(ISC)2北京分会第8次沙龙活动

商业银行密码技术应用

北京中科博安 孙书强

(ISC)2北京分会微信公众号：ISC2BJ
info@ISC2chapter-beijing.org

关于(ISC)²北京分会

- (ISC)²是推出信息安全领域金牌认证CISSP的美国非盈利教育组织，在中国的(ISC)²北京分会成立于2014年11月1日，专注信息安全，旨在建立北京及周边地区的一个安全技术交流的网络，促进分会会员之间的信息分享、经验交流、技术讨论和个人职业发展

- (ISC)²北京分会微信公众号：ISC2BJ
- 入会申请表
  - http://yunpan.cn/cJgzLuAUcbjx2
  - （提取码：871e）
- 联系邮件
  - info@isc2chapter-beijing.org

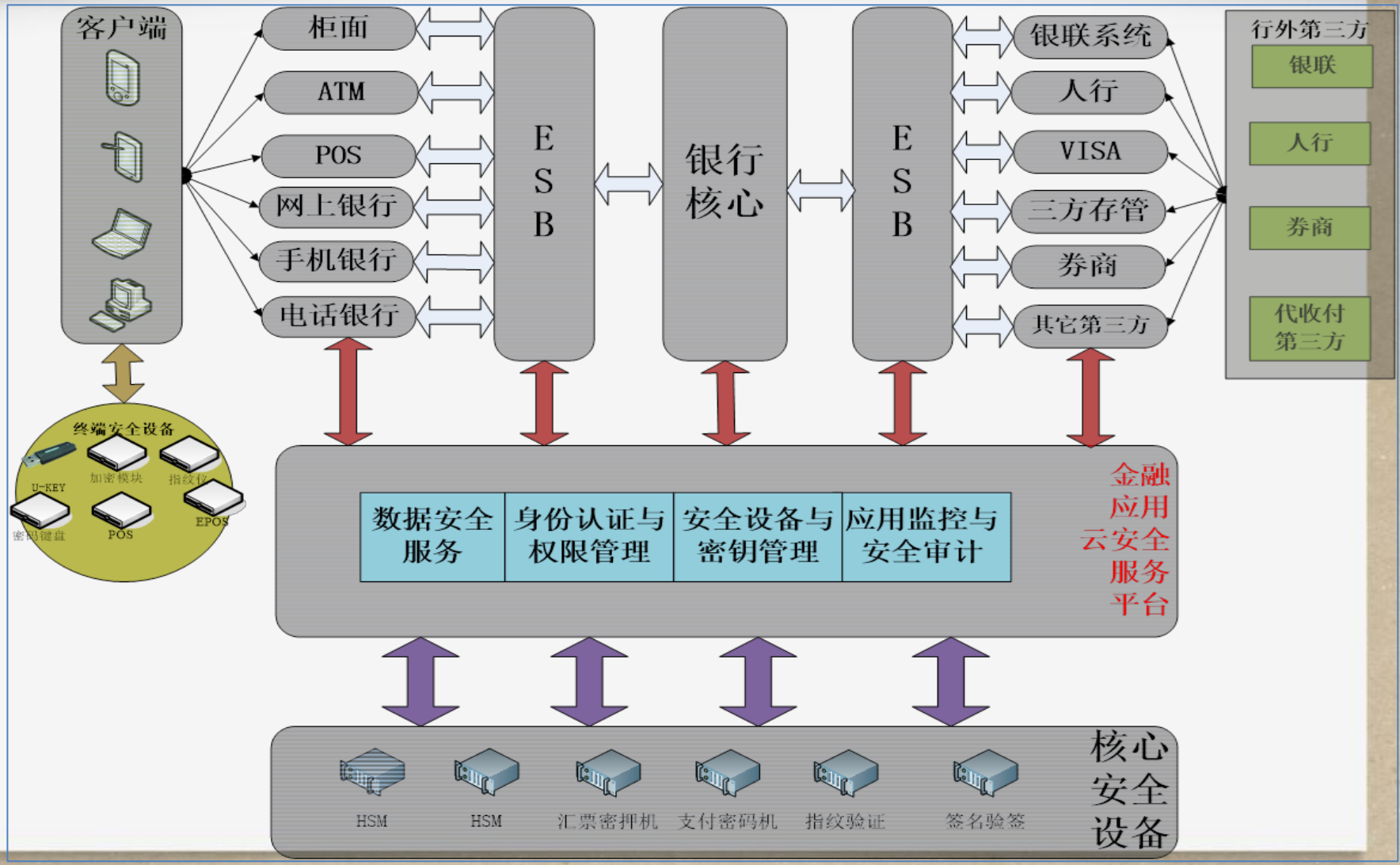
目录

- 概述
- 磁条卡
- IC卡
- 网银/手机银行
- 动态令牌（OTP）
- 手机指纹身份认证

概述

- 来源
  - 基于**银行的项目经验
- 范围
  - 数据安全，主要是PIN的保护和报文的安全（机密性、完整性）
  - 身份认证，动态令牌，手机指纹

概述-安全服务平台

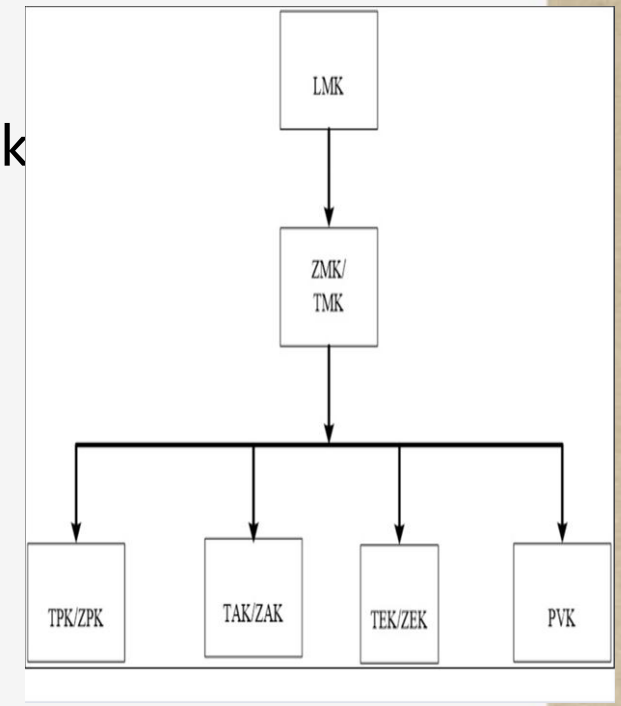

客户端
柜面
ATM
POS
网上银行
手机银行
电话银行
ESB
银行核心
ESB
银联系统
人行
VISA
三方存管
券商
其它第三方
行外第三方
银联
人行
券商
代收付第三方
终端安全设备
U-KEY
加密模块
指纹仪
密码键盘
POS
EPOS
数据安全服务
身份认证与权限管理
安全设备与密钥管理
应用监控与安全审计
金融应用云安全服务平台
HSM
HSM
汇票密押机
支付密码机
指纹验证
签名验签
核心安全设备

