生物特征识别身份认证技术研究与标准化

2020年11月21日

Alibaba Group 阿里巴巴集团

前言

人们对其通过**脑力劳动**创造出来的**智力成果**所享有的**权利**。
具有排他性、地域性和时间性。

借助**已有**的理论、知识、经验对科学问题的假设、分析、探讨和推出结论,其结果应该是力求**符合事物客观规律**的,是对**未知科学问题**的**某种程度的揭示**。

为在**一定范围**内获得最佳秩序，对活动或其结果规定**共同的和重复使用**的规则、导则或特性的文件。该文件经**协商一致**制定并经一个**公认机构**的批准。

数字经济

学术研究

知识产权

技术标准

测试评估

数字经济成为全球经济增长的新引擎，中国数字经济规模位居世界第二位

面向行业，服务产业。

目录

THE CATALOGUE

1 产业现状

产业现状 – 产业需求

互联网和产业融合，一方面对产业发展起了巨大推动作用，另一方面也对身份核实提出严格的要求。生物特征识别具备良好用户体验、高安全性和广泛覆盖性，已成为身份管理的标配。

产业现状 – 体验驱动

生物识别技术已成为移动智能终端的标配，生物识别技术成为终端身份认证发展方向！

新型身份认证需求

- 用户体验
  - 符合人的自然习惯
  - 便捷
- 安全性
  - 准确判断真实的操作者
- 覆盖度
  - 普适性


指纹识别

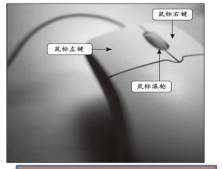

人脸识别


虹膜识别

声纹识别

生物特征


键盘按键行为


鼠标移动轨迹

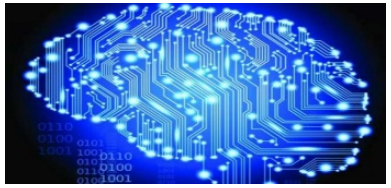

书写笔迹


指压行为

行为特征

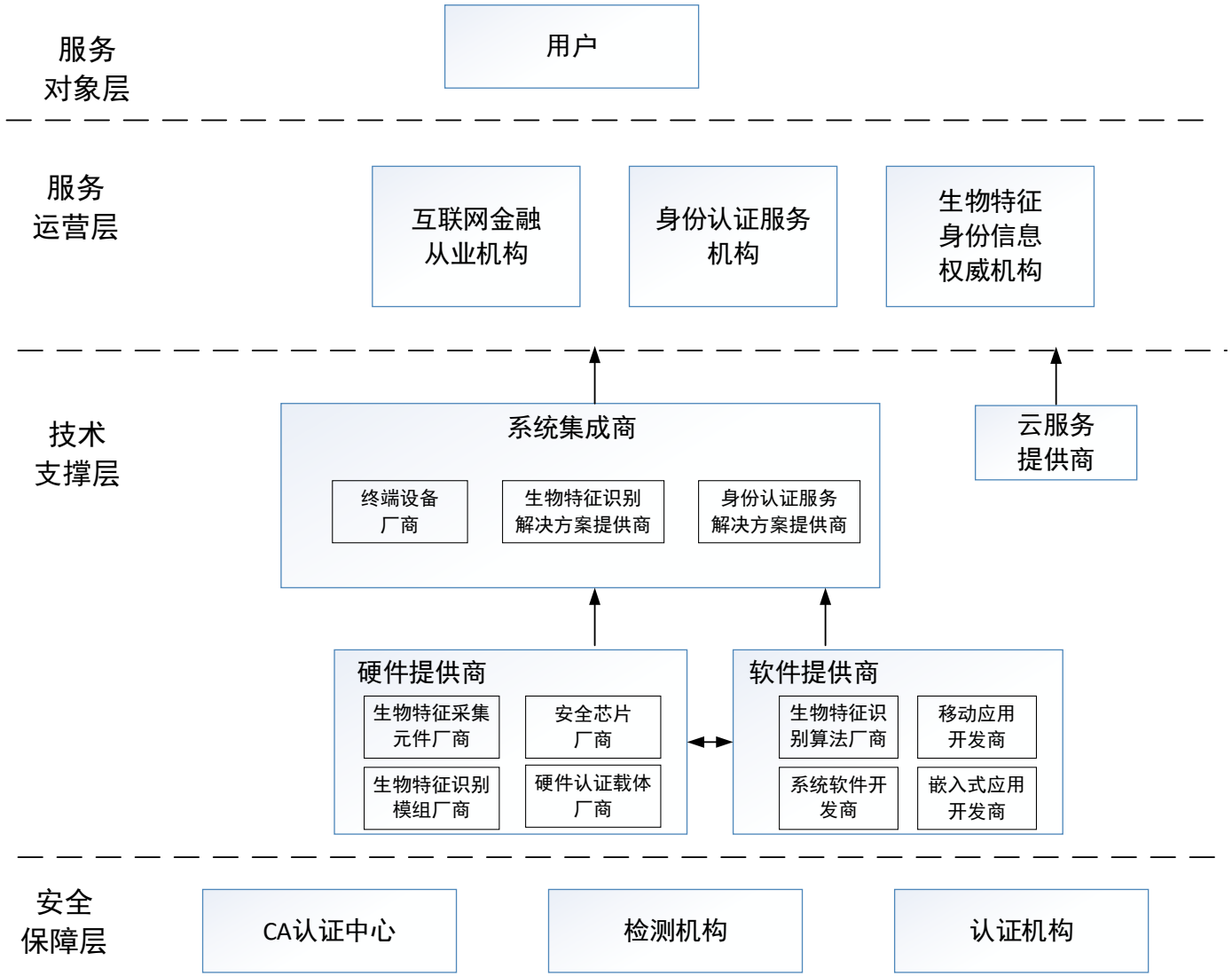

联合生态创新
身份认证手段

+


数据驱动挖掘
现有产品能力

核身体系

产业现状 – 产业链构成


服务对象层
用户
服务运营层
互联网金融从业机构
身份认证服务机构
生物特征身份信息权威机构
技术支撑层
系统集成商
终端设备厂商
生物特征识别解决方案提供商
身份认证服务解决方案提供商
云服务提供商
硬件提供商
生物特征采集元件厂商
安全芯片厂商
生物特征识别模组厂商
硬件认证载体厂商
软件提供商
生物特征识别算法厂商
移动应用开发商
系统软件开发商
嵌入式应用开发商
安全保障层
CA认证中心
检测机构
认证机构

