HCE 全面介绍

关于HCE的作用原理系统架构交易要素的全面介绍

NFC简介

定义

近距离无线通讯NFC是一种无线高频通讯技术

速度

每秒传1kbit

10公分之内近距离资料交换

距离

碰触就可连结

无需预先配对或开启应用程序

连接

NFC三种模式

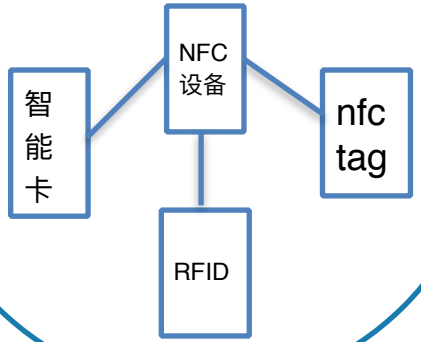
1

点对点模式

两台NFC设备间的信息交换

2

读写模式



3

卡模拟模式

模拟多种实体卡片功能，实现NFC装置支付或安全功能。NFC装置必须使用内建安全元件(Security Element, SE)的NFC芯片。

手机对手机通讯、手机当POS读写卡、手机当卡片与POS交互

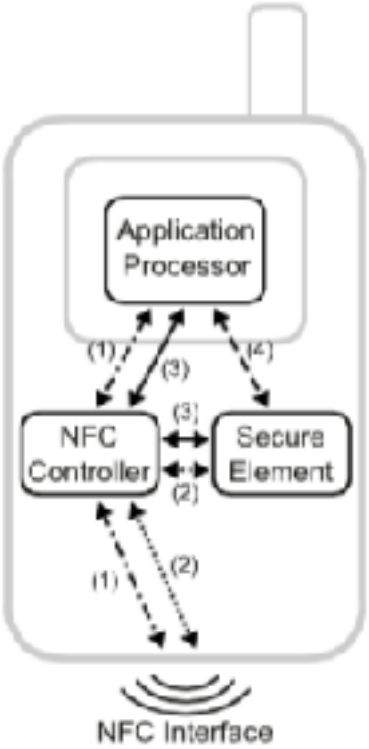
NFC特点

定义

近距离无线通讯NFC是一种无线高频通讯技术

速度

每秒传1kbit



10公分之内近距离资料交换

距离

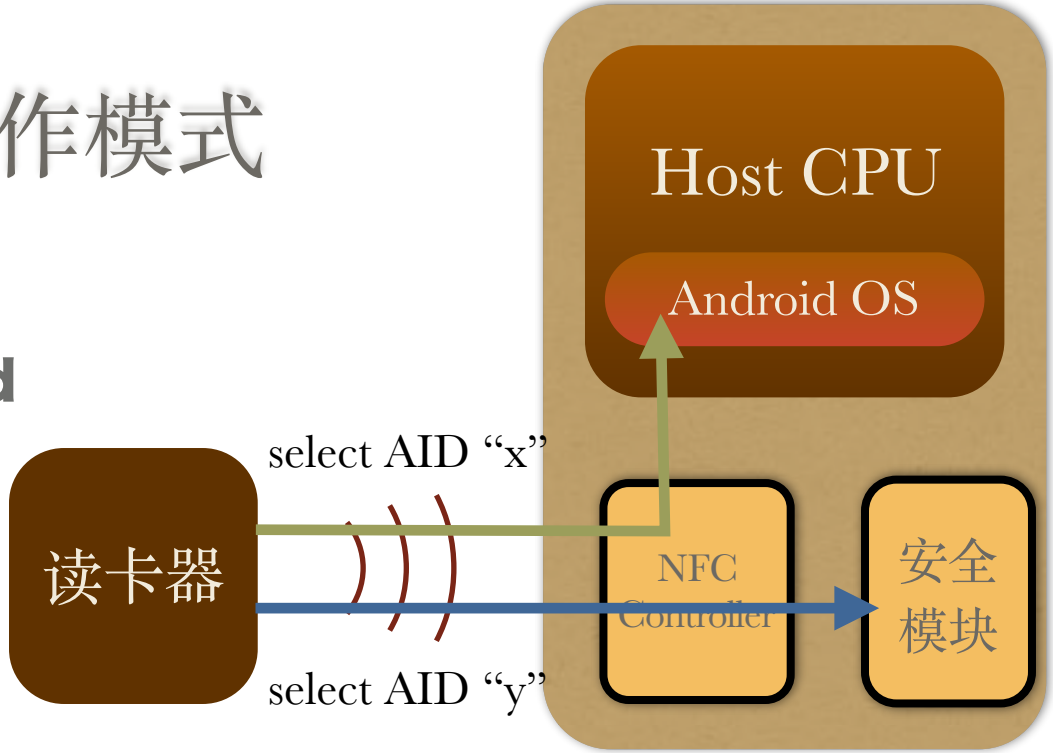
碰触就可连结

无需预先配对或开启应用程序

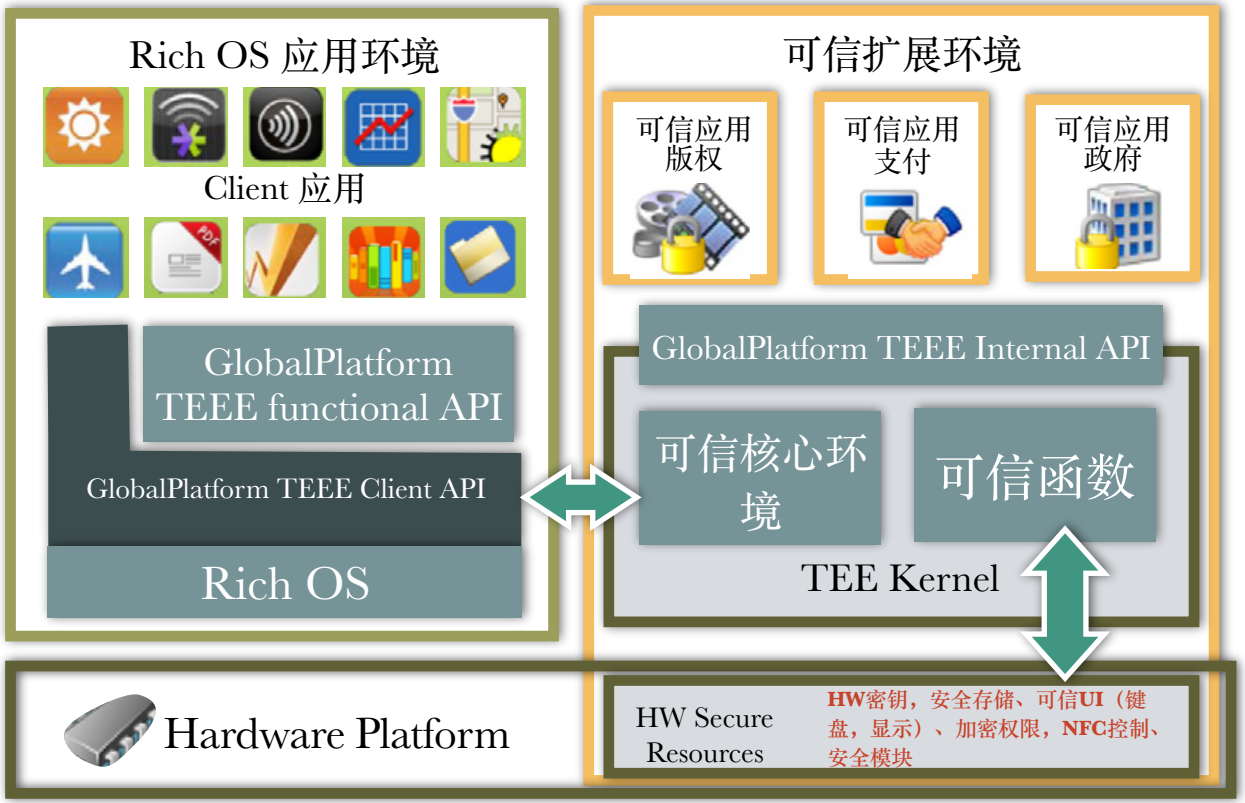
连接

Android 两种操作模式

- SE-based Card
- Host-based Card



NFC终端可信环境


Rich OS 应用环境
Client 应用
GlobalPlatform TEEE functional API
GlobalPlatform TEEE Client API
Rich OS
可信扩展环境
可信应用版权
可信应用支付
可信应用政府
GlobalPlatform TEEE Internal API
可信核心环境
可信函数
TEE Kernel
Hardware Platform
HW Secure Resources
HW密钥，安全存储、可信UI（键盘，显示）、加密权限，NFC控制、安全模块