概述-密码（PIN）

- PIN的保护
  - 传输：pinblock，格式ansi9.8 format0
  - 存储：PVV
- PIN的生命周期：输入，传输，校验，存储

概述-加密机（HSM）

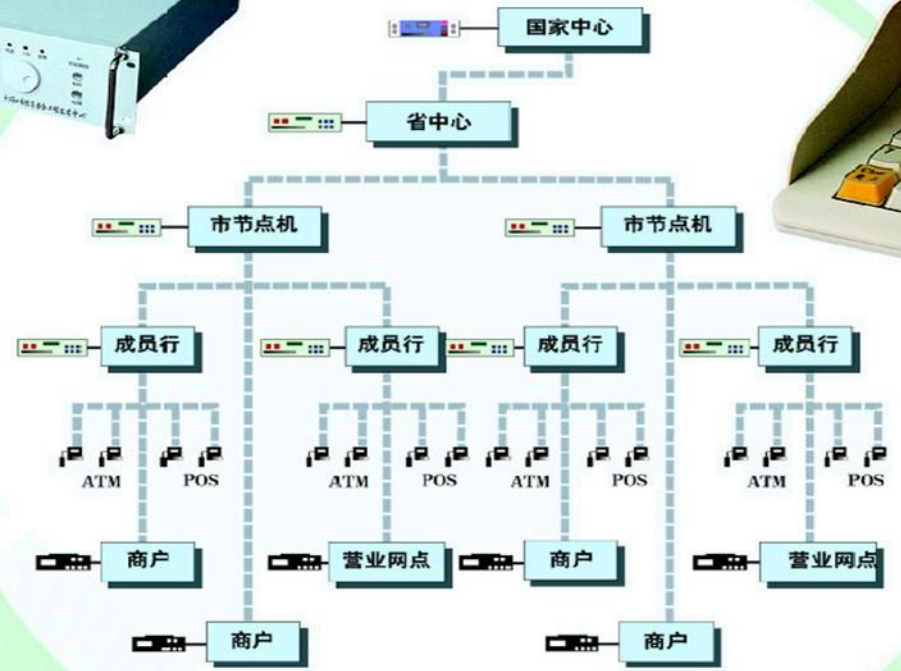
- 加密机
  - 硬件设备，功能，为什么用加密机，racal，国密算法
- 密钥
  - kek、wk
  - 专钥专用：tak、tpk、tek、zmk、pvk、cvk
  - 密钥的保护关系
- 指令集
  - Racal



SJL06E

密码键盘

SJL06T



终端密码模

SJL06S

磁条卡

- 标准：
  - GB/T 19584-2010 银行卡磁条信息格式和使用规范
- 磁道
  - 磁道1
  - 磁道2：主账号（PAN），CVV，有效期，服务码
  - 磁道3
- CVV、CVV2
  - CVV：计算要素（PAN，有效期YYMM，服务码）
  - CVV2

5.2 第 2 磁道的数据内容

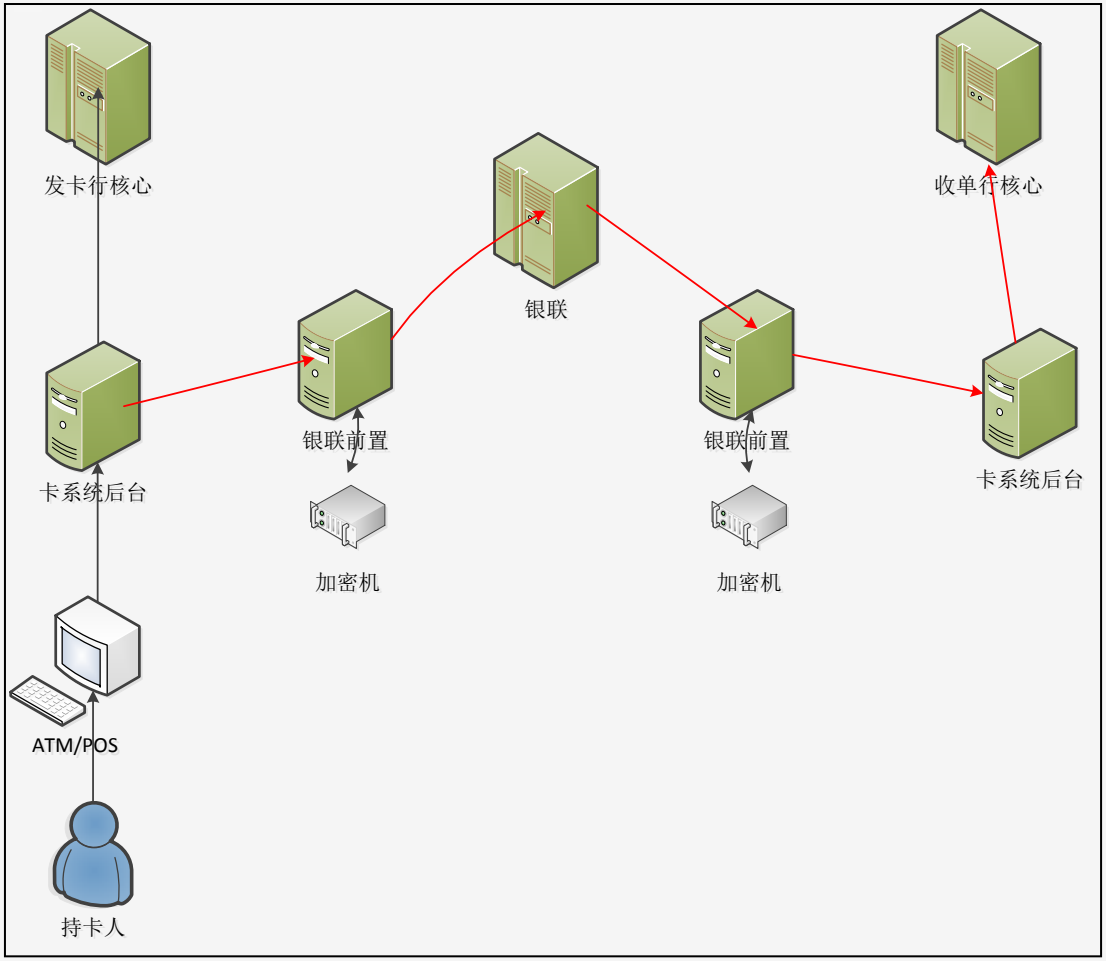
第 2 磁道数据编码最大记录长度为 40 个字符，数据字段的顺序和长度应与表 2 给数据格式一致。

第 2 磁道为只读磁道。

表 2 第 2 磁道数据格式

字段		D=动态 S=静态	字段长度	备注
序号	名称			
1	起始标志	S	1	“;”,见 6.1
2	主账号	S	13～19	见 6.3
3	字段分隔符	S	1	“=”,见 6.4
4	失效日期	S	4	YYMM,见 6.6
5	服务代码	S	3	见 6.7
6	附加数据	S	可变	见 6.8
7	结束标志	S	1	“?”,见 6.9
8	纵向冗余校验码	S	1	见 GB/T 15120.2

