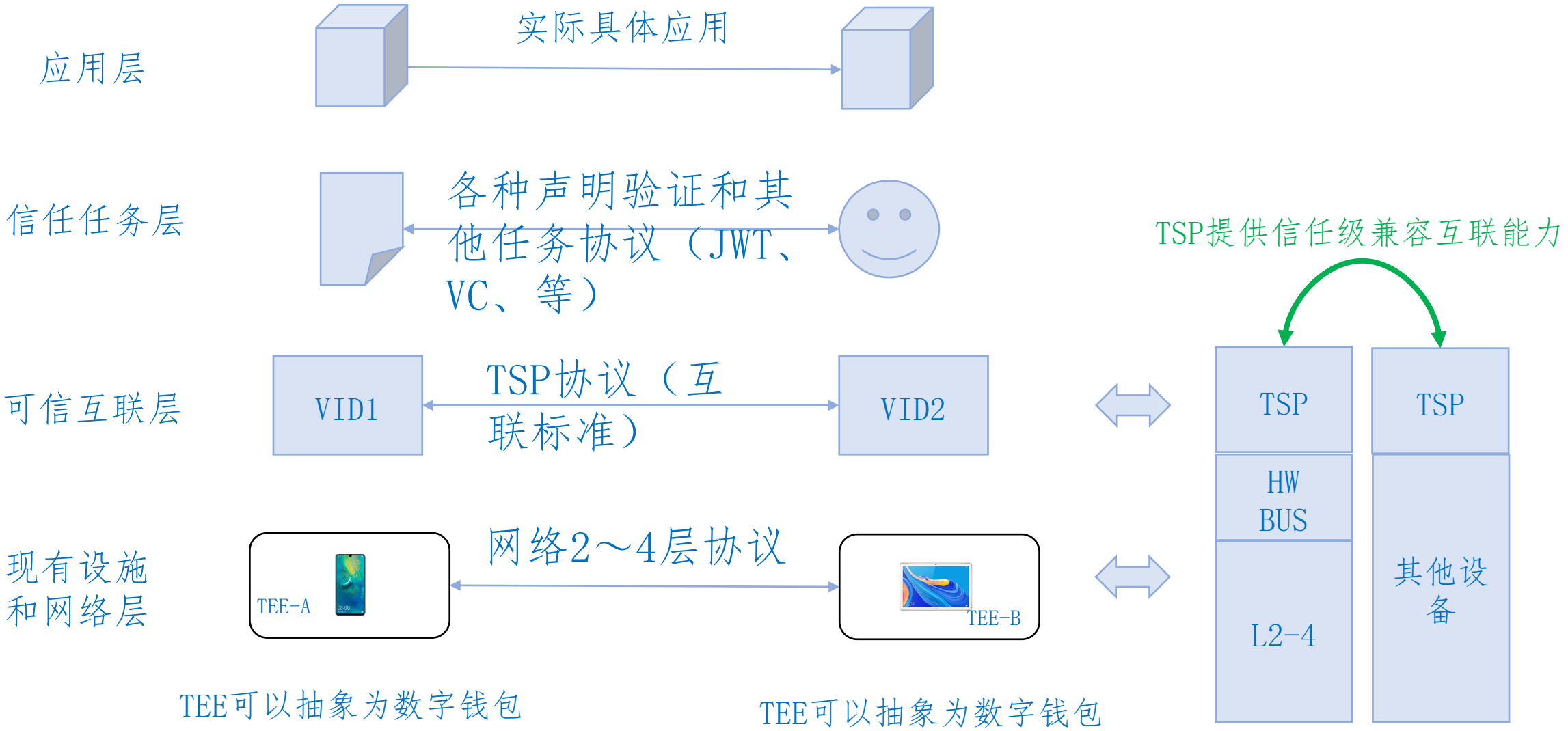
假设平板电脑不是华为产品、或不同OS带来不可信、或APP、或用户未有可信性确证等，网络完全不可信

可信互联协议TSP

VID + TSP + OIDC-JWT | VC =》 结合三块技术

- VID：可验证标识符、可以是分布式DID也可以是基于X509证书
- TSP：VID之间的高真实、高保密、高隐私通讯协议
- OIDC-JWT | VC | 或其他格式：OIDC JWT、X509基于CA的证书、或分布式的可验证声明/证书、其他信任任务等等