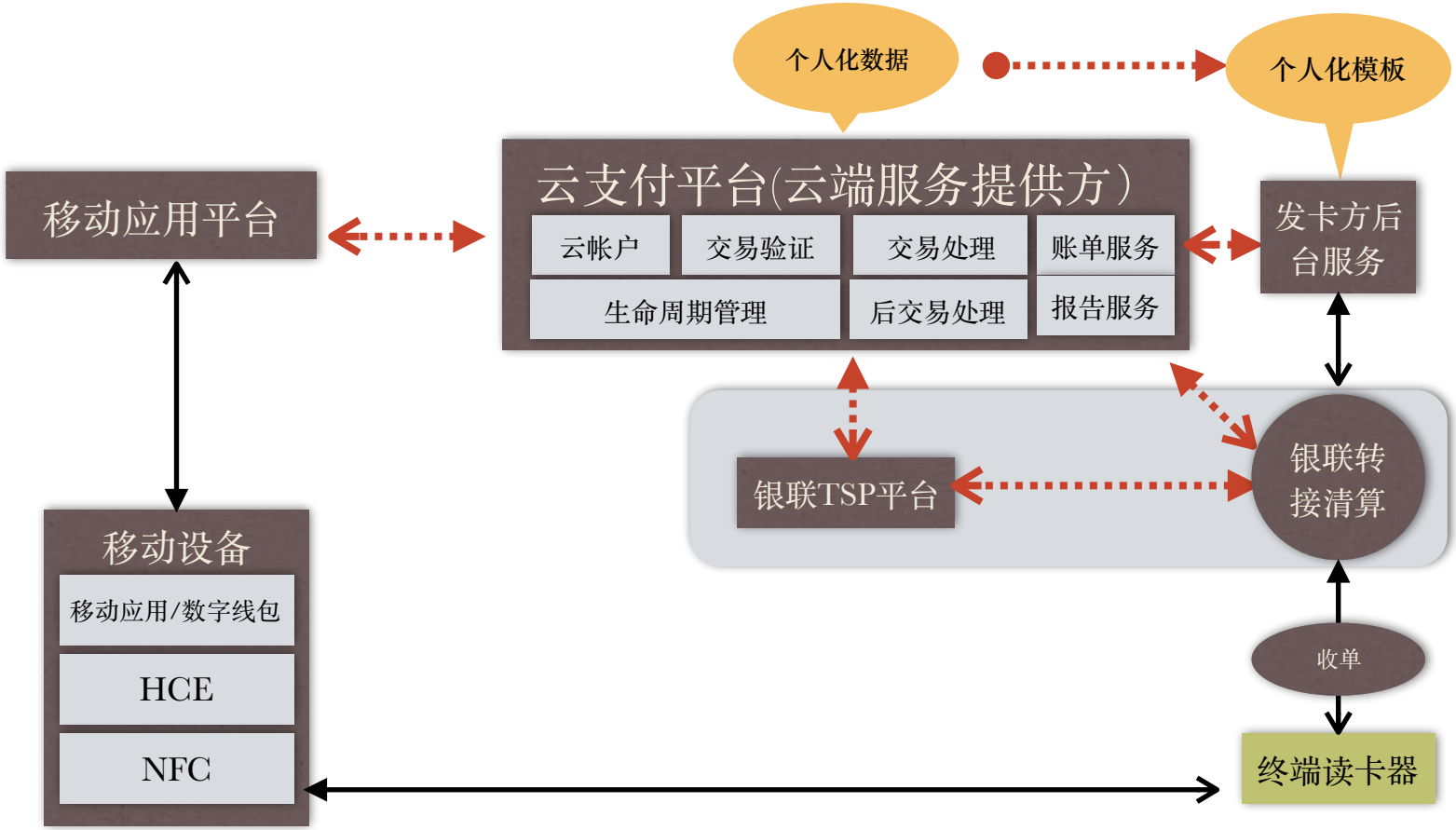
CONTENT

1

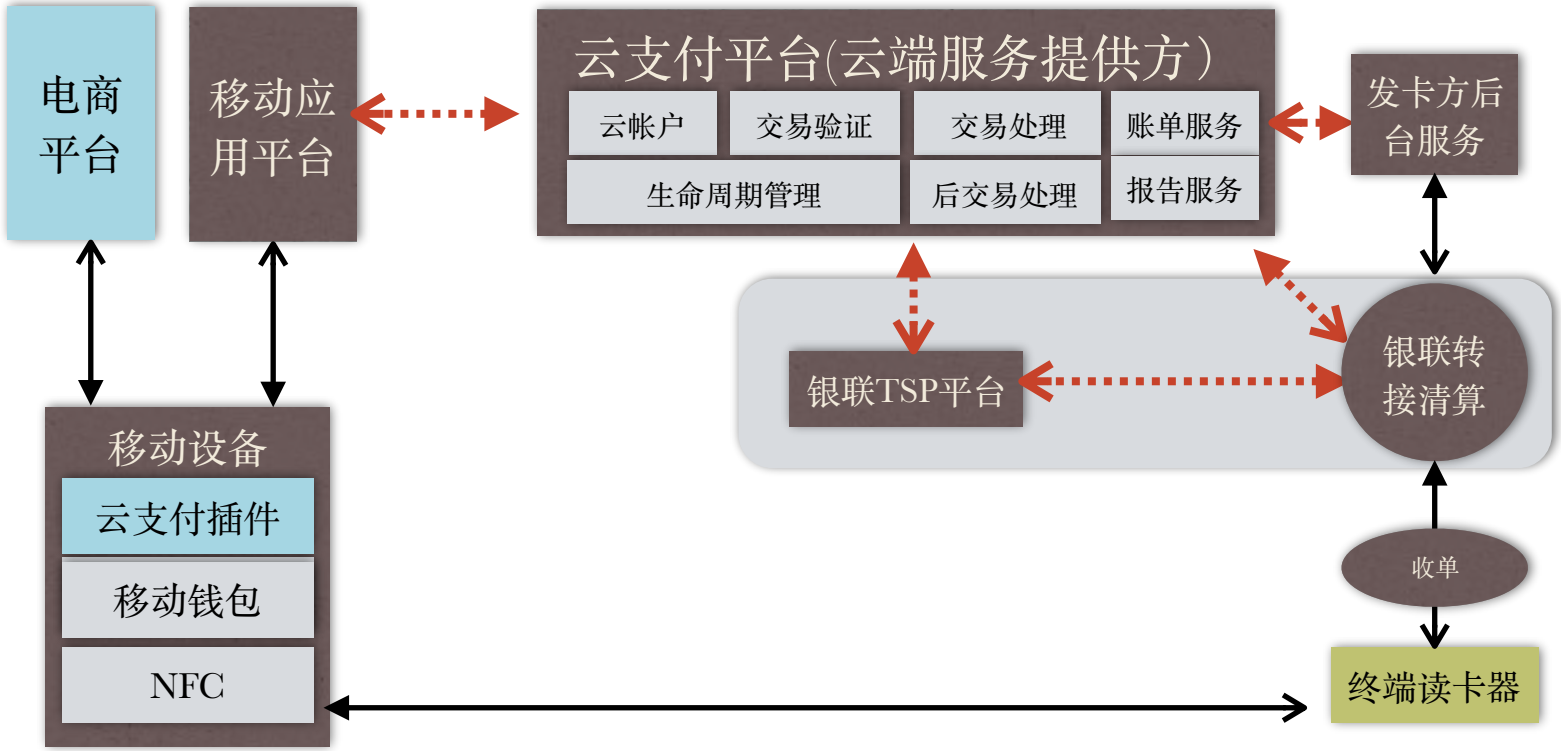
PART ONE

银联关于HCE的架构

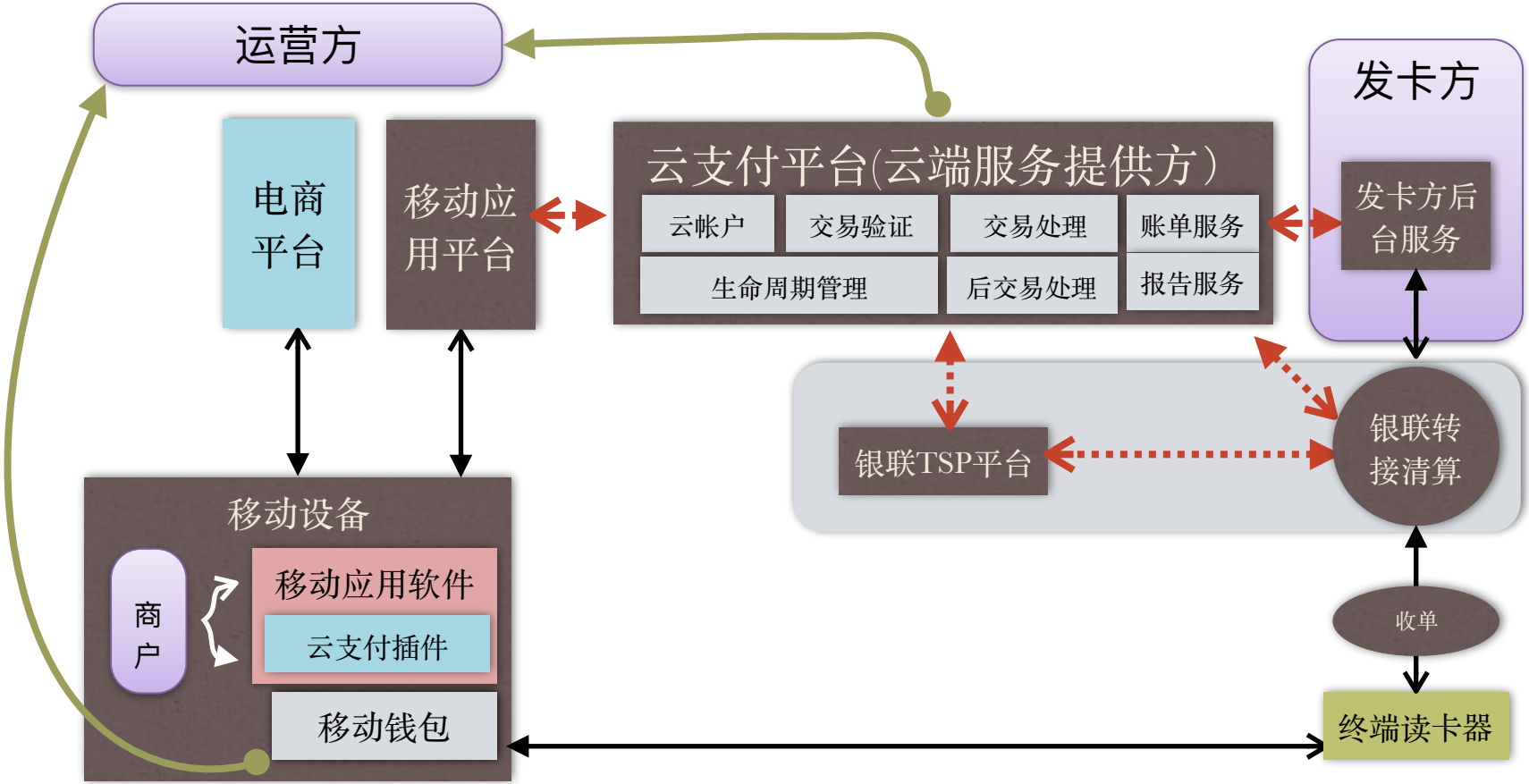
银联HCE发卡架构


个人化数据
个人化模板
移动应用平台
云支付平台(云端服务提供方)
云帐户
交易验证
交易处理
账单服务
生命周期管理
后交易处理
报告服务
发卡方后台服务
银联TSP平台
银联转接清算
移动设备
移动应用/数字线包
HCE
NFC
收单
终端读卡器