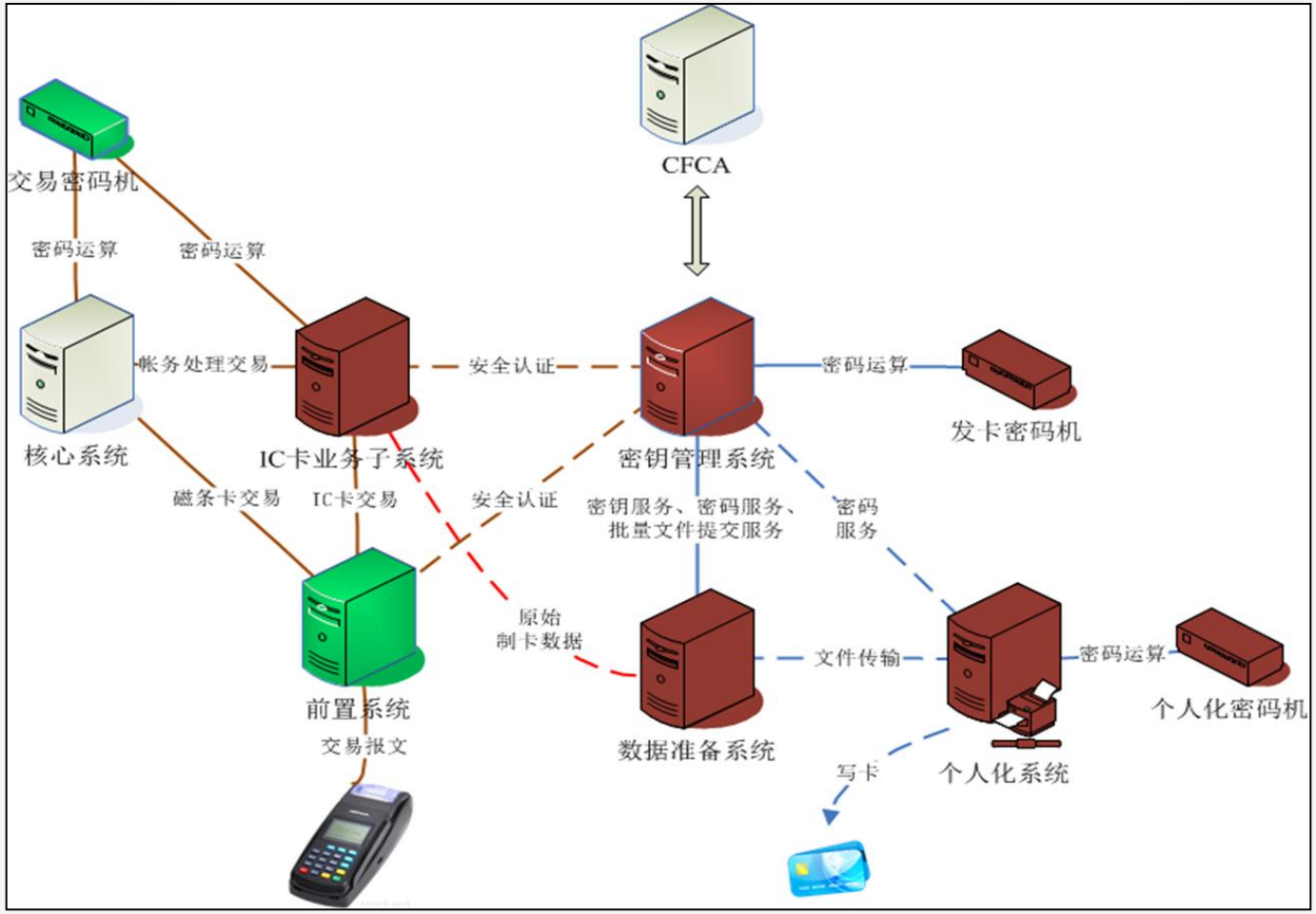
PIN加密、验证、转加密



IC卡-概述

- 需求
  - 卡片安全：防复制
  - 交易安全：ARQC/ARPC
- 标准
  - PBOC1.0：电子钱包、电子存折
  - PBOC2.0：借贷记、小额支付
  - PBOC3.0：行业应用、国密算法