可信互联协议TSP层次



实例一

- 假设手机出厂时TEE-A设制不改，含iTrustee发的CA证书：
  - 钱包可自生成VID1,基于CA，验证方式与传统X509一样（V5X协议）
  - 平板电脑那一方也一样、基于CA证书生成VID2
  - 手机和平板接触传递VID：NFC、BlueTooth、WI-FI、Internet、QR…
  - TSP协议建立VID1与VID2之间的真实保密隐私通讯，双方建立长期通讯关系，以后的联系使用VID即可。

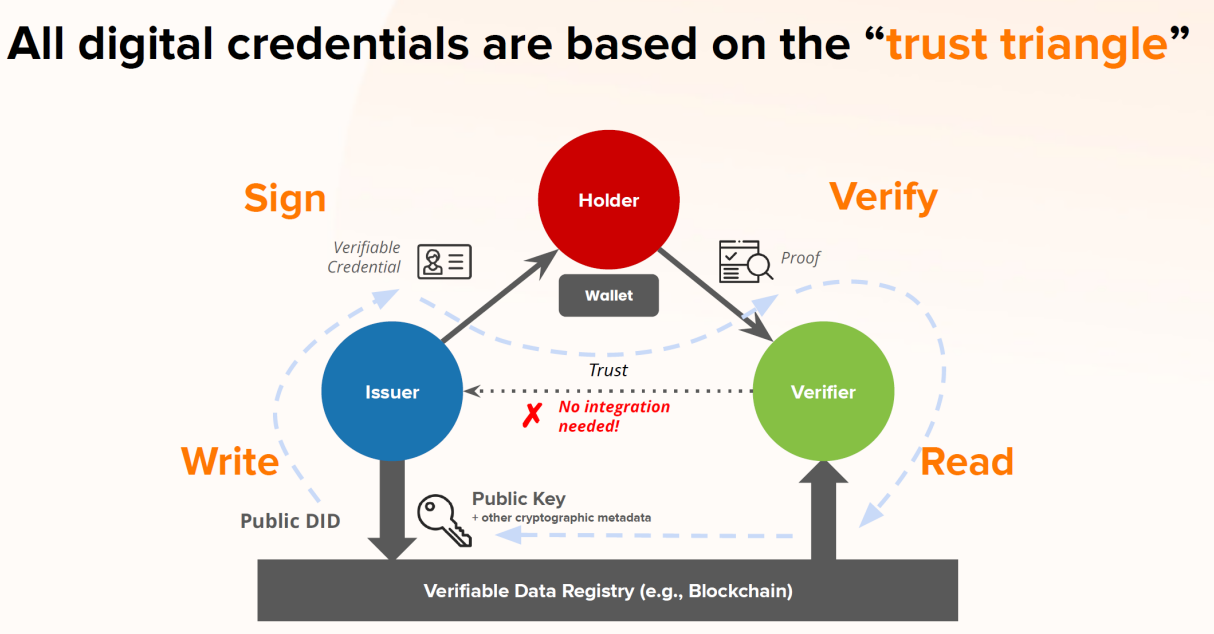
实例二

- 假设我们更多采用分布式设计的优点：
  - 钱包可自生成VID1,不一定各方都基于CA（或根不同），验证方式各异（比如V5X和DID:WEBS）
  - 平板电脑那一方也一样、但可以其他方式自生成VID2，不需与VID1统一
  - 手机和平板接触传递VID：NFC、BlueTooth、WI-FI、Internet、QR…
  - TSP协议建立VID1与VID2之间的真实保密隐私通讯，双方确认VID的信任根机制并建立长期通讯关系，以后的联系使用VID即可
  - 钱包或应用层若需要其他证书，比如实名或法律牌照，则可接受VC或JWT证书
    - 发证方、持证方、验证方

TEE信任软总线

- 基于TSP的设计思路图
  - （1）选择一个合适的VID机制
  - （2）使用TSP Rust（2024上半年）- 移植到OpenHarmony OS界面
  - （3）移栽TSP到软总线上
  - （4）选择一些显现特别功能的案例作为示范