银联HCE架构与电商的关系



银联HCE架构产业链间的关系



2

PART TWO

银联关于HCE的交易流程说明

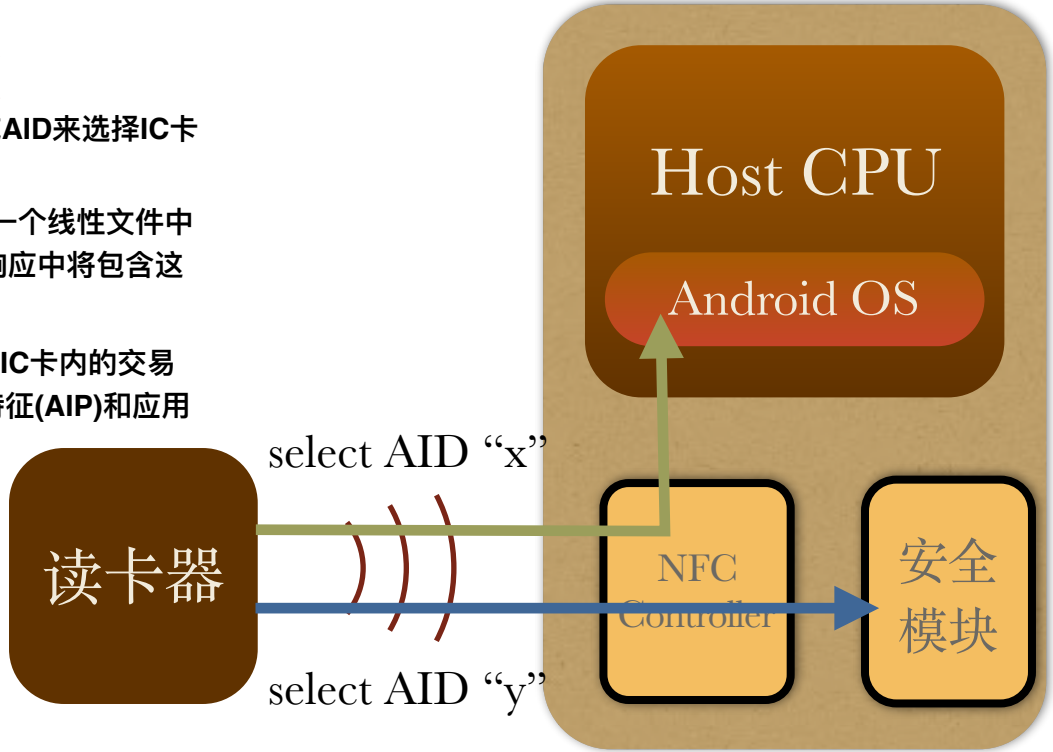
NFC终端交易指令要求

APDU指令只能来自NFC控制器，否则一律不接收
可接收指令列表：

SELECT 命令：选择(SELECT)命令通过文件名或AID来选择IC卡中的PPSE或支付应用的AID。

ReadRecord ：读记录(READ RECORD)命令从一个线性文件中读一条文件记录。从IC卡返回的响应中将包含这条被读出的记录。

GPO 命令 ：获取处理选项(GPO)命令用来启动IC卡内的交易IC卡的响应报文中包含应用交互特征(AIP)和应用文件定位器(AFL)。



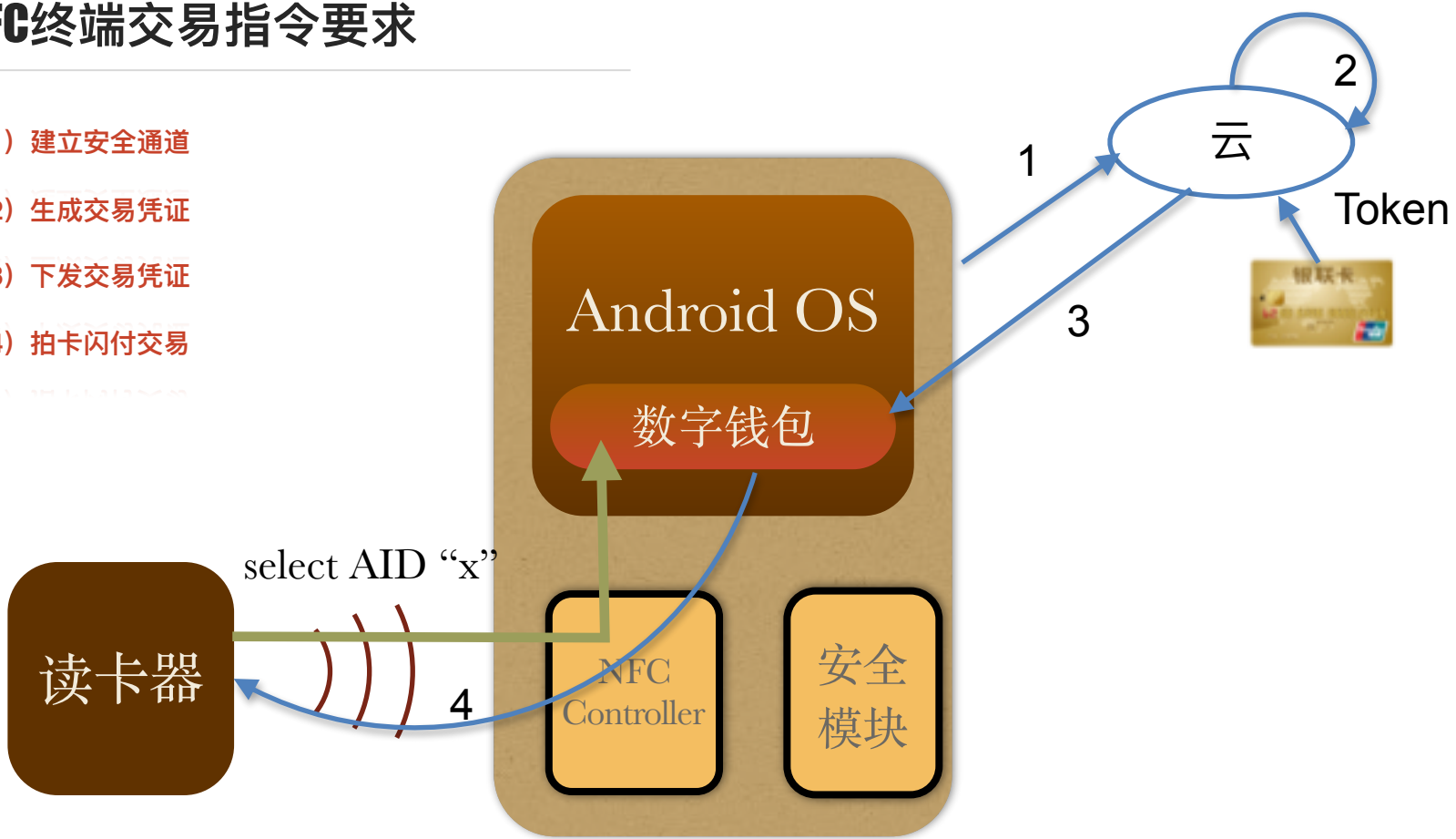
NFC终端交易指令要求

(1) 建立安全通道

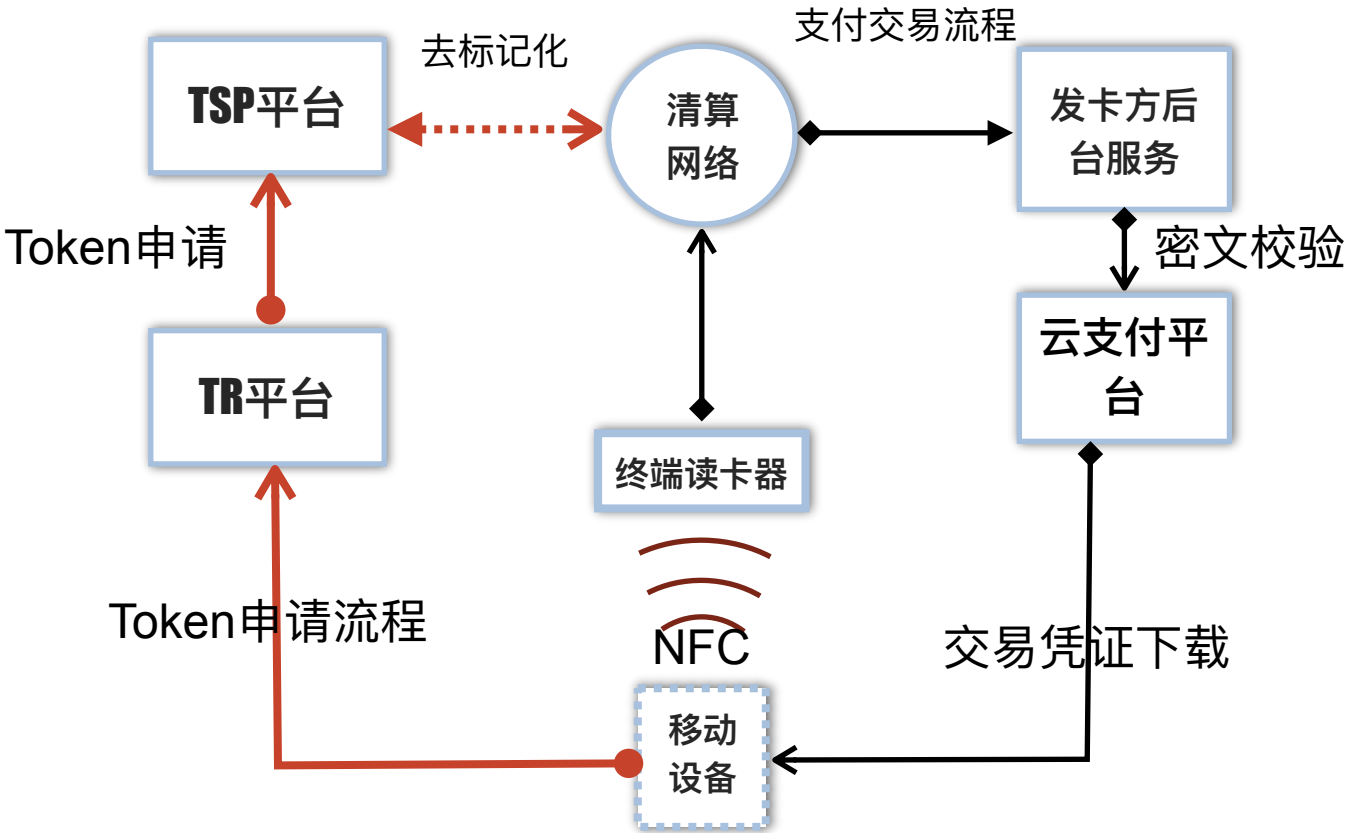
(2) 生成交易凭证

(3) 下发交易凭证

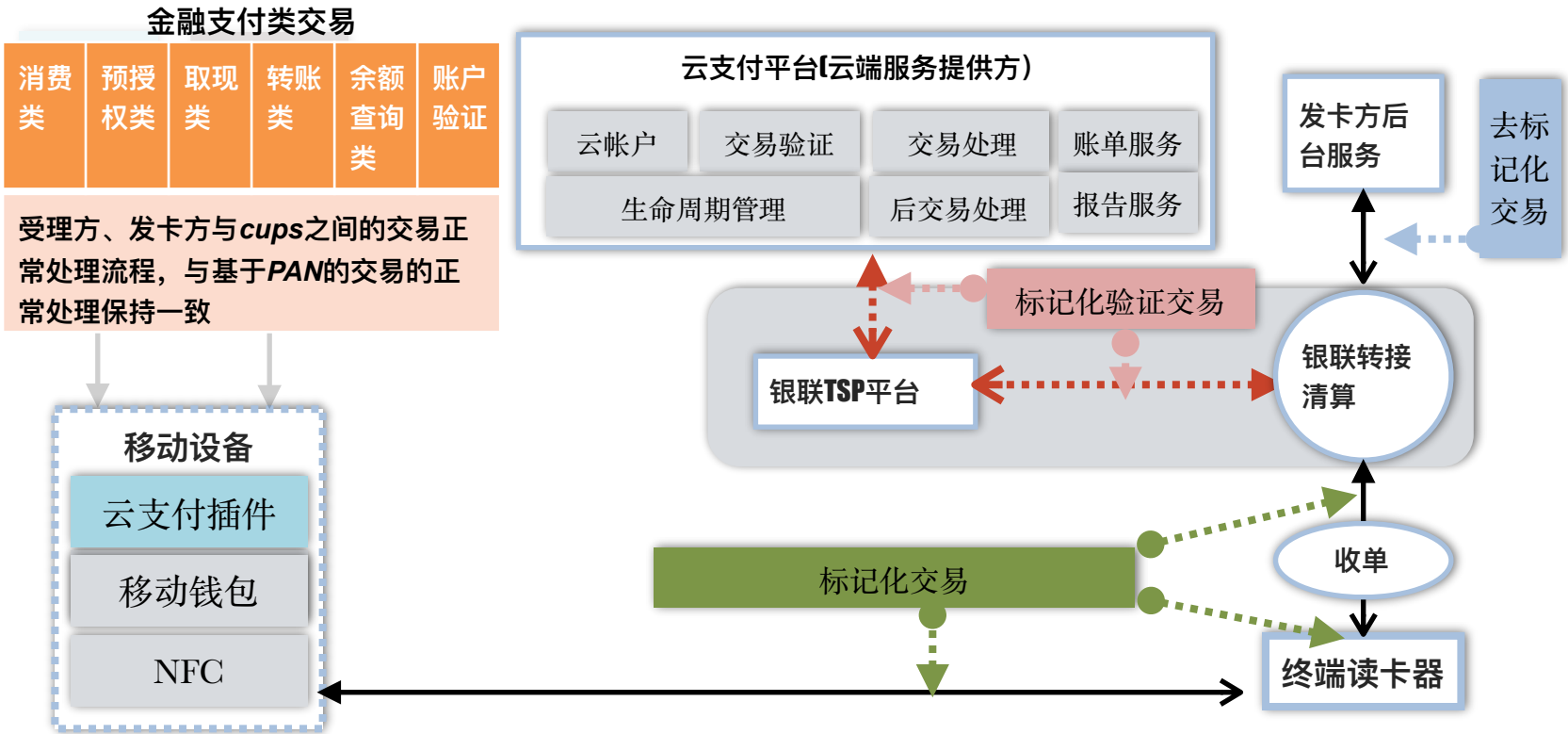
(4) 拍卡闪付交易



银联HCE架构中的支付流程及要素

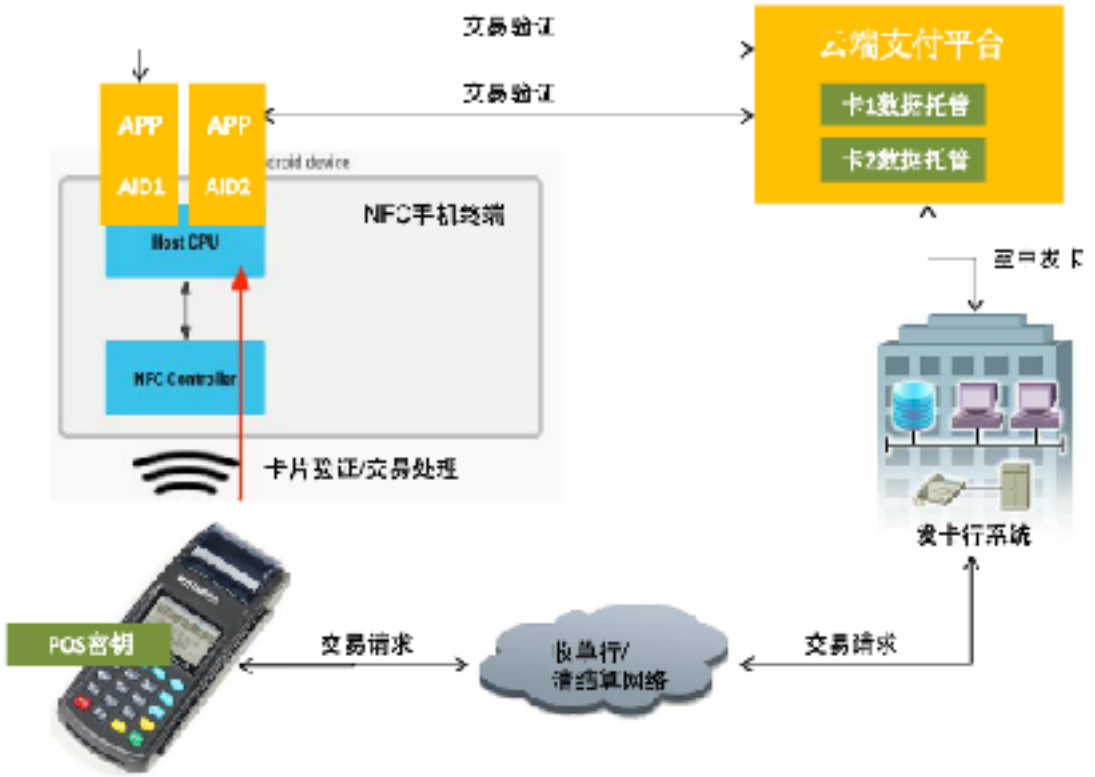


银联HCE架构中的支付流程及要素



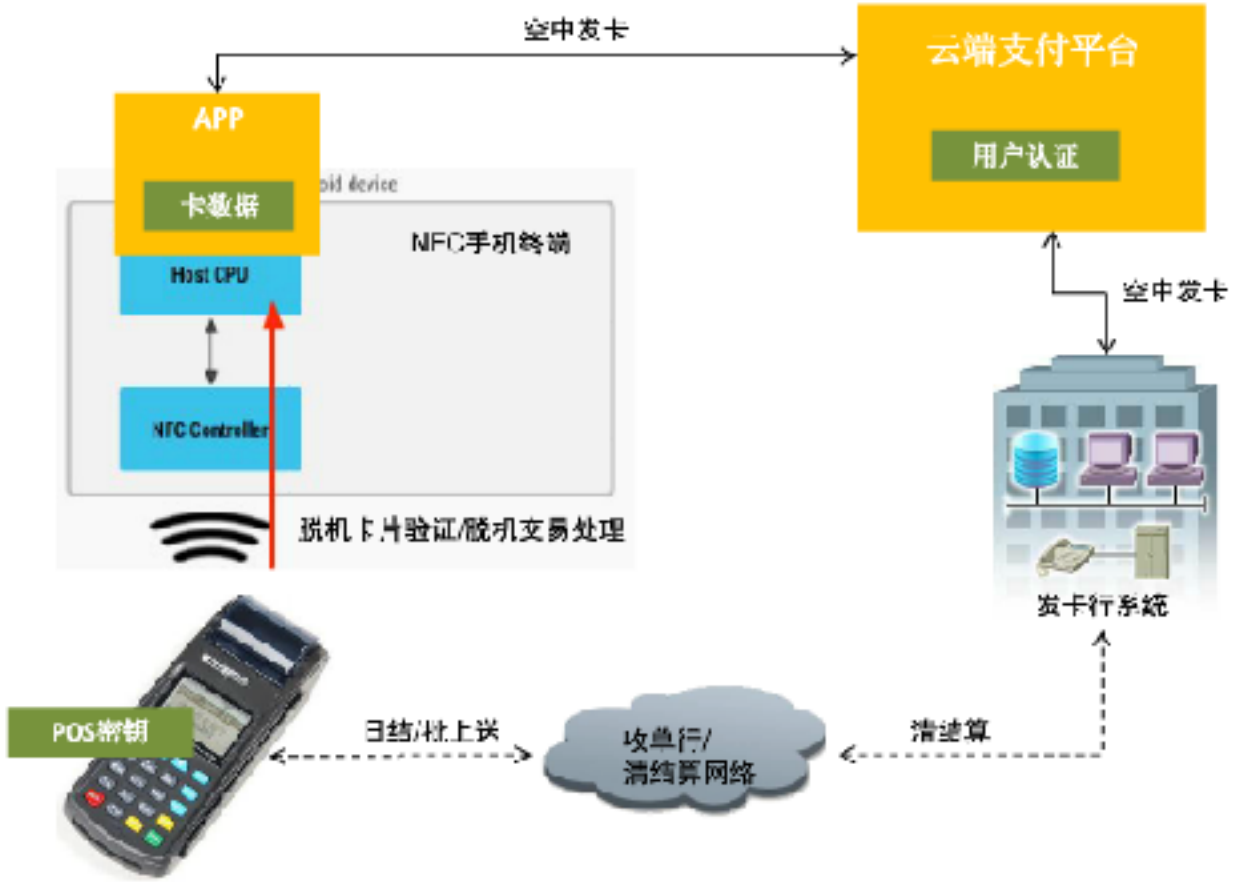
银联HCE架构中的支付业务模型

云端支付业务模型



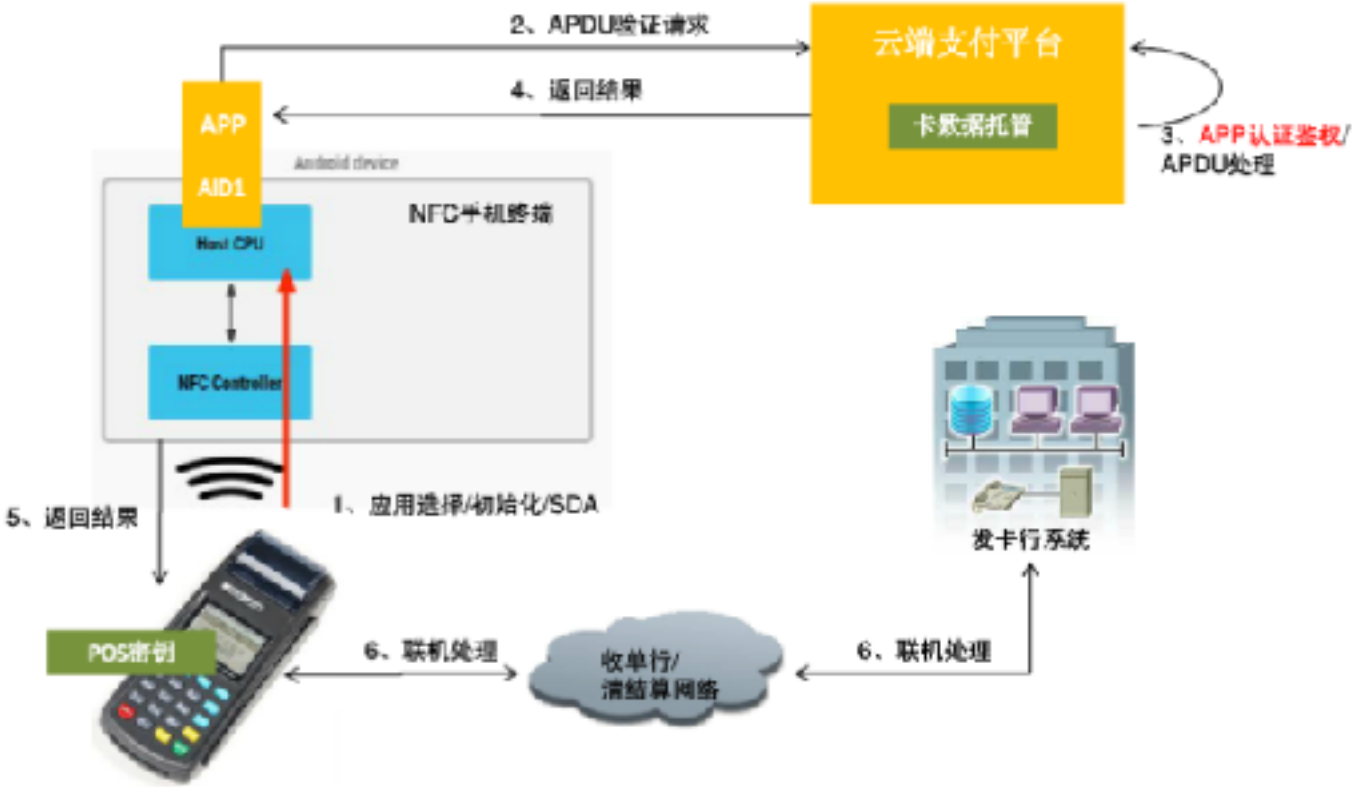