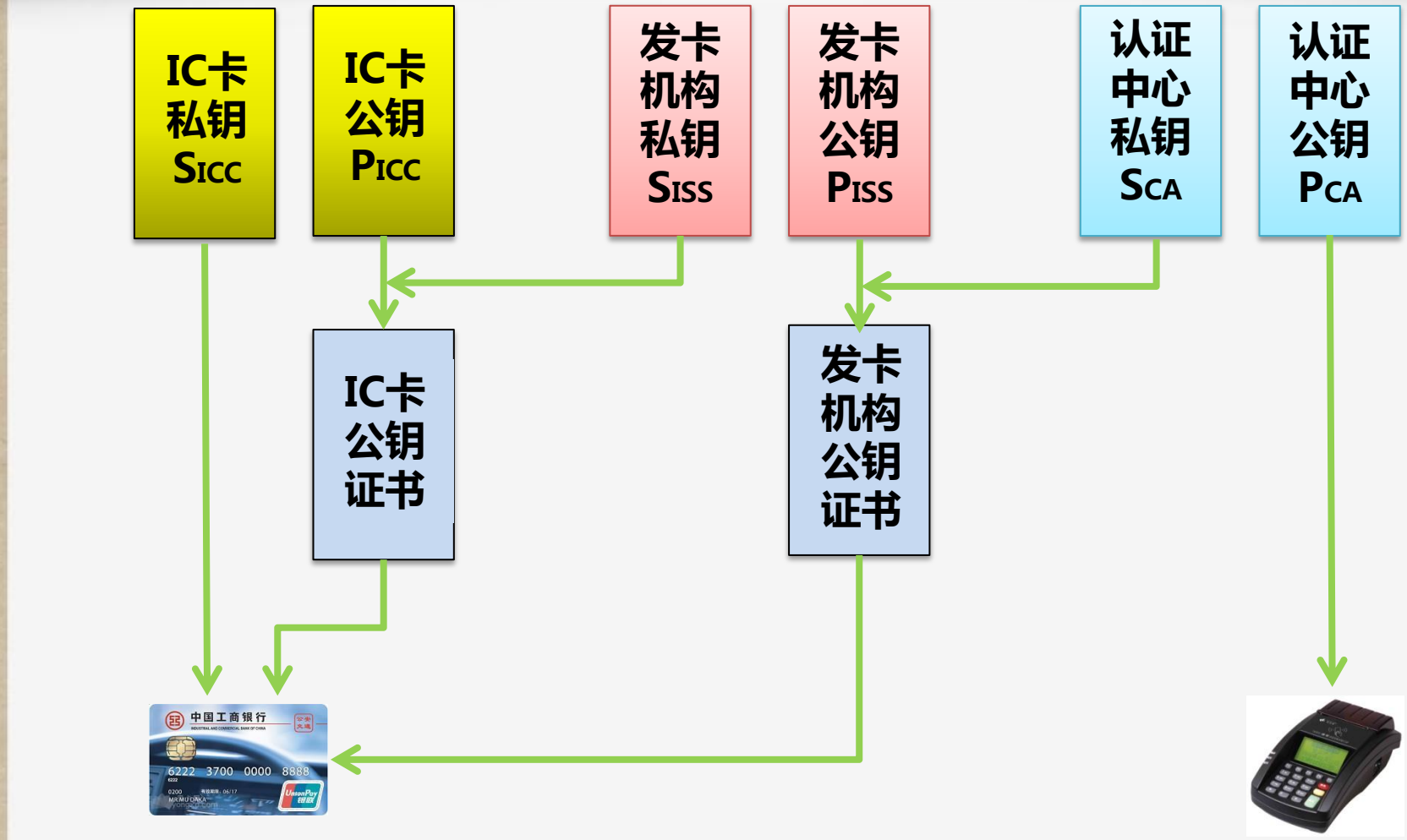
IC卡-概述


CFCA
交易密码机
密码运算
密码运算
帐务处理交易
安全认证
密码运算
发卡密码机
核心系统
IC卡业务子系统
密钥管理系统
磁条卡交易
IC卡交易
安全认证
密钥服务、密码服务、
批量文件提交服务
密码
服务
原始
制卡数据
文件传输
密码运算
个人化密码机
前置系统
交易报文
数据准备系统
个人化系统
写卡

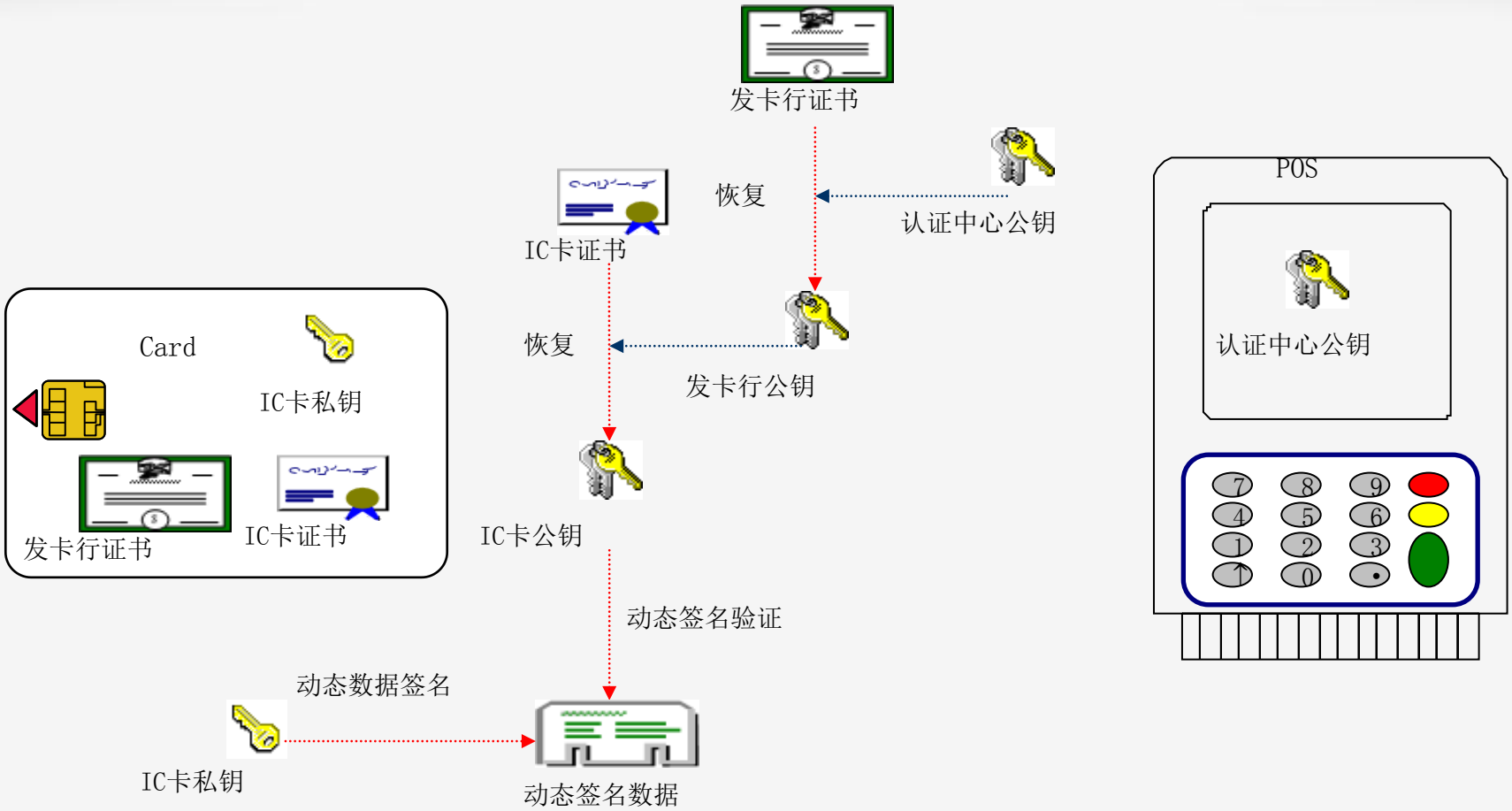
IC卡-密钥体系

- 非对称
  - CFCA根公钥
  - 发卡行公钥、私钥
  - IC卡片公钥、私钥
- 对称
  - MDK
  - UDK/SUDK
  - KMC：DES Master Key for Personalization Session Keys