待讨论-没有验证

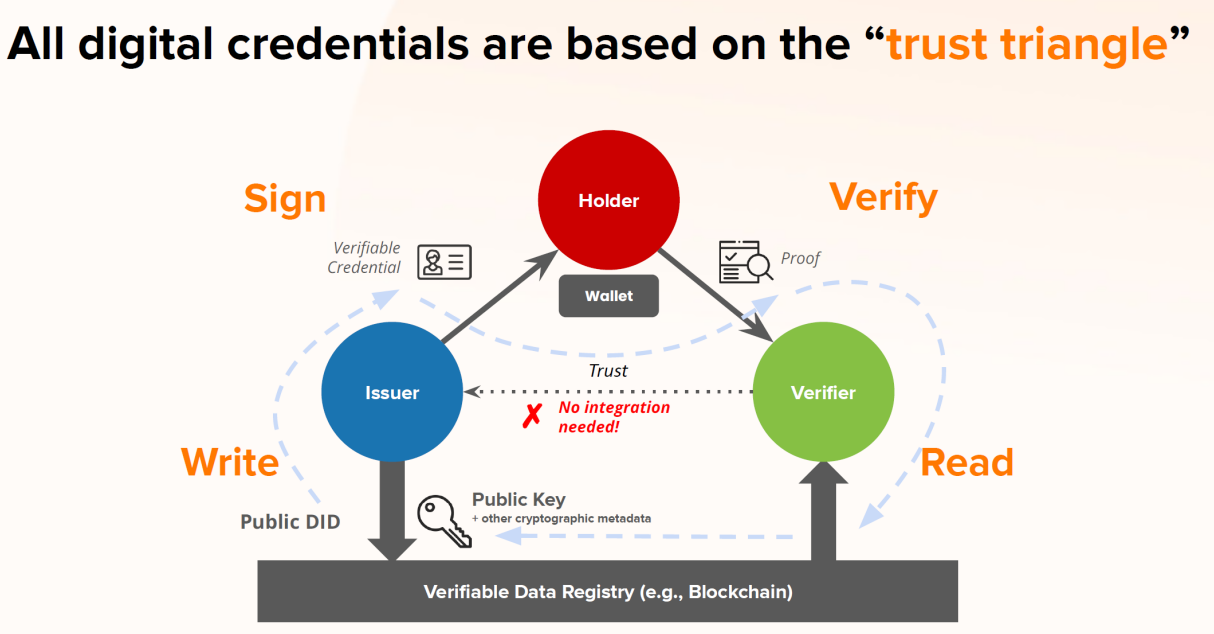


Issuer（发证方）：可以是iTrustee（我们团队）作为CA，也可以是其他厂家

Holder（持证方）：手机TEE-A
情况一：所有iTrustee共用一个DID
情况二：所有iTrustee出厂都有一个DID
先考虑不同TEE不同DID场景