2 应用场景

应用场景 – 总体应用

金融：用于银行、保险、互金等场景认证使用者身份，防止身份冒用

教育：用于在线考试报名、认证考生身份，防止替考

社保：用于电子社保卡、养老金提取，身份认证

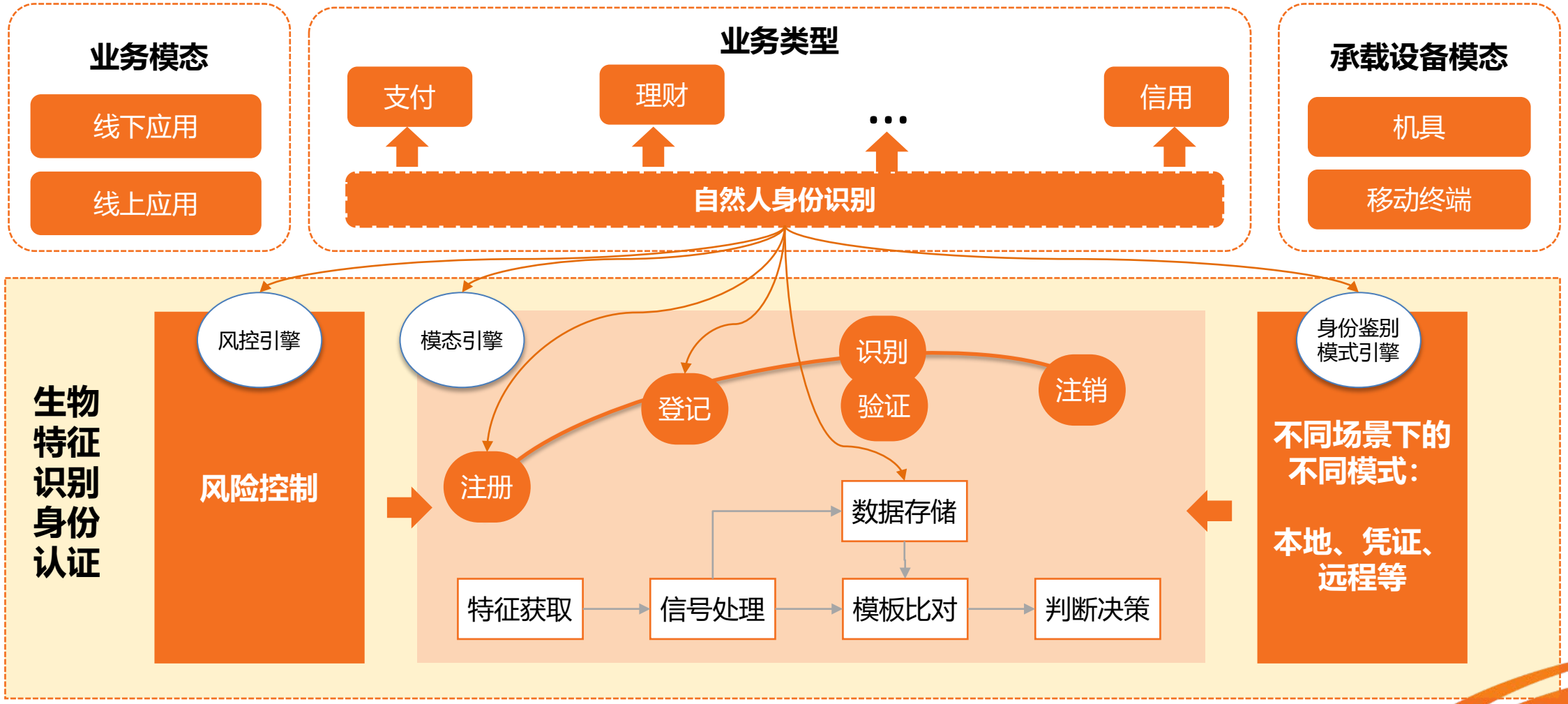
房产：用于房屋租赁、售卖场景，认证身份，保证交易安全

办公：用于移动考勤，认证人员身份，防止替打卡

娱乐：用于直播，认证主播身份，防止身份冒用

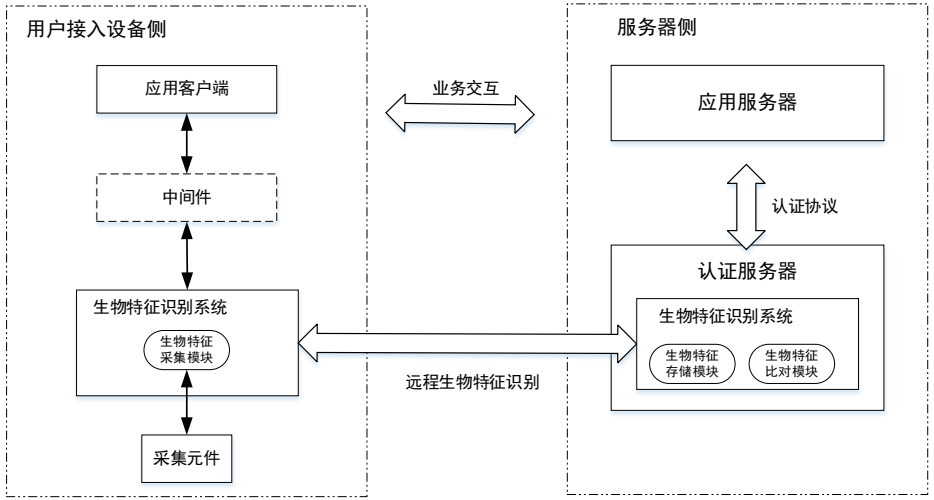
应用领域	细分场景	案例	类型	数据采集	识别方式	目前主要技术
公安	公共安全	电信、网吧、酒店、交通	嵌入式	公安部	1:1	人脸
	刑侦	罪犯追踪	人员筛查、找到疑似	公安部	多种方式1:N	人脸、虹膜、指纹、DNA
金融	线下取款（自助机具）	ATM、助农POS	嵌入式	个人采集	1:1	人脸、指静脉（？）
	线下支付（自助机具）	助农POS、自助贩卖机、自助售药机、自助收银机、就医支付	嵌入式	个人采集	1:1	人脸、指静脉
	线下支付（交通）	地铁、公交	嵌入式	个人采集	城市范围1:N	掌静脉（？）