银联HCE架构中的支付业务模型

前端支付业务模型



银联HCE架构中的支付业务模型

云端支付业务流程

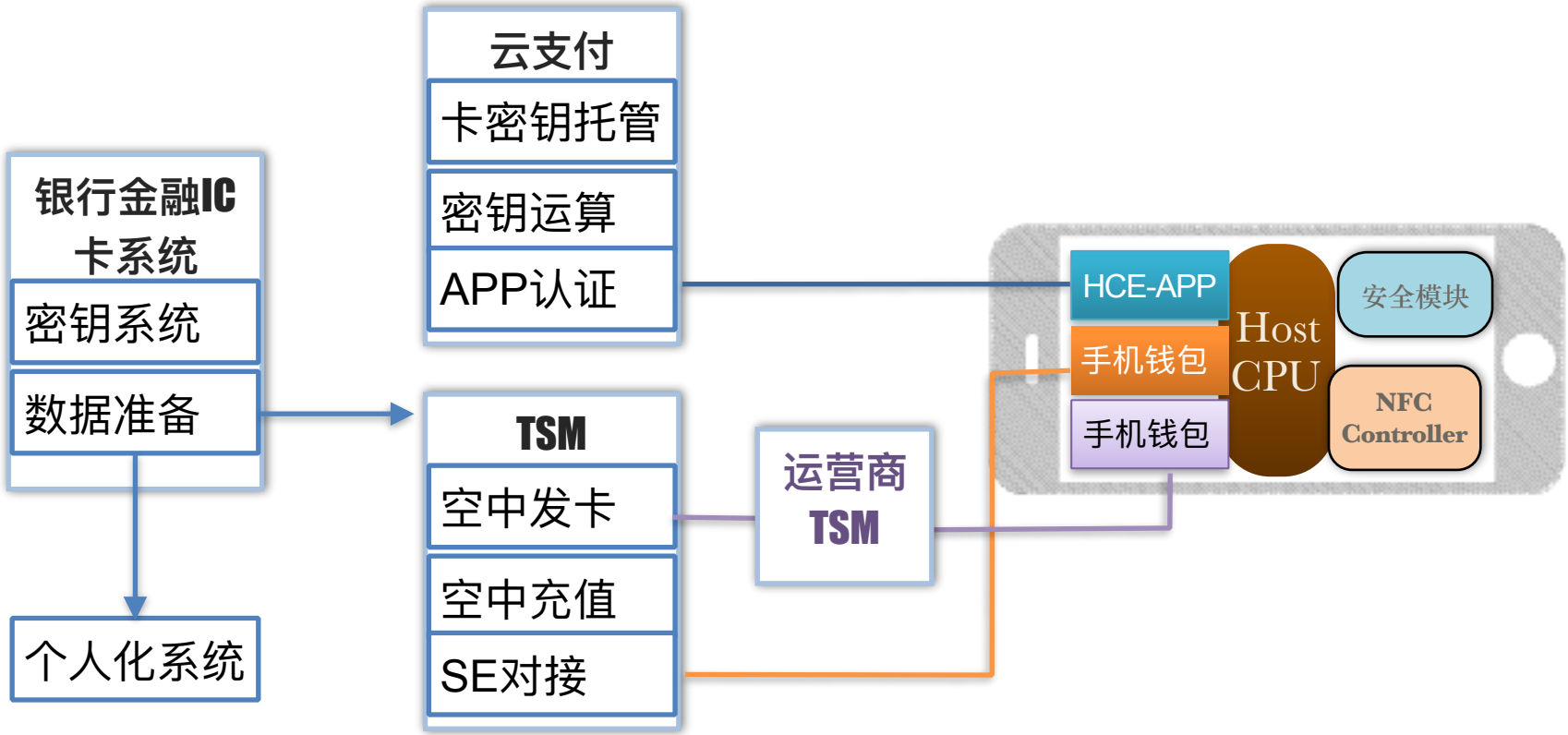


银联HCE架构中的支付业务模型

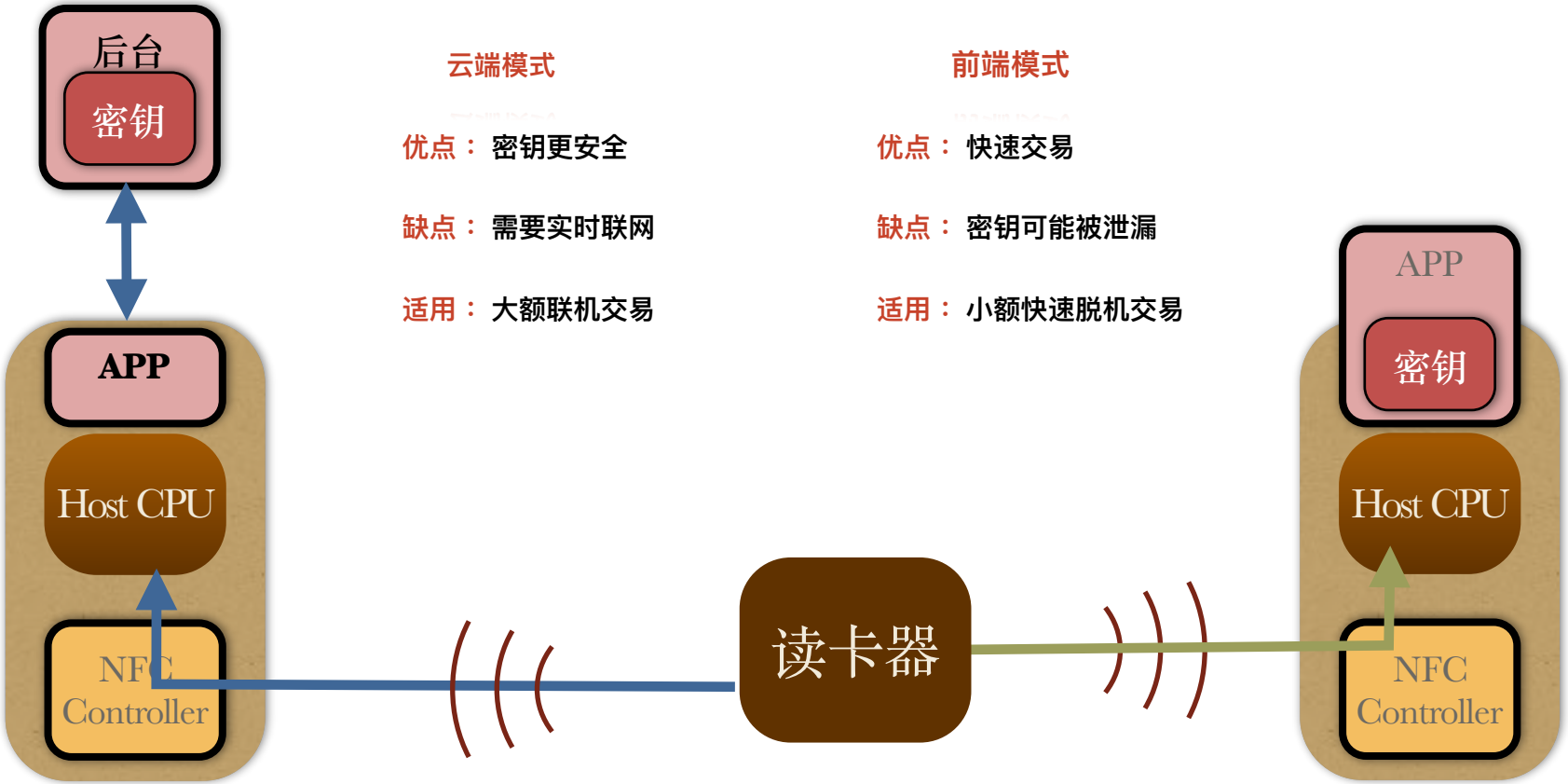
云端支付发卡流程

3、用户身份验证

银行HCE支付系统架构



NFC终端两种认证方式



云端模式

优点： 密钥更安全

缺点： 需要实时联网

适用： 大额联机交易

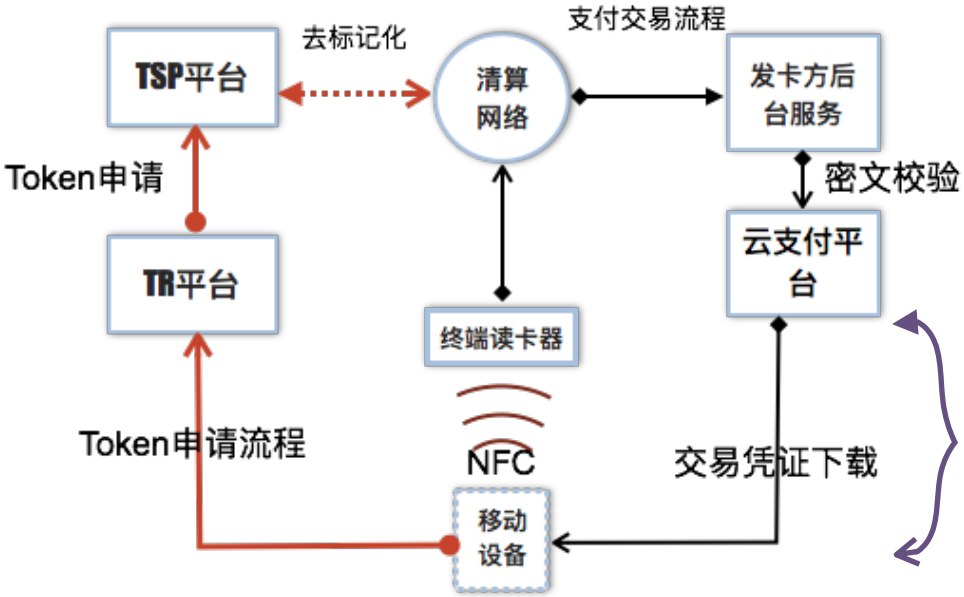
前端模式

优点： 快速交易

缺点： 密钥可能被泄漏

适用： 小额快速脱机交易

银联HCE架构中的支付安全性



敏感数据：
- 云存储
- 下载加密
- 终端安全存储使用

通讯安全：TLS/SSL

银联HCE架构中的支付流程数据说明

金融支付类交易

消费类	预授权类	取现类	转账类	余额查询类	账户验证
消费（一次性付款）					
消费（一次性付款）冲正					
受理方、发卡方与cups之间的交易正常处理流程，与基于PAN的交易的正常处理保持一致					

银联HCE架构中的支付流程63域数据说明

金融支付类交易

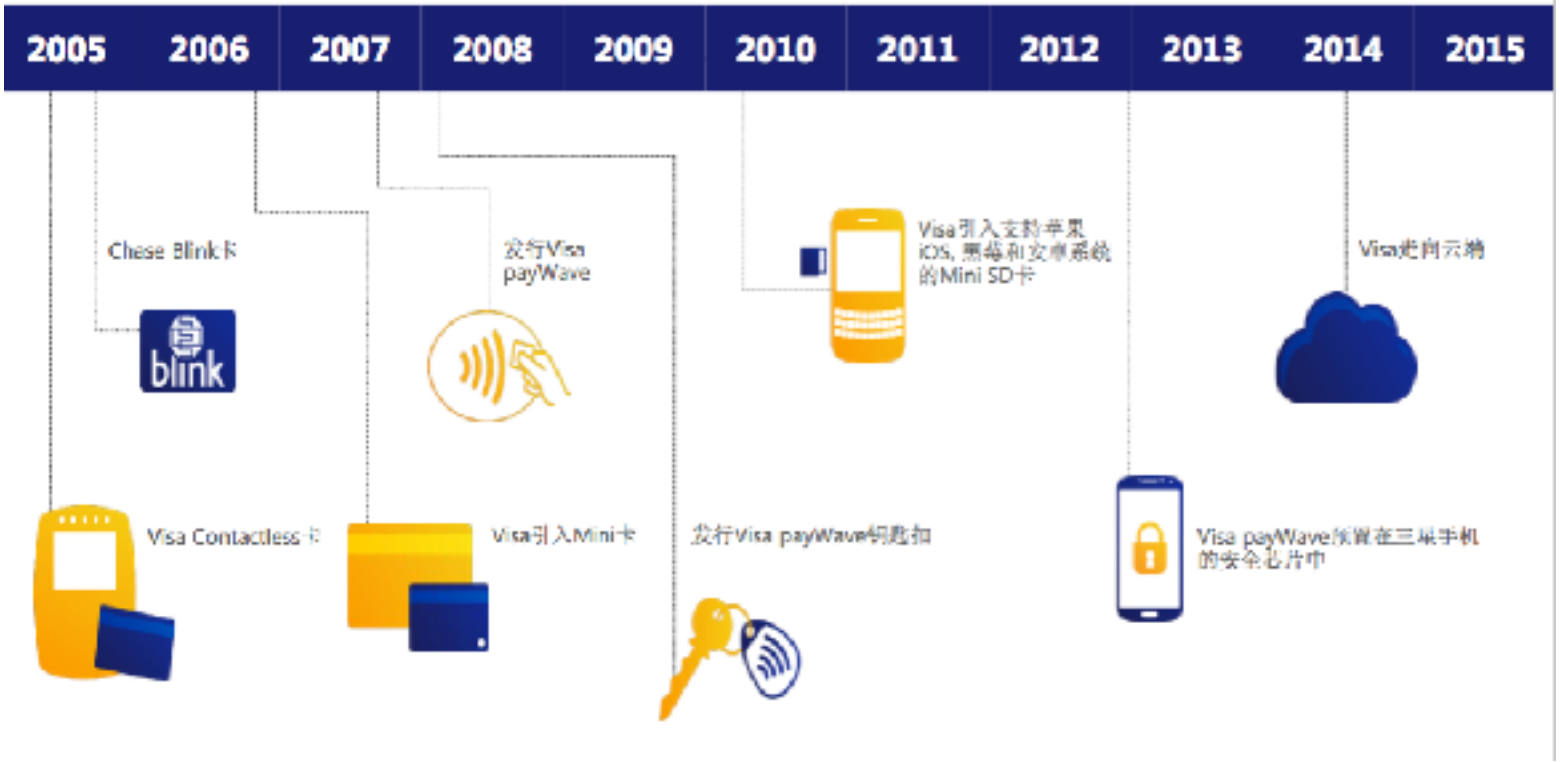
子域名称	tag标签	子域属性	子域说明
银联是否验证token	1	an1	
token	2	an..19(LLVAR)	
有效期	3	an4	
担保级别	4	an..2(LLVAR)	
应用场景	5	n2	