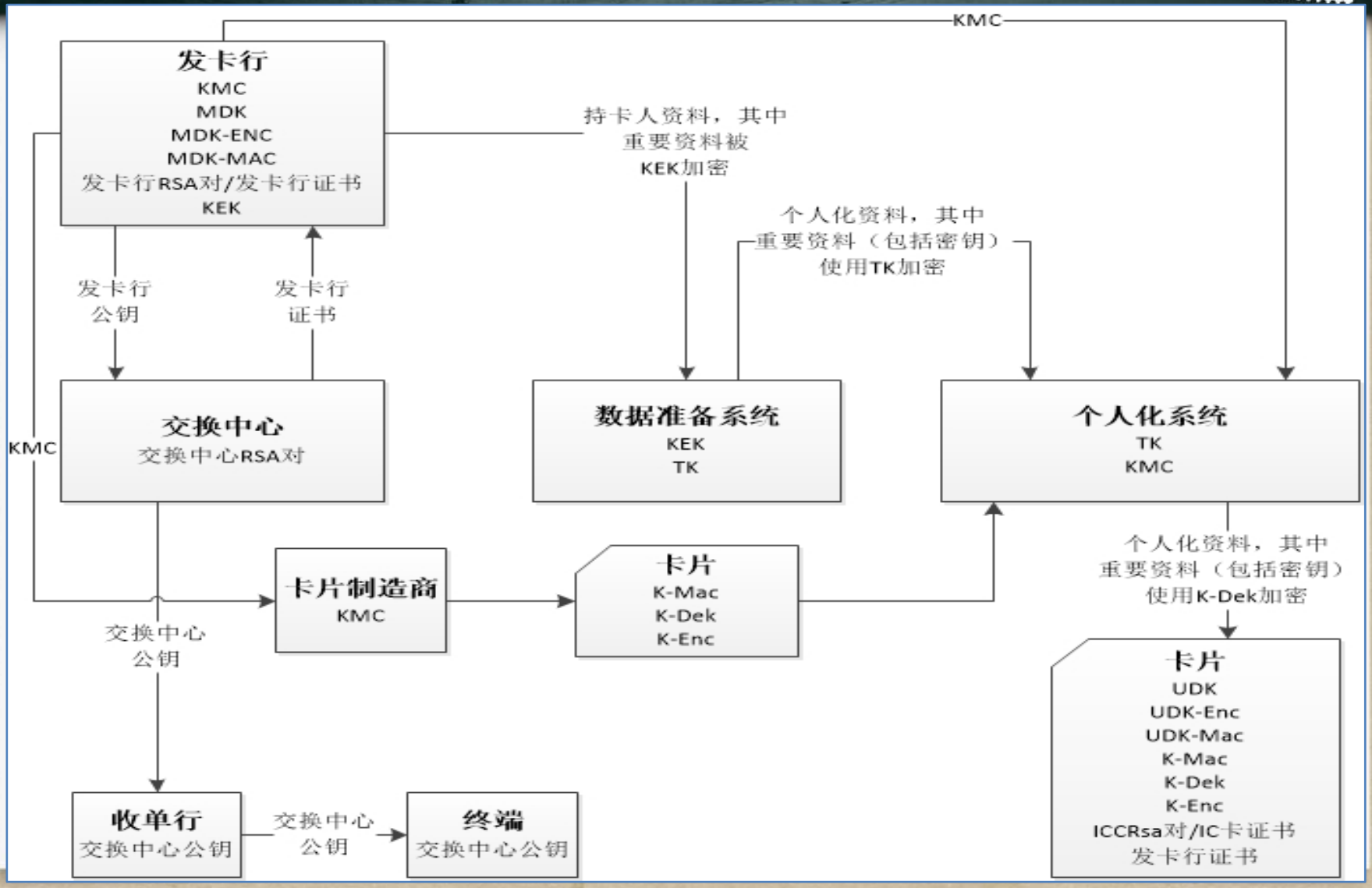
IC卡-证书体系


IC卡
私钥
SICC
IC卡
公钥
PICC
发卡
机构
私钥
SISS
发卡
机构
公钥
PISS
认证
中心
私钥
SCA
认证
中心
公钥
PCA
IC卡
公钥
证书
发卡
机构
公钥
证书
中国工商银行
6222 3700 0000 8888

IC卡-脱机数据认证SDA/DDA



IC卡-密钥体系


KMC
发卡行
KMC
MDK
MDK-ENC
MDK-MAC
发卡行RSA对/发卡行证书
KEK
持卡人资料，其中
重要资料被
KEK加密
个人化资料，其中
重要资料（包括密钥）
使用TK加密
发卡行
公钥
发卡行
证书
KMC
交换中心
交换中心RSA对
数据准备系统
KEK
TK
个人化系统
TK
KMC
个人化资料，其中
重要资料（包括密钥）
使用K-Dek加密
卡片制造商
KMC
卡片
K-Mac
K-Dek
K-Enc
交换中心
公钥
卡片
UDK
UDK-Enc
UDK-Mac
K-Mac
K-Dek
K-Enc
ICCRsa对/IC卡证书
发卡行证书
收单行
交换中心公钥
交换中心
公钥
终端
交换中心公钥

IC卡-密钥体系

	密钥名称	缩写	用途	产生流程
	发卡行 卡片主控密钥	KMC	用来派生KMAC、KENC、KDEK，KMC对每个发卡行是独有的。（DES Master Key for Personalization Session Keys）	发卡行初始化，与卡商共享
	IC卡 主控密钥	K-mac	用来保证在个人化过程中写入卡片数据的完整性（用来锁闭中国金融集成电路（IC）卡的应用区，并对个人化过程中装载到卡片的个人化数据进行检验，证实它们完整无损，且没有被修改；）	卡片芯片序列号+填充数据，通过kmc离散
		K-enc	用来生成IC卡密文和验证主机密文	
		K-dek	用来加密在个人化过程中写入卡片的私密数据	
	发卡行 应用主密钥	MDK		发卡行初始化（就每个BIN而言，MDK、MDK-ENC和MDK-MAC通常是唯一的）
		MDK-AC	用于联机的卡认证和发卡行认证；	
		MDK-ENC	用来加密发卡行的脚本机密信息；	
		MDK-MAC	用来校验发卡行的脚本信息；	
	IC卡 交易主密钥	UDK-AC	用于联机的卡认证（ARQC）和发卡行认证（ARPC）	卡号+卡序列号，通过MDK-AC离散
		UDK-ENC	用来加密发卡行的脚本机密信息（如脱机PIN等）	卡号+卡序列号，通过MDK-ENC离散
		UDK-MAC	用来校验发卡行的脚本信息	卡号+卡序列号，通过MDK-MAC离散
	每笔 交易密钥	SUDK-AC	生成与校验ARQC/ARPC	交易计数器，通过UDK-AC离散
		SUDK-ENC	加密应用数据明文/密文	交易计数器，通过UDK-ENC离散
		SUDK-MAC	校验完整性校验数据与MAC	交易计数器，通过UDK-MAC离散
	保护传输 密钥	KEK	密钥管理系统与数据准备系统约定的KEK	
		TK	数据准备系统与个人化系统约定的TK	
		K-dek	个人化卡片保护密钥K-dek	

网上银行/手机银行

- PIN保护
  - 对称算法：软件实现
  - 非对称算法：（pin长度+pin+随机数）公钥加密
  - 数字信封：对称算法的密钥、pin，公钥加密
  - Ukey：硬件实现
- 控件
  - 保护PIN、交易敏感信息

动态令牌

- 算法

  T = T0 / Tc

  ID = {T | C | Q }

  S = F(K , ID)

  OD = Truncate(S)

  P = OD % (10^N)