	线上支付	电子商务、网上交易		个人采集	1:1	声纹、人脸（？）
政府	政府服务	政务服务线上、自助终端、基层网点、第三方网点延伸	嵌入式	服务范围人员采集	1:1	线上：人脸；线下：指静脉
	资格认证	养老保险、民政、财政补助		人社部	1:1	人脸、指静脉、声纹，隐形认证
	实名认证	养老、就医购药、就业培训、财政补助		认证范围人员采集	1:1	人脸
安防	门禁	园区、校园、企业、办公楼、公寓楼、监狱	独立设备	安防范围人员采集	安防范围内1:N	人脸/多模态
	闸机	园区、校园、企业、办公楼	嵌入式	安防范围人员采集	安防范围内1:N	人脸/多模态
	储物柜	快递柜、枪弹柜	嵌入式	安防范围人员采集	安防范围内1:N	人脸
智能家居	锁（传统锁替代）	门锁、车锁、柜锁	嵌入式，小型化；	个人采集	小范围1:N，约等于1:1	指纹、指静脉
身份鉴别	电脑登录（密码替代）	笔记本电脑、PAD和手机移动设备授权	嵌入式，小型化；	个人采集	1:1	人脸、指纹
	网络登录和授权（密码/Ukey替代或增强）	企业系统登录、互联网应用登录	PKI/SSO结合	系统范围采集	1:1	指纹