3

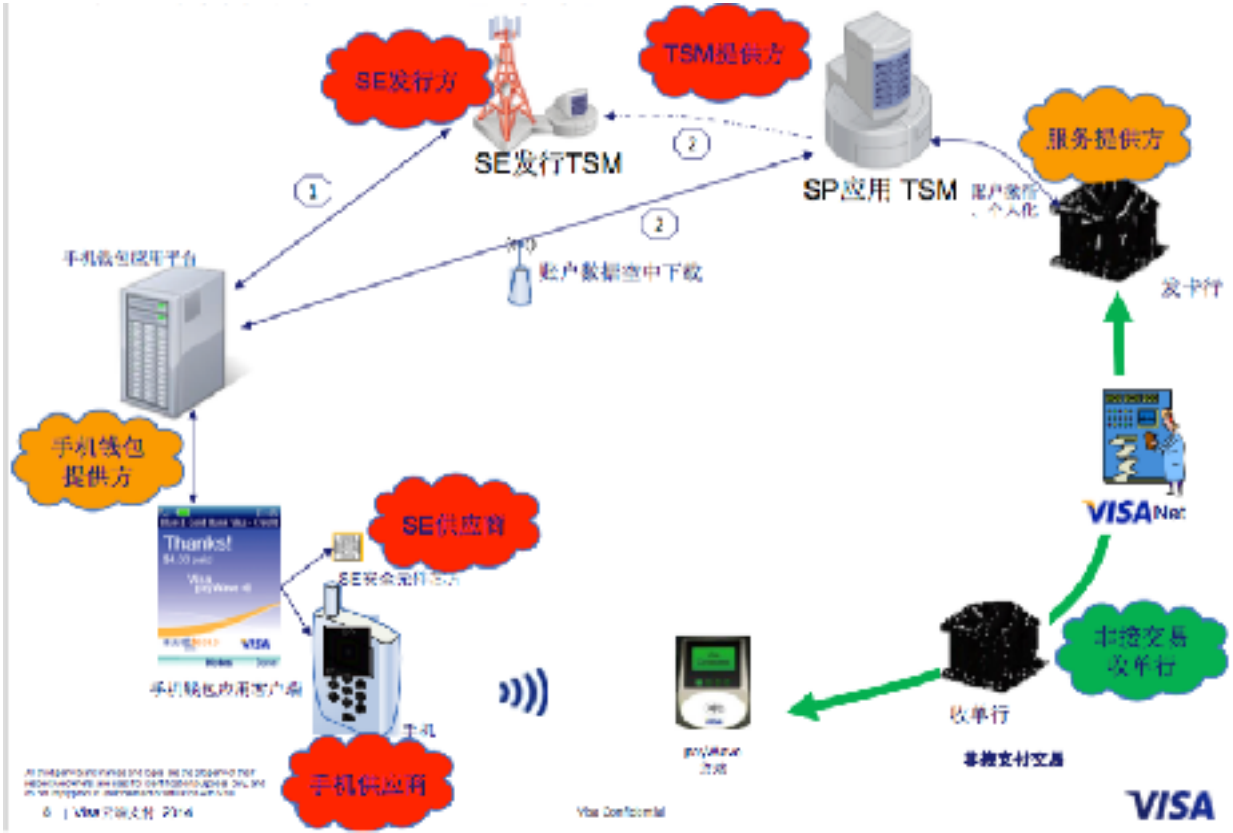
PART THREE

visa 移动支付体系建设介绍

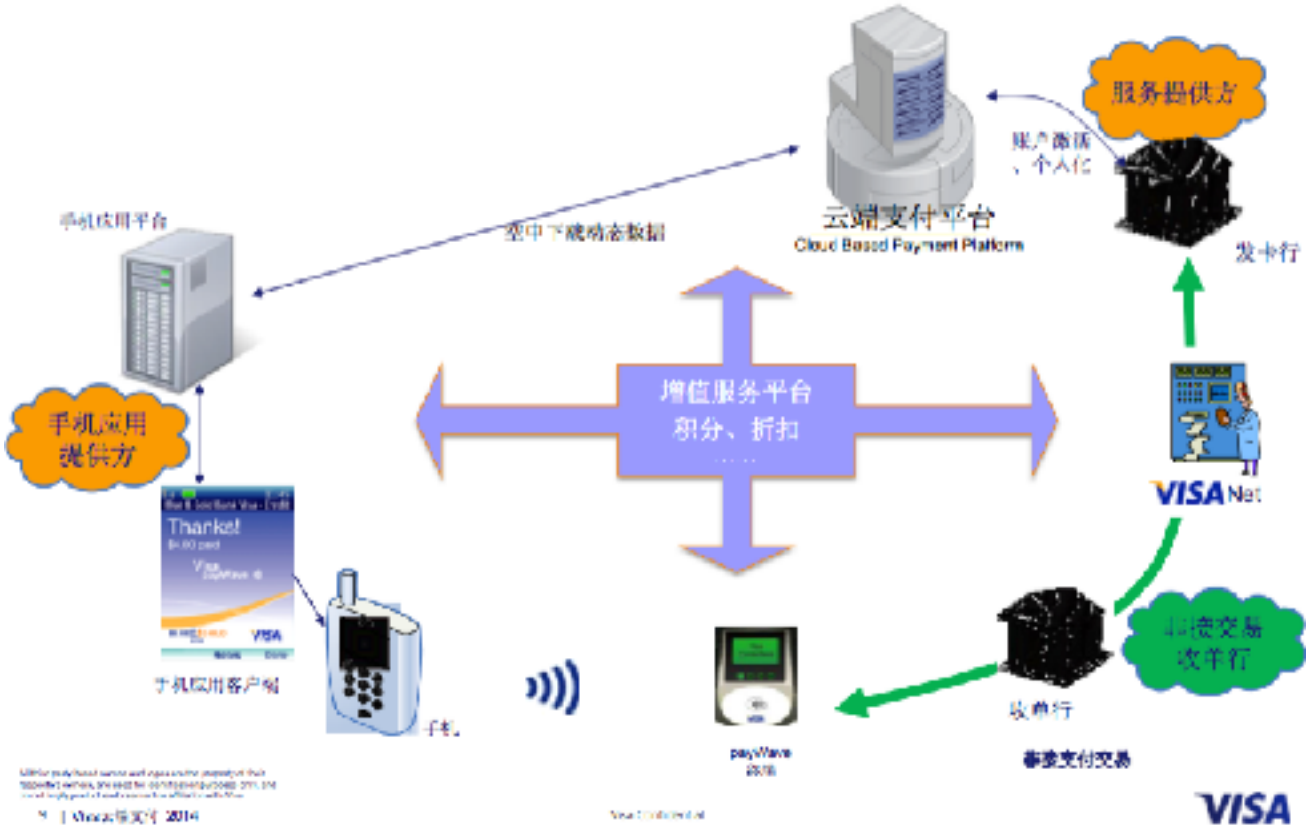
visa在移动支付上历程



目前基于SE的移动非接支付生态系统



目前的移动非接支付生态系统



Visa Cloud Based Payment(VCBP)

HCE

Host Card Emulation　主机芯片模拟

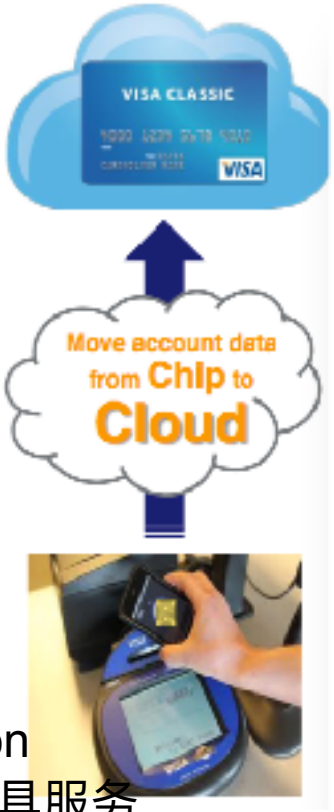
A new feature in Android 4.4(kit kat)that allows any NFC application on an Android device to emulate a smart card　新增功能允许手机应用模拟安全芯片

Cloud-Based Payments

Payments that are enabled by accounts that are managed in systems residing in a network rather than in secure hard ware solutions inside the mobile device 安全芯片云端化方案

Visa Cloud Based Payment(VCBP)

Provides standards,specifications,tools,and services to issuers, merchants,and 3rd party partners that enable a systems solution for cloud-based payments 面向整个交易链条的标准、规范、工具服务



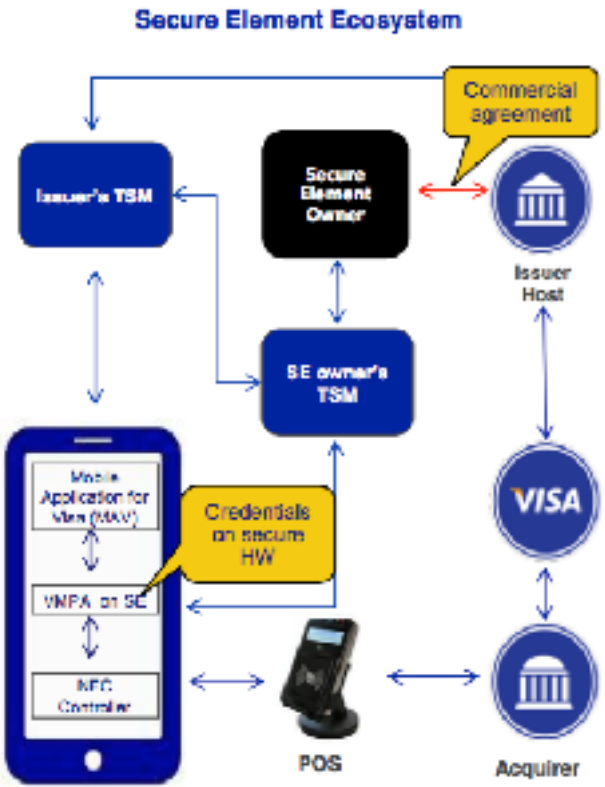
on-Device vs. Cloud-Based Payments+HCE

Secure Element

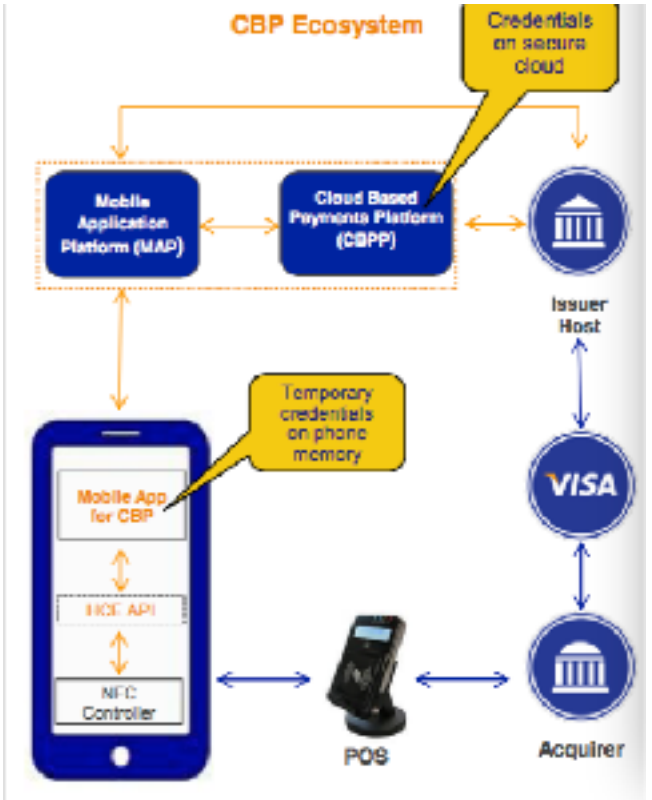
Host Card Emulation

on-Device vs. Cloud-Based Payments+HCE

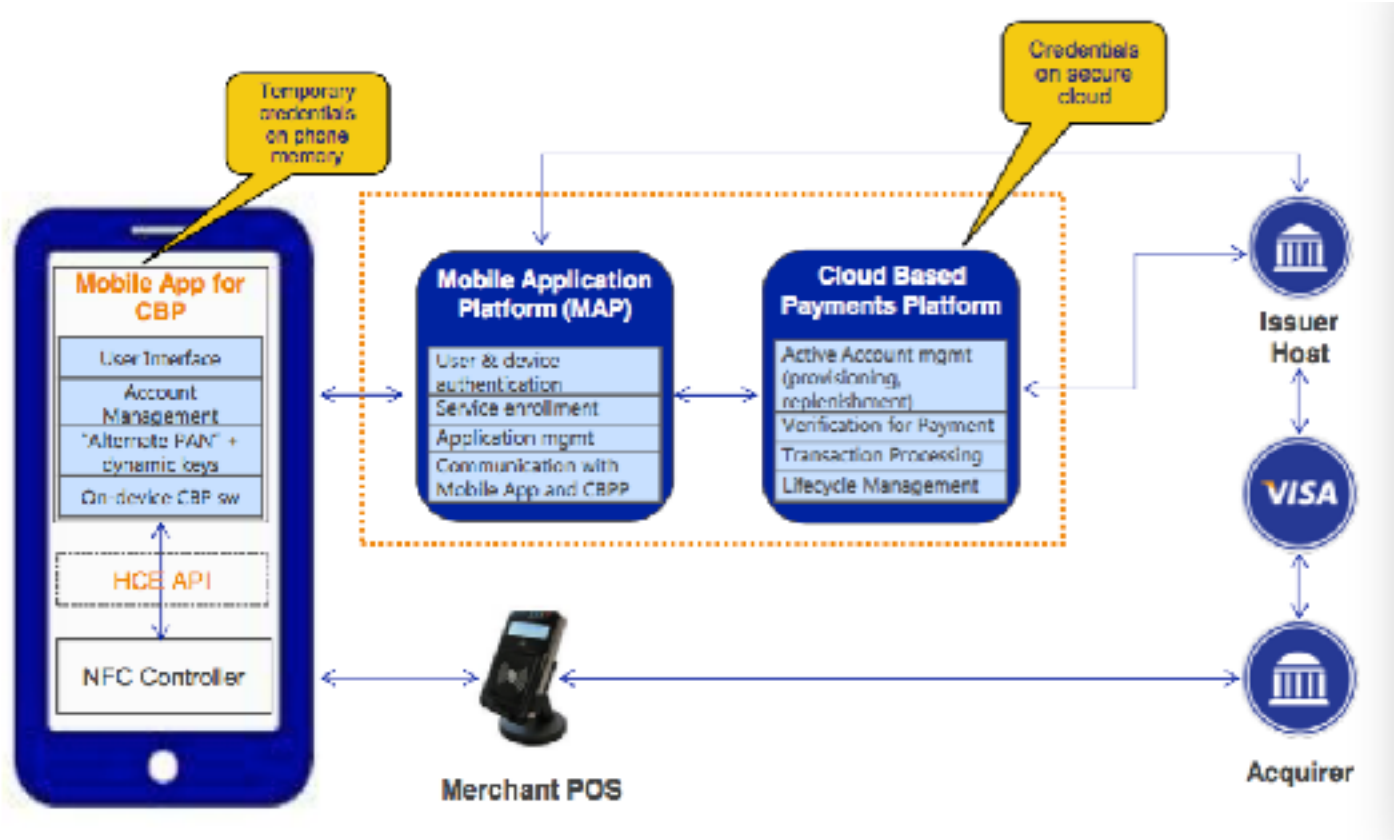
Secure Element



Host Card Emulation



Core Functions needed for Cloud-Based Payments



How to ensure the security

Multiple layers of security measures collectively ensure the security of the ecosystem 多层级的综合安全