Verifier（验证方）：平板TEE-B
用于验证对方的身份

待讨论-没有验证



Step1：

手机出厂时，手机（TEE-A）需要创建自己的DID标识与DID文档，私钥灌装在TEE中，公钥存储在区块链上。

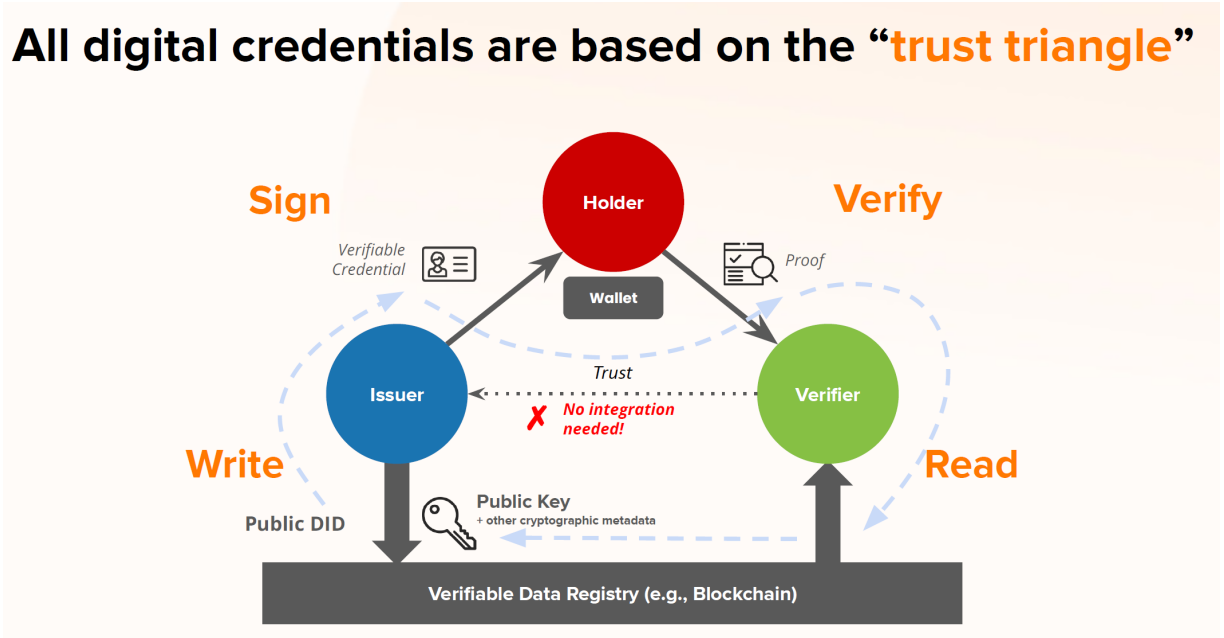
Step2：

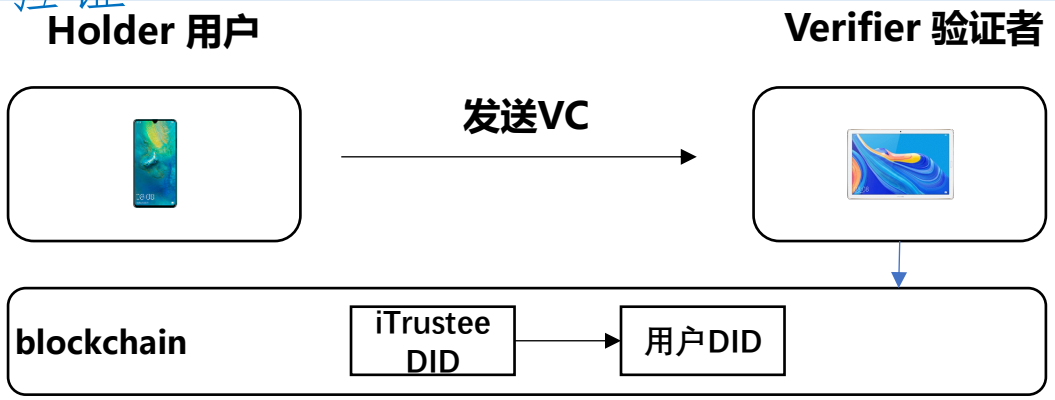
iTrustee作为Issuer，要确认DID关联的TEE是华为的TEE，然后颁发VC可验证声明，表明是华为的TEE。

Step3：

将可验证声明存储于TEE中。

待讨论-没有验证





Step1：

手机上的TEE用自己的私钥，将华为颁发的VC进行签名，发送给验证者

Step2：

验证者在区块链上通过用户的DID获取公钥信息，验证发过来消息确实是这个DID发送的消息。

Step3：

用华为的DID获取华为的公钥信息，验证VC信息

最终确认是华为的TEE

是否一定要用区块链？如果不用区块链，公钥存储采用什么方法？是否还需要新建一个基础设施

不一定需要。公钥是非保密信息，可以储存到任何方便的系统上，比如：DNS Record、WEB URL。如果Harmony作为生态的主服务器，那存储在harmony.com就可以了。Harmony需要提供reliability、accessibility，但不需要类似区块链的可信性，因为它不是信任根。当然这个问题最终是生态伙伴之间要讨论的事。

当前OpenTrustee与分布式TEE代码仓

OpenTrustee：
https://gitee.com/openharmony-sig/tee_tee_dev_kit/tree/master/docs/opentrustee-guidelines

分布式TEE：
https://gitee.com/openharmony-sig/tee_distributed_tee_framework/
https://gitee.com/openharmony-sig/tee_distributed_tee_service/

谢谢！