  T是参与运算的时间因子；

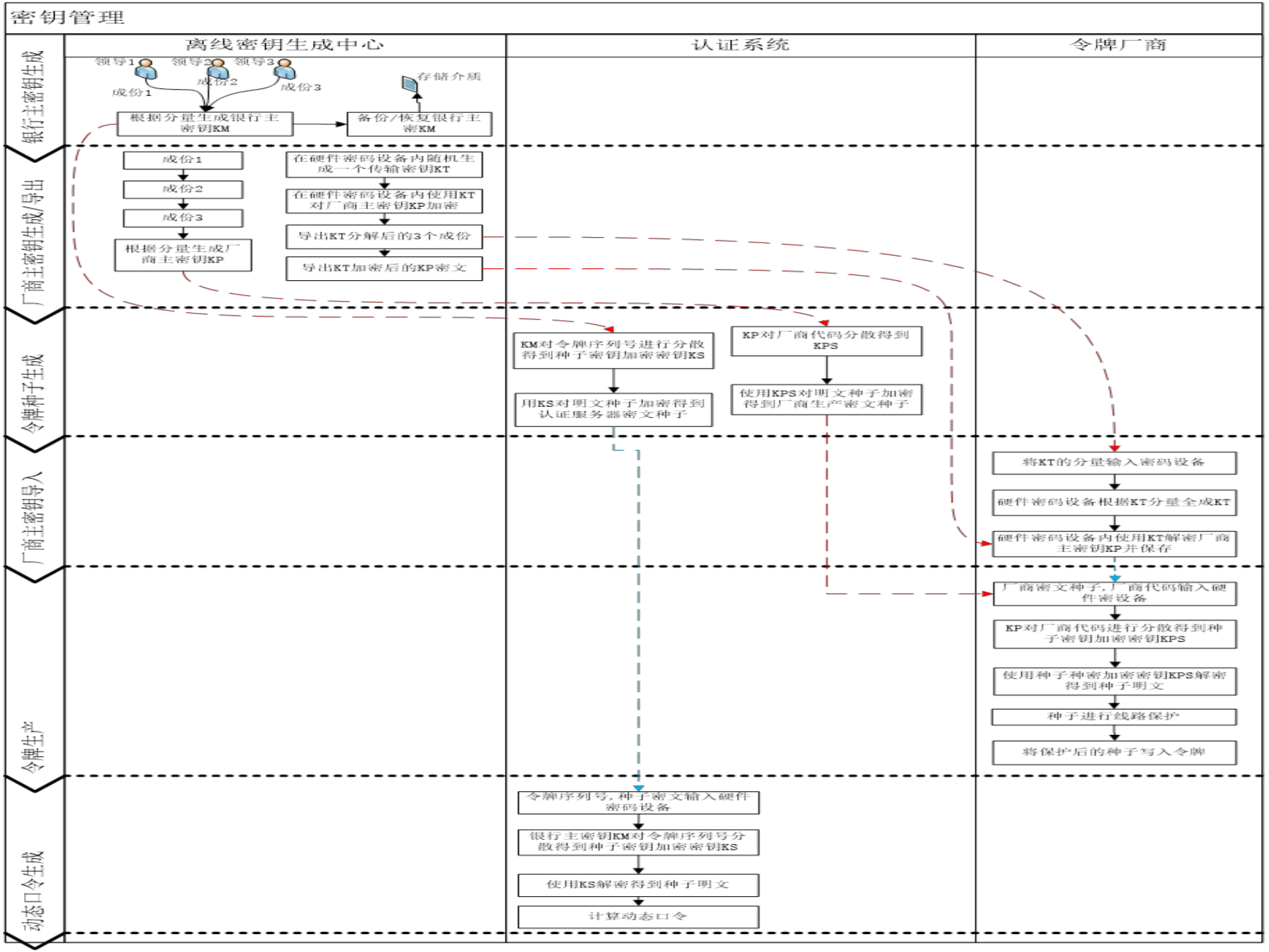
  ID是杂凑及分组算法的输入信息；

  C是参与运算的事件因子；

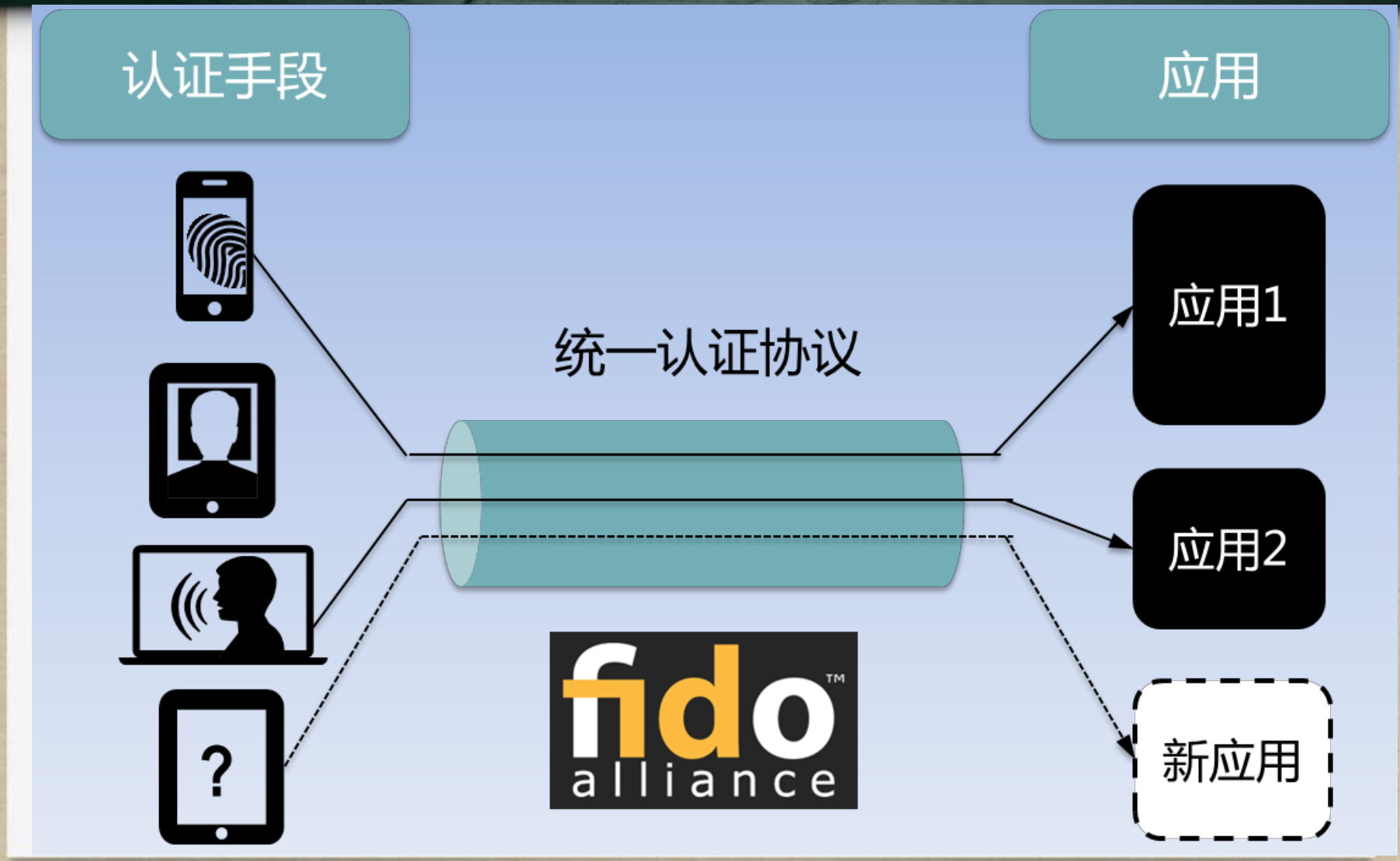
  Q是认证双方通过协商输入的挑战因子；

  F()是算法函数，即SM3；

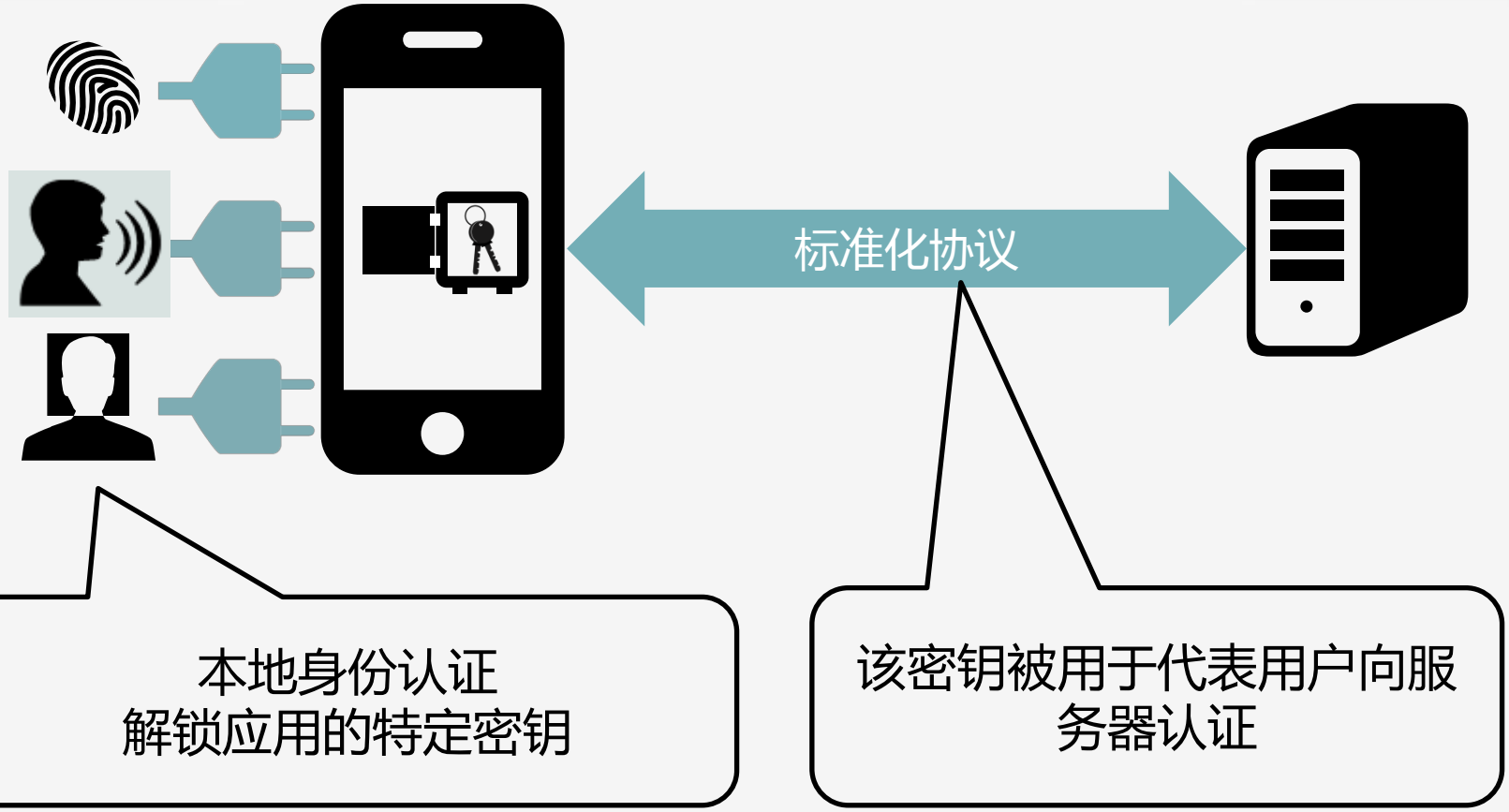
  N是令牌或其他终端显示口令的位数，N不小于6。


密钥管理
离线密钥生成中心
认证系统
令牌厂商
银行主密钥生成
厂商主密钥生成/导出
令牌种子生成
厂商主密钥导入
令牌生产
动态口令生成
领导1
领导2
领导3
成份1
成份2
成份3
存储介质
根据分量生成银行主密钥KM
备份/恢复银行主密KM
成份1
成份2
成份3
根据分量生成厂商主密钥KP
在硬件密码设备内随机生成一个传输密钥KT
在硬件密码设备内使用KT对厂商主密钥KP加密
导出KT分解后的3个成份
导出KT加密后的KP密文
KM对令牌序列号进行分散得到种子密钥加密密钥KS
用KS对明文种子加密得到认证服务器密文种子
KP对厂商代码分散得到KPS
使用KPS对明文种子加密得到厂商生产密文种子
将KT的分量输入密码设备
硬件密码设备根据KT分量全成KT
硬件密码设备内使用KT解密厂商主密钥KP并保存
厂商密文种子，厂商代码输入硬件密设备
KP对厂商代码进行分散得到种子密钥加密密钥KPS
使用种子种密加密密钥KPS解密得到种子明文
种子进行线路保护
将保护后的种子写入令牌
令牌序列号，种子密文输入硬件密码设备
银行主密钥KM对令牌序列号分散得到种子密钥加密密钥KS
使用KS解密得到种子明文
计算动态口令