- Dynamic chip based cryptography 动态的交易验证码
- Tokenization or alternate PAN 隔离帐户数据
- Storing and processing sensitive data on a server “in the cloud” 云端存储
  To ensure the card data is secured on the phone 移动终端上的数据安全
- Mobile Payment Application Security 移动支付应用安全性
- Operating Systems check for rooting, malware, viruses OS提供的安全性
- Payment data lifecycle management 帐户信息的生命周期管理

4

PART FIVE

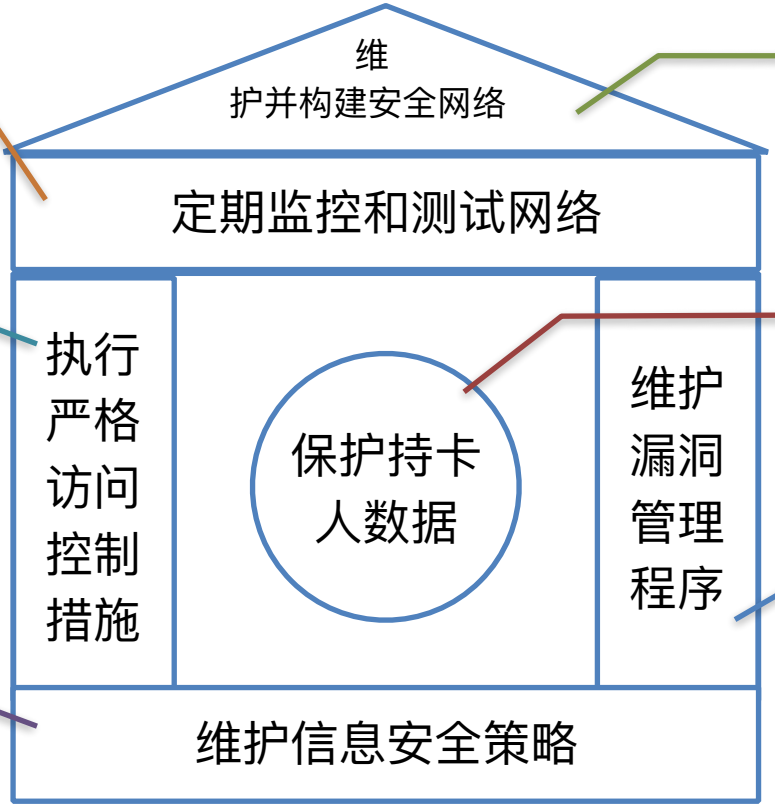
关于数据安全中的PCI规范思想

支付卡行业 (PCI) 数据安全标准

制定支付卡行业 (PCI) 数据安全标准 (DSS) 以促进并提高持卡人数据安全,有利于全球广泛采用统一的数据安全标准。

PCI 数据安全标准 要求和安全评估程序将 12 条 PCI DSS 要求作为基础,并将这些要求与相应的测试程序融入到安全评估工具中。此标准的设计目的是供评估者使用,以对必须验证 PCI DSS 合规性的商家和服务提供商进行现场评估。

支付卡行业 (PCI) 数据安全标准—安全体系结构



要求10：跟踪和监控访问网络资源和持卡人数据的所有操作

要求11：定期测试安全系统和流程

要求1：安装防火墙配置并予以保护

要求2：不要使用默认的系统密码及其它参数

要求7：只有业务需求人才可访问

要求8：为每位访问计算机的人员分配唯一的标识

要求9：限制对持卡人数据的物理访问

要求3：保护持卡人数据

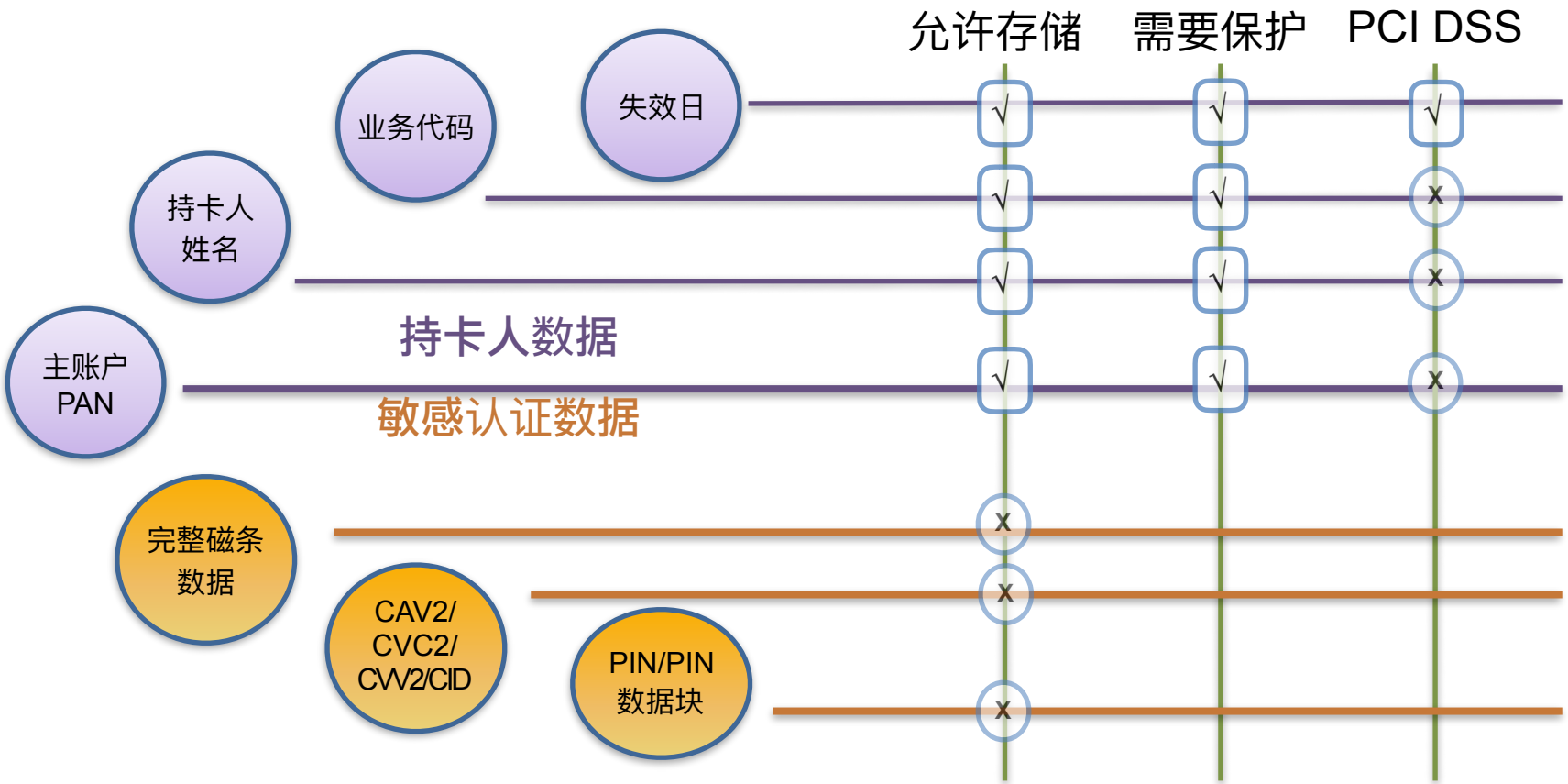
要求4：开放型的公共网持卡人数据加密

要求5：杀毒软件并更新

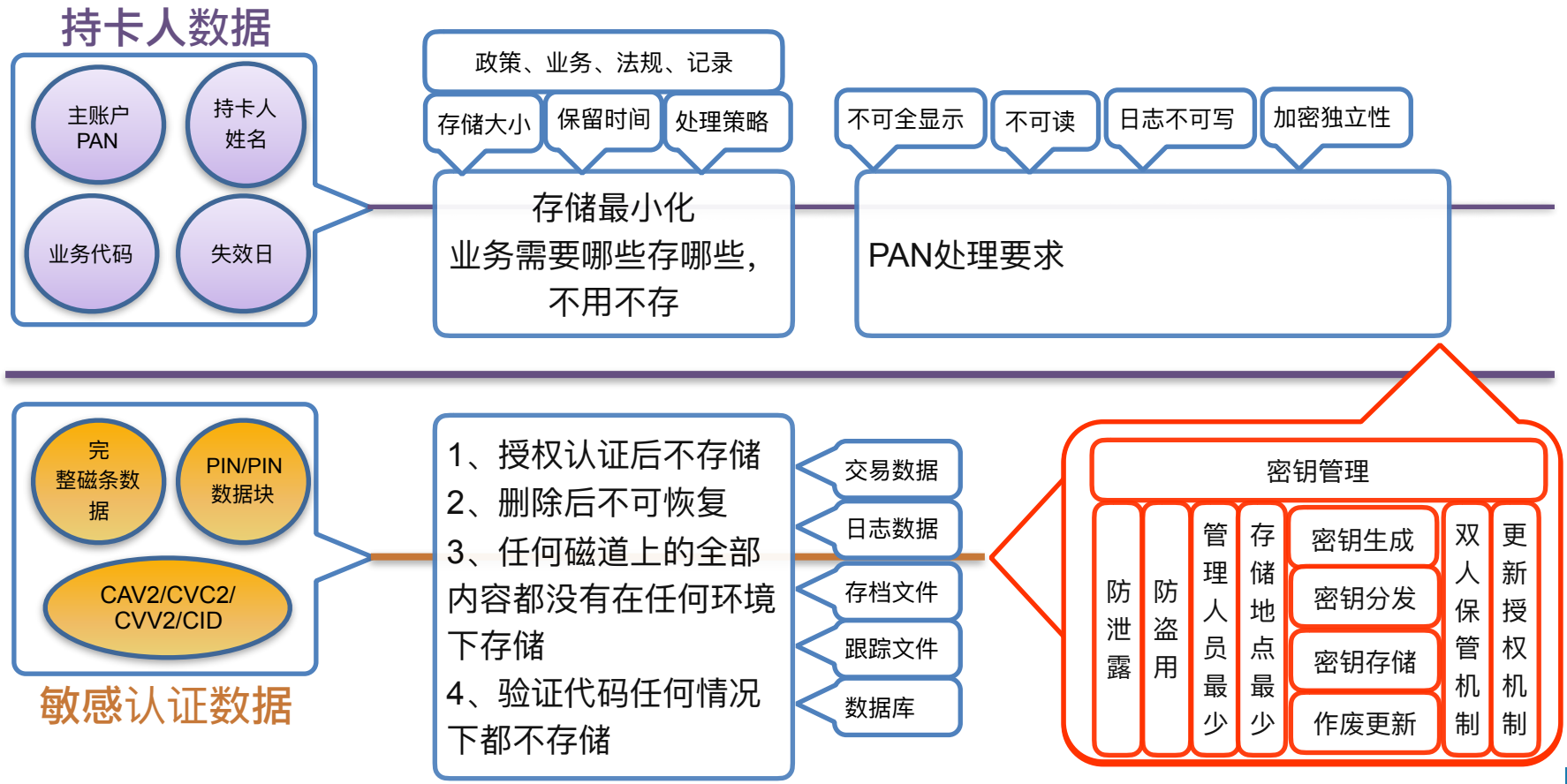
要求6：开发维护安全系统和应用程序

要求12：维护针对信息安全的政策

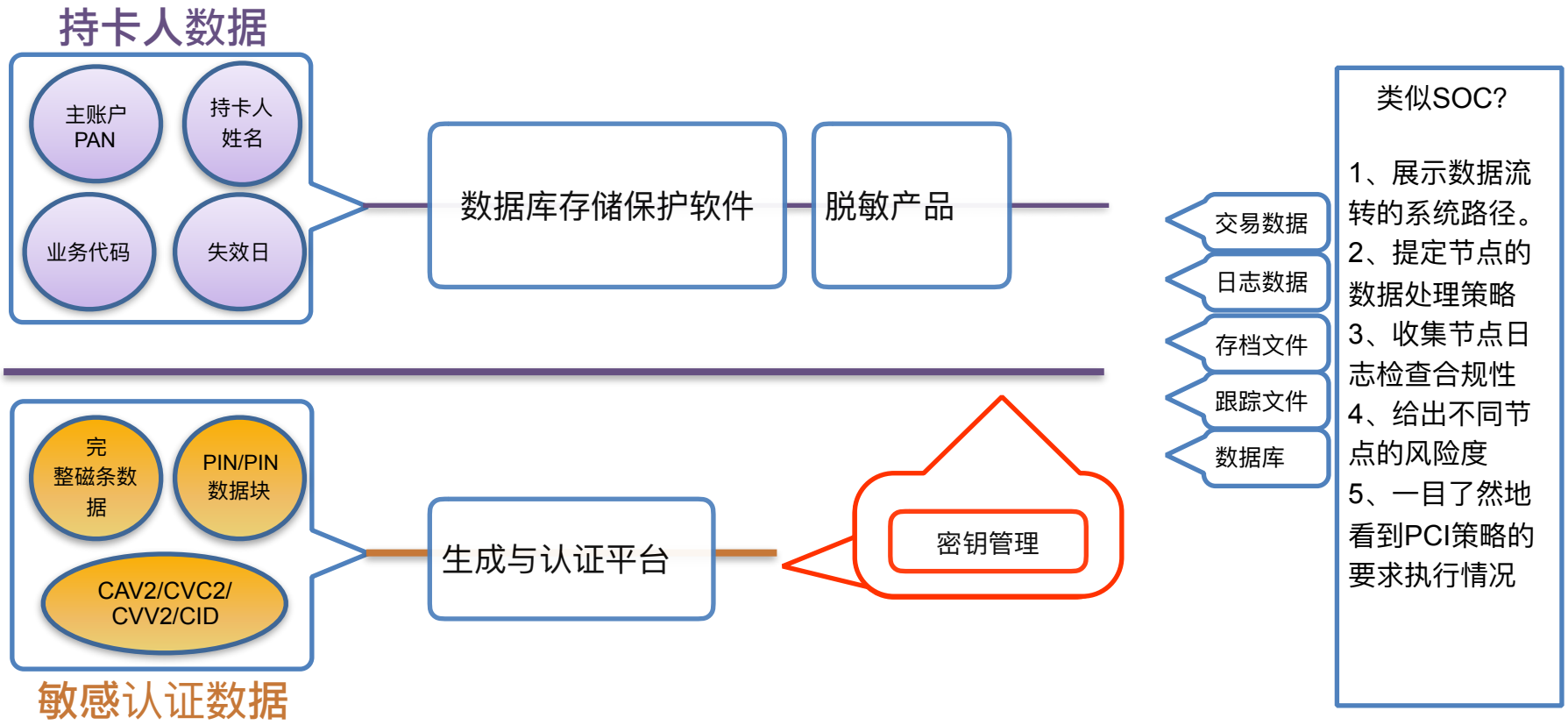
支付卡行业 (PCI) 数据安全标准—需要保护的核心数据对象



支付卡行业 (PCI) 数据安全标准—保护持卡人数据对象具体要求



支付卡行业 (PCI) 数据安全标准—根据这些要求可能会出现的产品

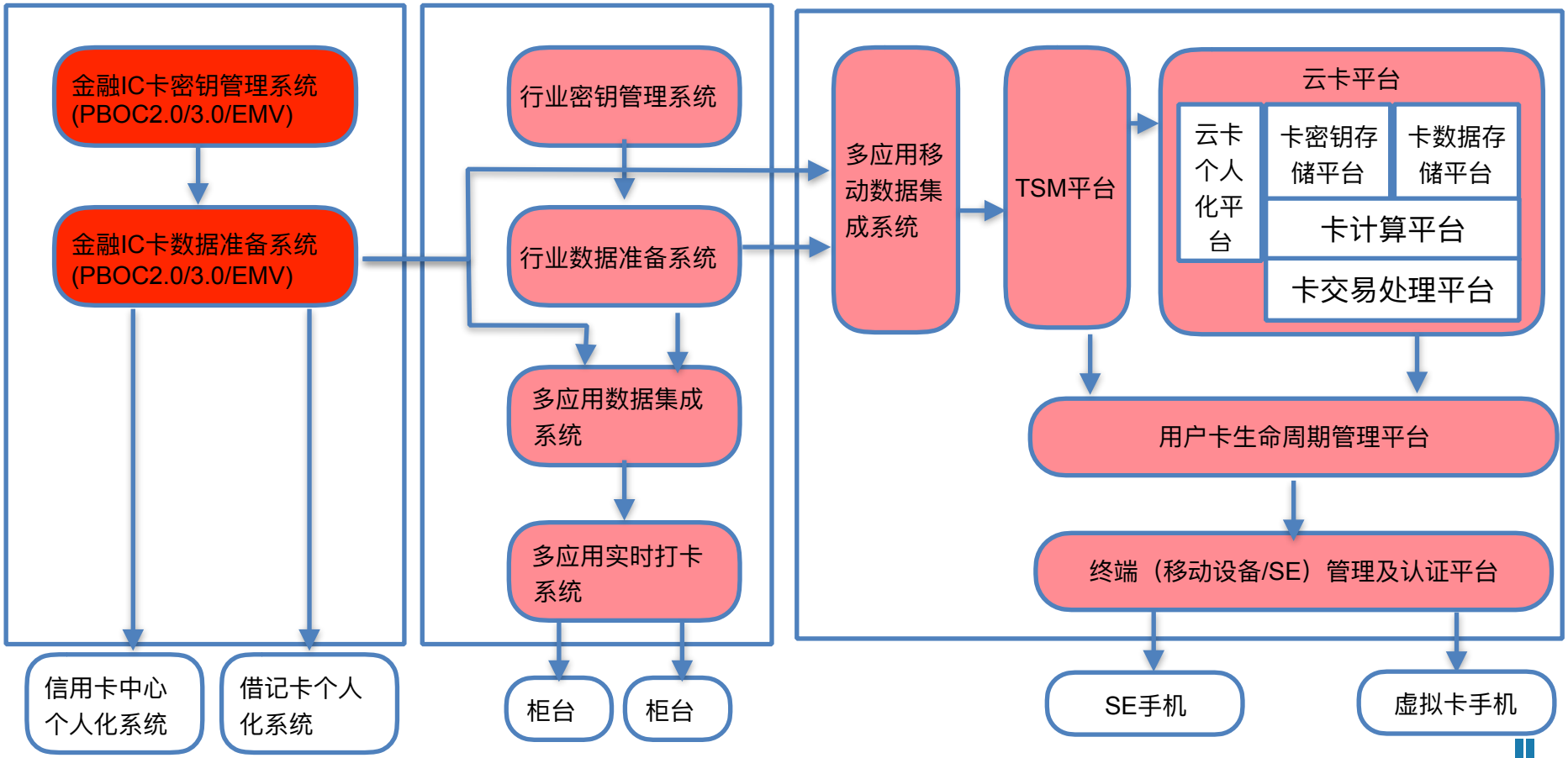


3

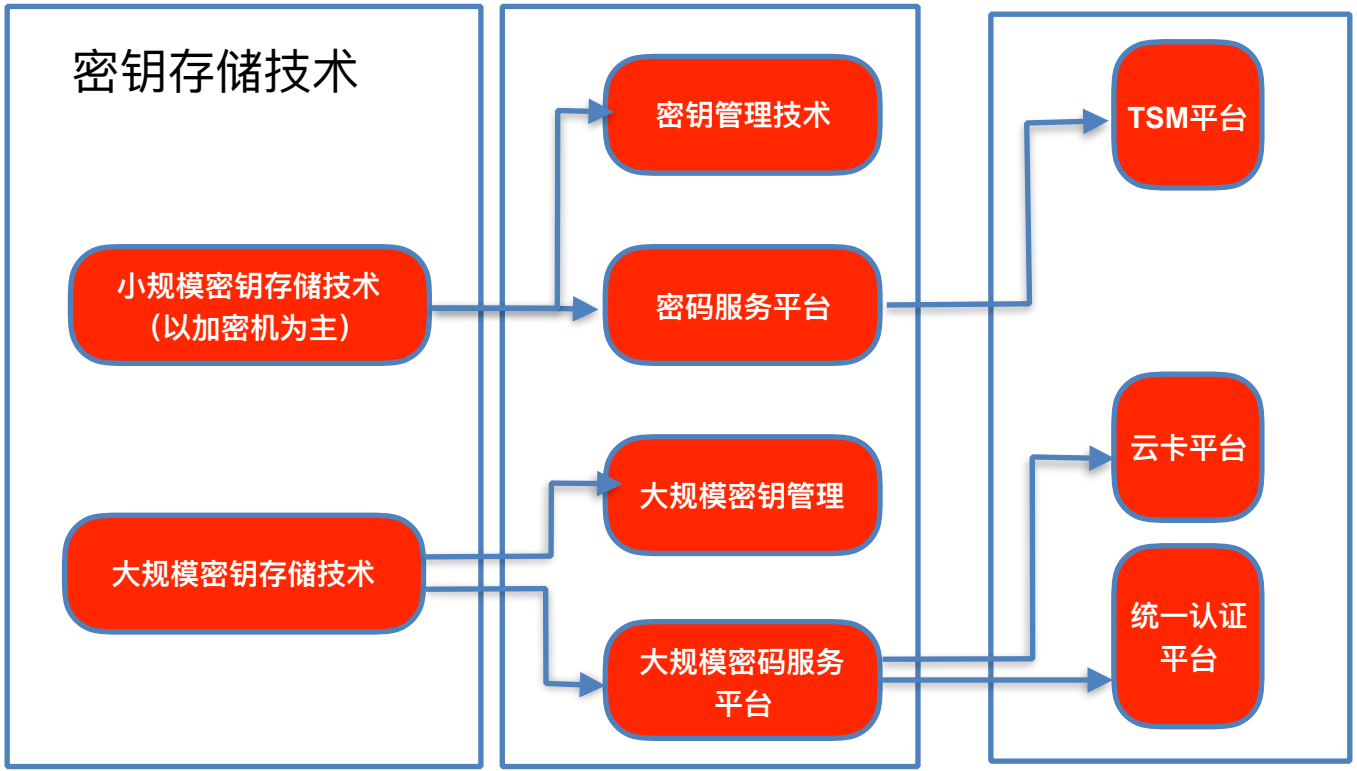
PART THREE

产品思路整体规划

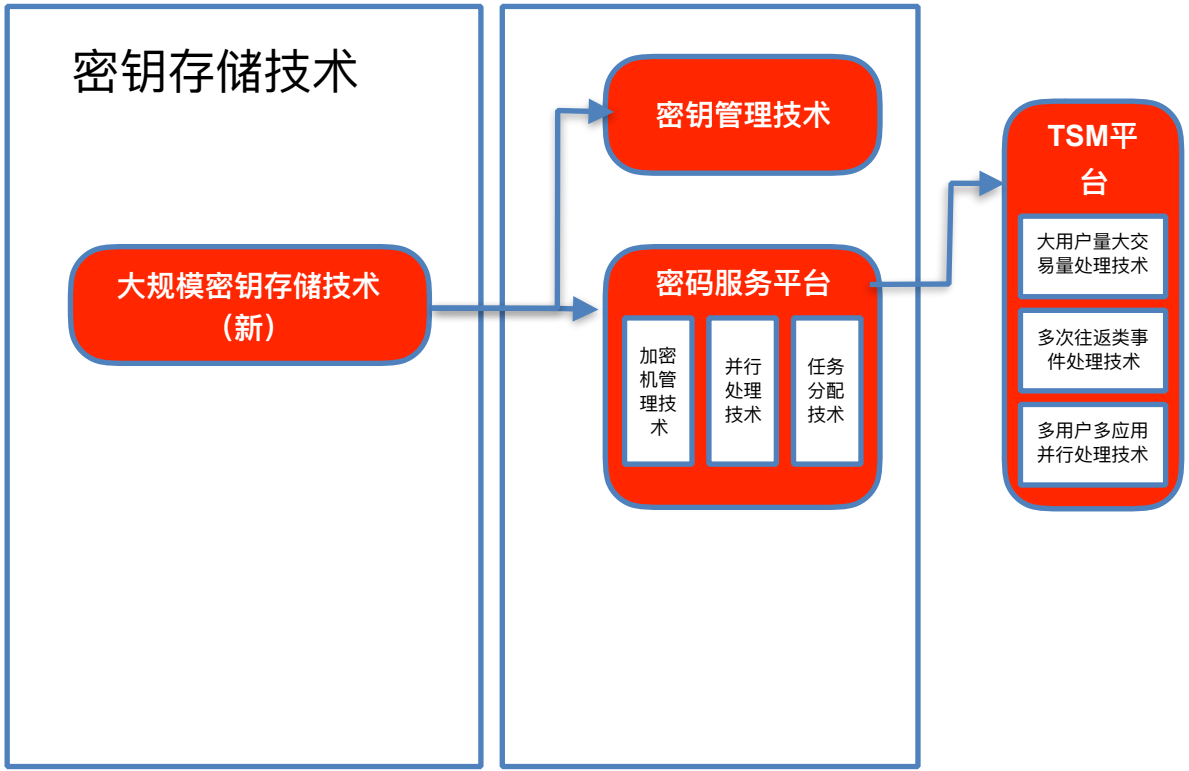
金融IC卡整体解决方案



密码产品发展路线


密钥存储技术
小规模密钥存储技术
（以加密机为主）
大规模密钥存储技术
密钥管理技术
密码服务平台
大规模密钥管理
大规模密码服务
平台
TSM平台
云卡平台
统一认证
平台

密码产品发展路线与技术沉淀的关系



1、密钥存储技术—加密设备应用技术
2、密钥管理技术。
3、任务分配与并行处理技术
4、大用户量大交易量处理技术
5、多次往返类事件处理技术
6、多用户多应用并行处理技术