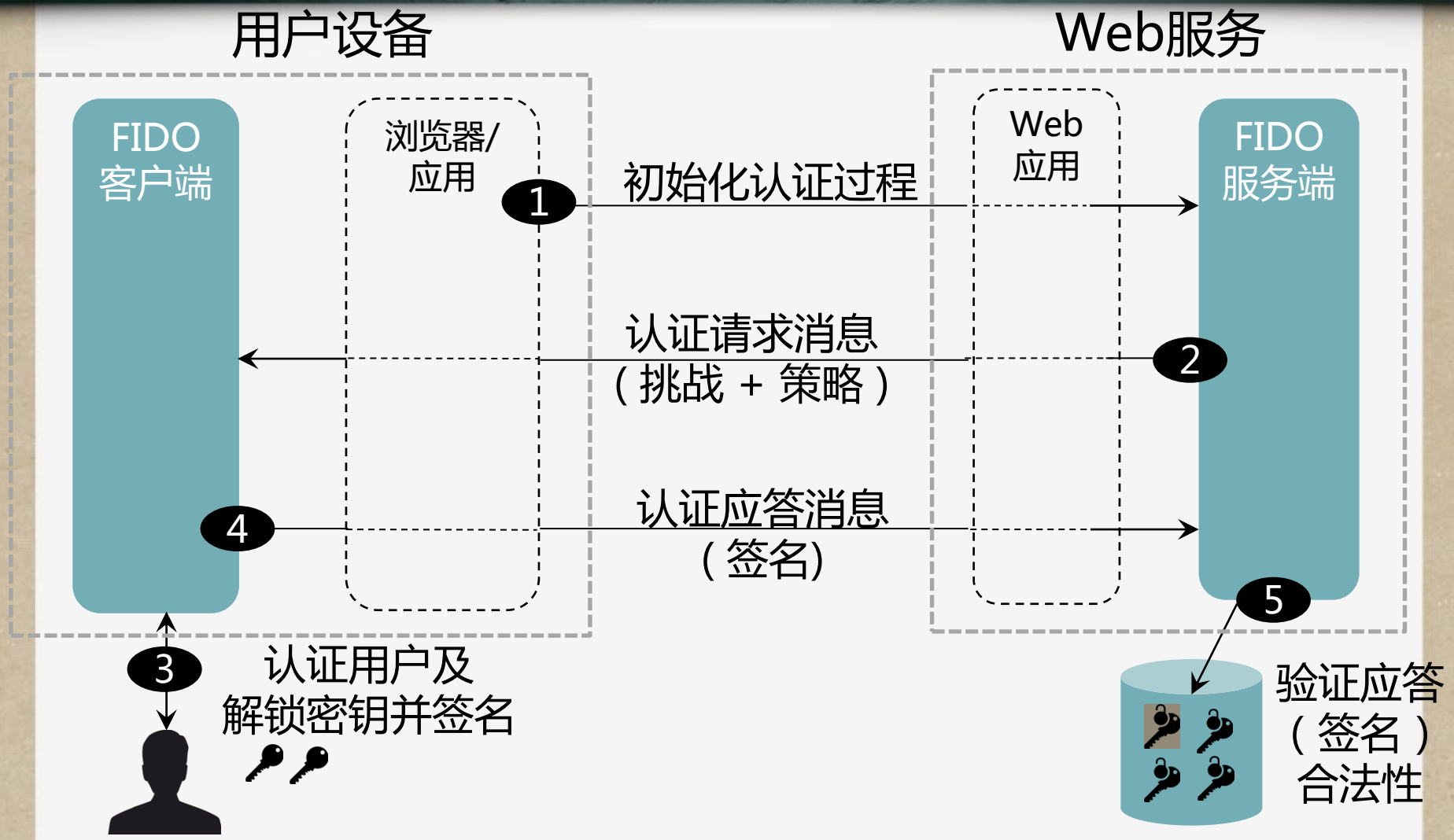
手机指纹身份认证



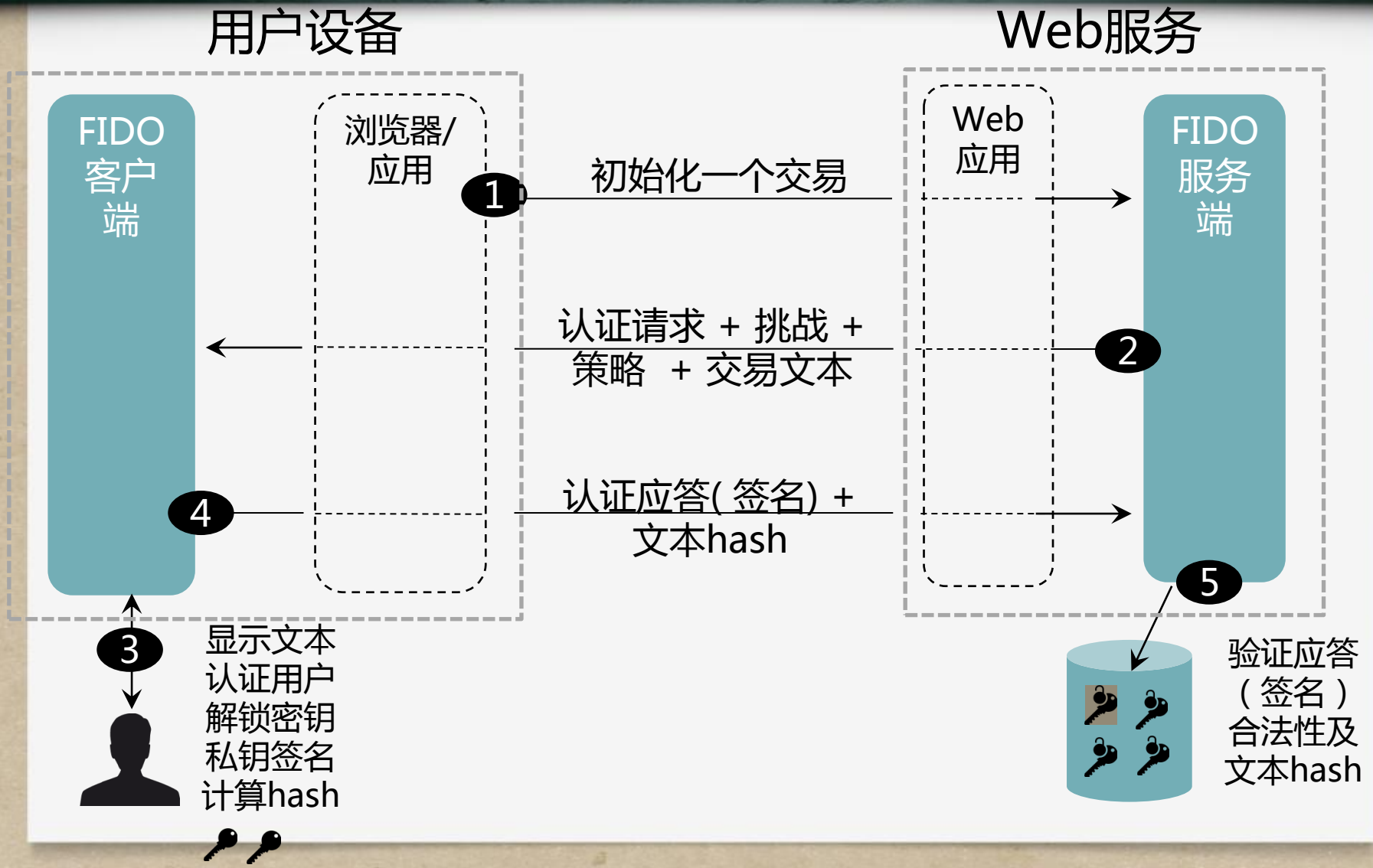
手机指纹身份认证-基于FIDO UAF



手机指纹身份认证-认证流程



手机指纹身份认证-交易确认流程



谢谢！