密码产品发展路线与应用销售的关系

密钥存储技术

小规模密钥存储技术
（以加密机为主）

小规模密钥存储技术的特点

小规模密钥存储技术是指以加密机、加密卡为基础，存储和使用的技术。它的特点是：

1）存储的密钥少，多以对称密钥的应用为主，非对称密钥为辅。

2）对称密钥多以分散为主要的密钥产生方法

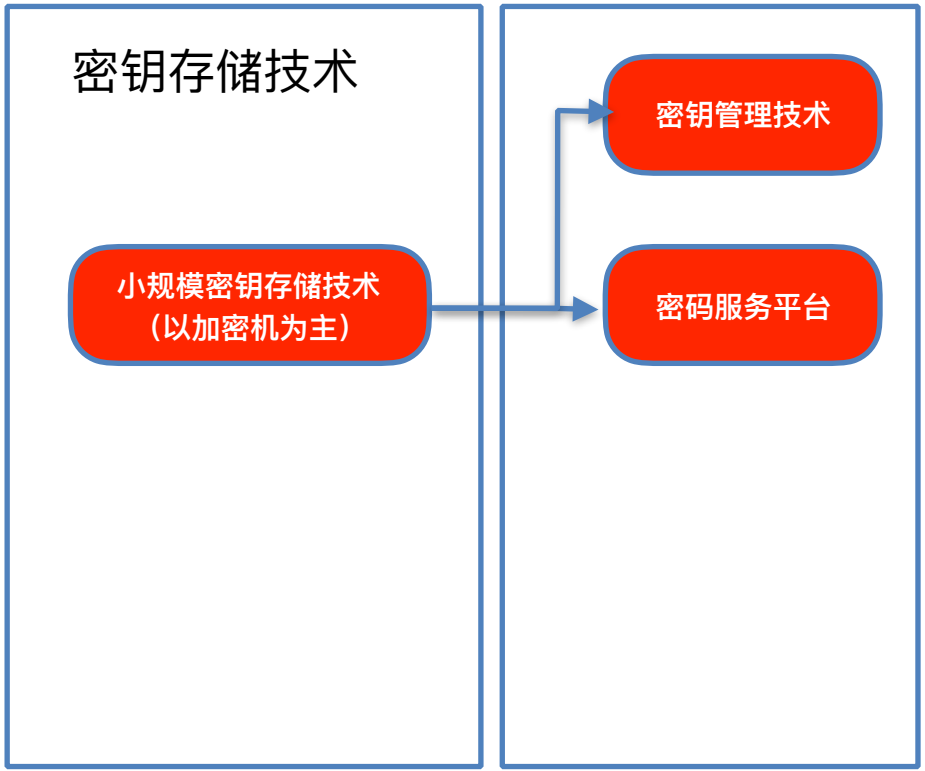
3）非对称密钥目前来看，主要应用在金融IC卡上，证书格式为特殊格式，即非x509标准的证书。

4）它的应用范围多集中在支付工具的发行使用上，支付认证工具泛指各行各业的ic卡应用、动态口令应用、usbkey应用。扩展来看，凡是拿在用户手中的具有独立安全芯片可以存储密钥的（与外形接口无关）工具，这类工具都可称为支付认证工具。

5）所谓小规模密钥存储技术对我们的销售并无太意义，实质上它就是加密机、加密卡、ic卡、usbkey的别称。在这里提出只是为了技术和概念纳入到一个体系中。

6）销售过程中只需要将其与加密机、加密卡、ic卡、usbkey挂勾就可。其中后台与加密机、加密卡挂勾，终端层面与ic卡、usbkey挂勾。

密码产品发展路线与应用销售的关系



基于小规模密钥存储技术的密钥管理技术

基于小规模密钥存储技术密钥管理是指以加密机、加密卡为基础，为业务系统提供密钥的产生、存储、备份、分发的管理功能。它的特点是：

1）由于对称密钥采用分散产生的方法，因此理论上管理的密钥数量是有限的。

2）密钥管理系统与业务应用过程中的密钥使用系统是分离的

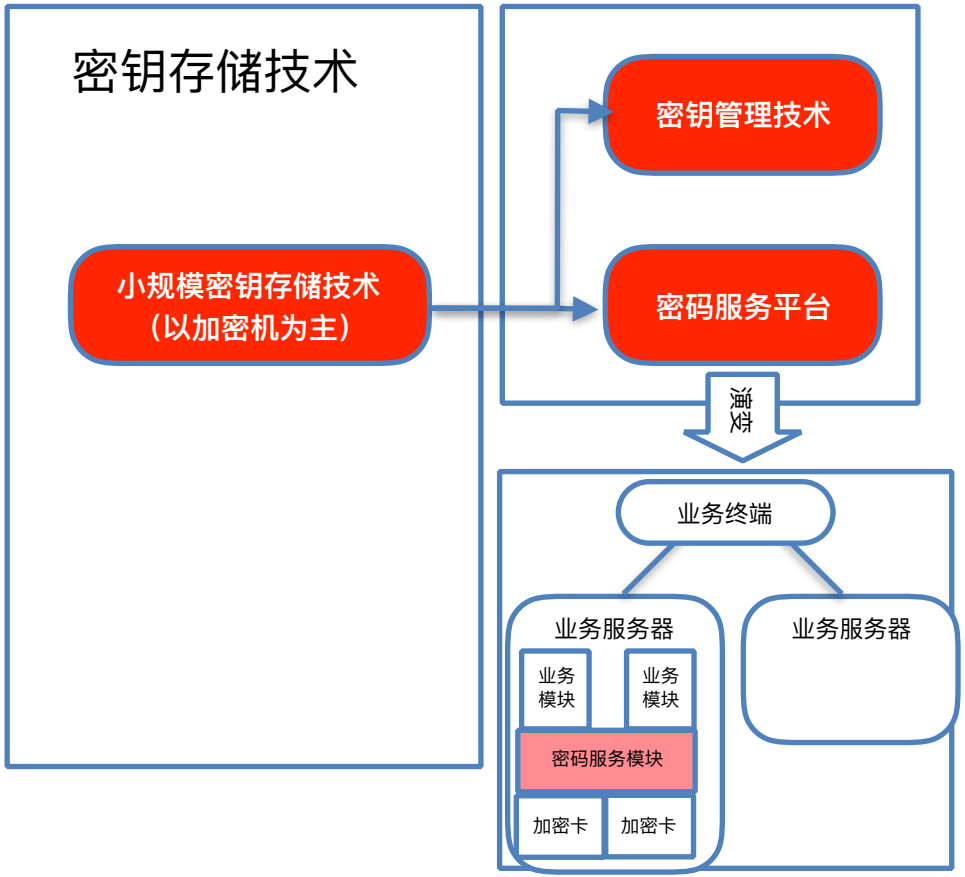
3）密钥管理系统负责产生和管理密钥，密钥使用系统负责密钥的使用。

4）它的应用范围多集中在支付工具的发行使用上也可以系统内部信息交流传输所需的密钥进行统一管理。

5）所谓小规模密钥密钥适用树状的管理体系中。

6）销售过程中它实质上集成了加密机的密钥存储技术和数据库的密钥存储技术。它的典型应用领域包括：金融IC卡（pboc2.0/3.0/emv/第三方预付费卡）、行业卡（社保、公交、市民卡、校园卡、智能小区卡、加油卡等）

密码产品发展路线与应用销售的关系



基于小规模密钥存储技术的密码服务技术

基于小规模密钥存储技术密码服务是指以加密机、加密卡为基础，为业务系统提供加密、解密、签名认证等密钥使用功能。它的特点是：

1）密码服务以使用密钥使用为核心。

2）它实质上也有密钥存储

3）它实质上也有密钥管理，不过是使用管理。

4）从整体考虑，它不负责密钥的产生，只负责使用。

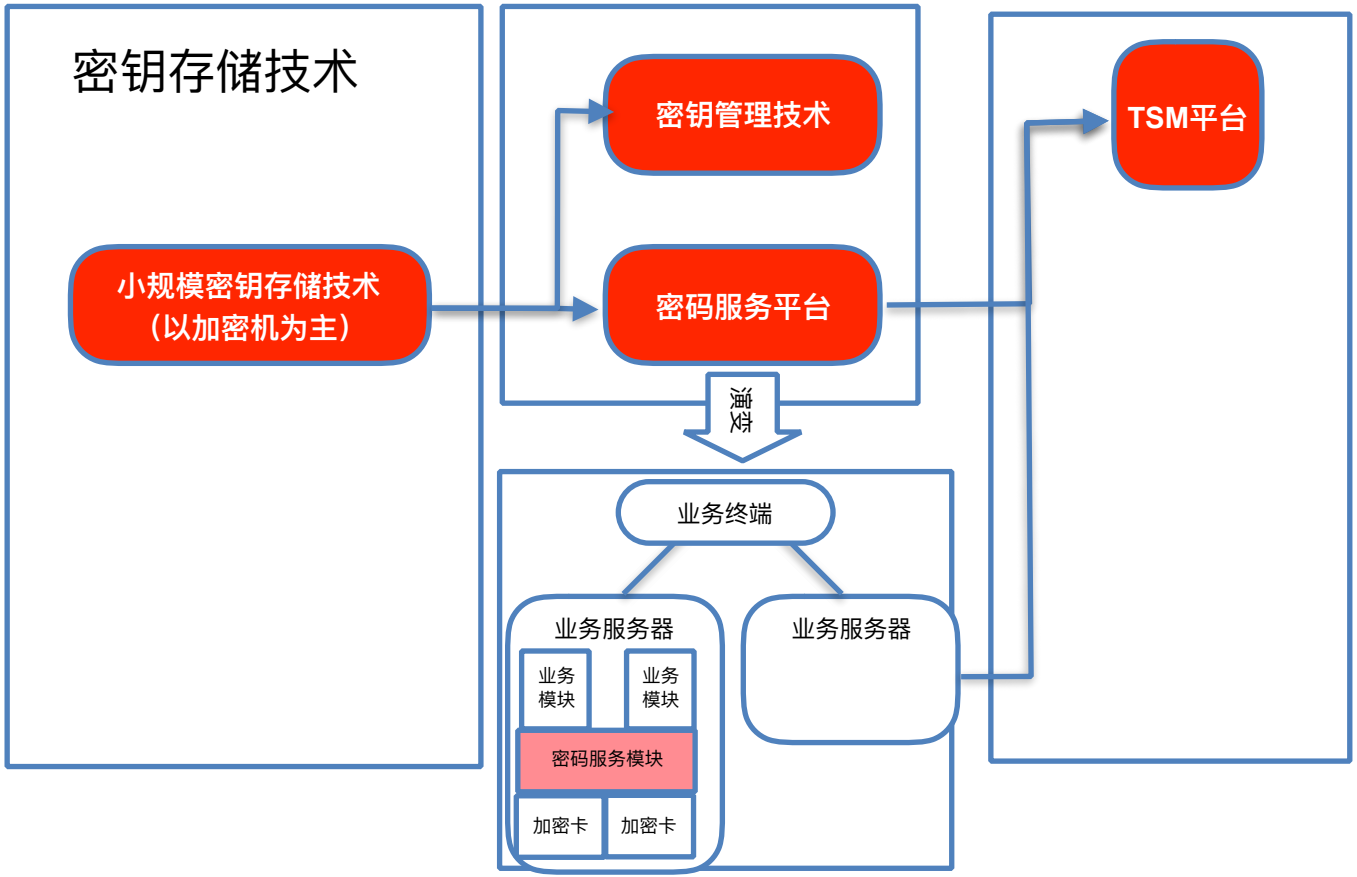
5）它与业务通过接口服务体现。

6）销售过程中、它可以不局限在IC卡领域，任何业务系统都可以。

7）密码服务平台演变—如果密钥存储采用加密卡形式。即一台服务器通过插加密机而不是连接加密机。则会演变为左下结构

8）演变后的密码服务模块对三味公司的服务器+密码卡的支持会提升到一个实用领域。

密码产品发展路线与应用销售的关系



TSM

TSM平台目前较为混乱，我们的理解是否得到业界一致还需要检验。我们的理解是发行完成为出发点，而不是刻意强调TSM。

1、组成或需要的技术：se应用及se管理技术、se的应用发行技术、se应用数据个人化技术

2、从使用场景上看，它可以应用于手机等移动发行、也可以应用于柜台等远程发行。

3、从销售领域来看，它可以用在银行、第三方的移动支付，也可以用在任何行业的远程柜台发卡

密码产品发展路线与应用销售的关系

小规模密码产品的路线就是以加密机、加密卡为切入、通过密钥管理和密码服务平台逐步向应用归集的路线

小规模密码产品，以加密机为切入点、从密钥管理和密码服务为基础，逐步向业务结合的方向发展。例如，我们现与IC卡行业结合.

小规模密码产品，以密钥管理和密码服务平台为基础，并不局限在以IC卡应用为代表的领域，还可以广泛应用在各行各业的需要数据加密的系统中。这可能难以具象化，比如现在通讯加密领域、数据库加密领域、如果和CA结合起来，可以构成音像制品、图书的版本保护和在线分发、传统的文档加密等等。

对于各位销售来说，对以下事项应密切关注，并引起足够重视：

1）以工控为代表，数据表现为指挥命令的安全
2）以交易为代表，数据表现为钱的支付安全
3）以审批为代表，数据表现为办公数据的安全
4）以档案为代表，数据表现为文件数据的安全
5）以音像图书为代表，数据表现为版权的安全

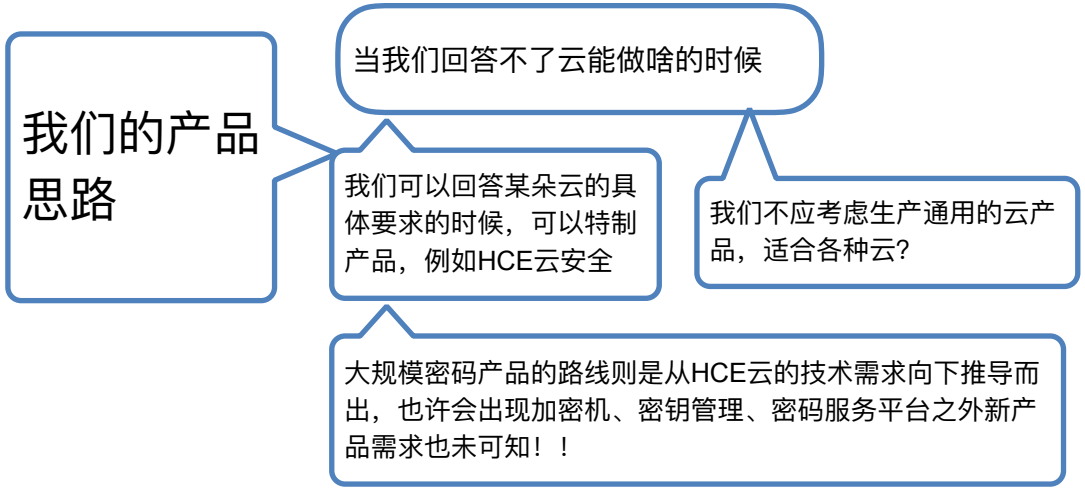
这些安全都与密码学密切相关，是我们与CA结合的产物，至少也可以将加密机引入。

密码产品发展路线与应用销售的关系

大规模密码产品的路线就不能走小规模产品从小到大（从加密机向应用结合）的路线

事实上加密机的诞生，也是因为金融安全的需要，从业务到产品、从上到下发展起来的。

站在加密机的角度去看、或思考：『云该要啥？』实质是削足适履。



密码产品发展路线与技术沉淀的关系

1、密钥存储技术—加密设备应用技术
2、密钥管理技术。
3、任务分配与并行处理技术
4、大用户量大交易量处理技术
5、多次往返类事件处理技术
6、多用户多应用并行处理技术