应用场景 – 金融应用

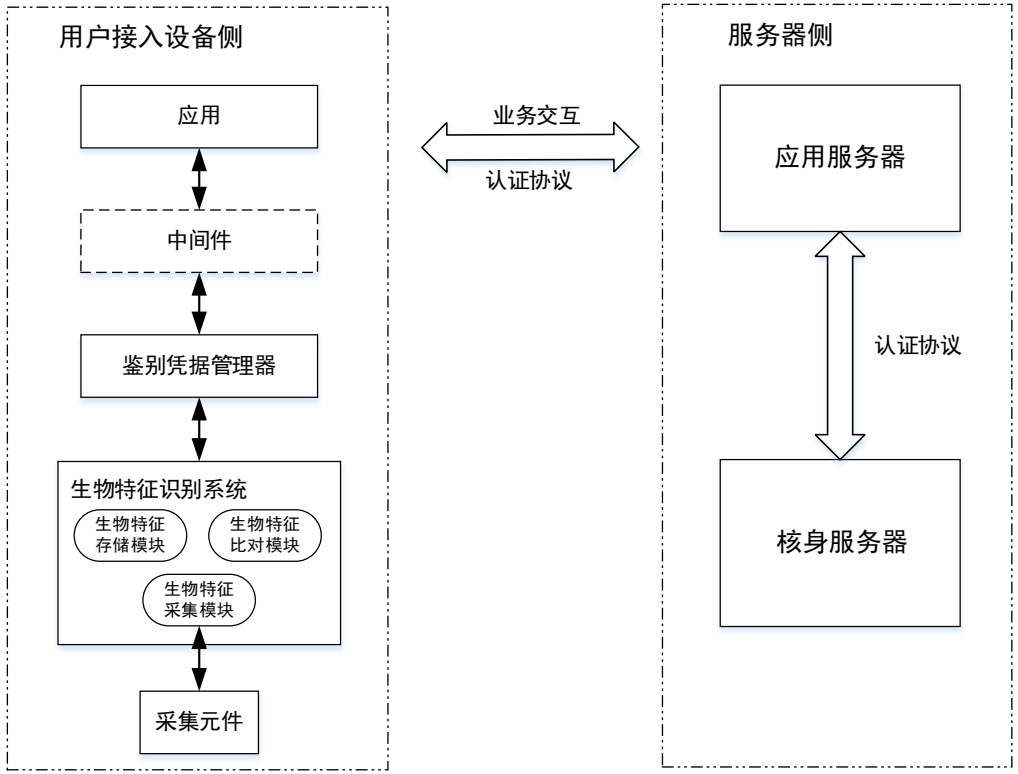

业务模态
线下应用
线上应用
业务类型
支付
理财
...
信用
自然人身份识别
承载设备模态
机具
移动终端
生物特征识别身份认证
风险控制
风控引擎
模态引擎
注册
登记
识别
验证
注销
数据存储
特征获取
信号处理
模板比对
判断决策
身份鉴别模式引擎
不同场景下的不同模式：
本地、凭证、远程等

应用场景 - 认证模式

本地模式采用了生物特征+鉴别密钥联合认证的方式，且通过PKI/CA机制保证了远程传输的安全性；远程模式则支持与权威库的对接，可以直接进行实人认证。

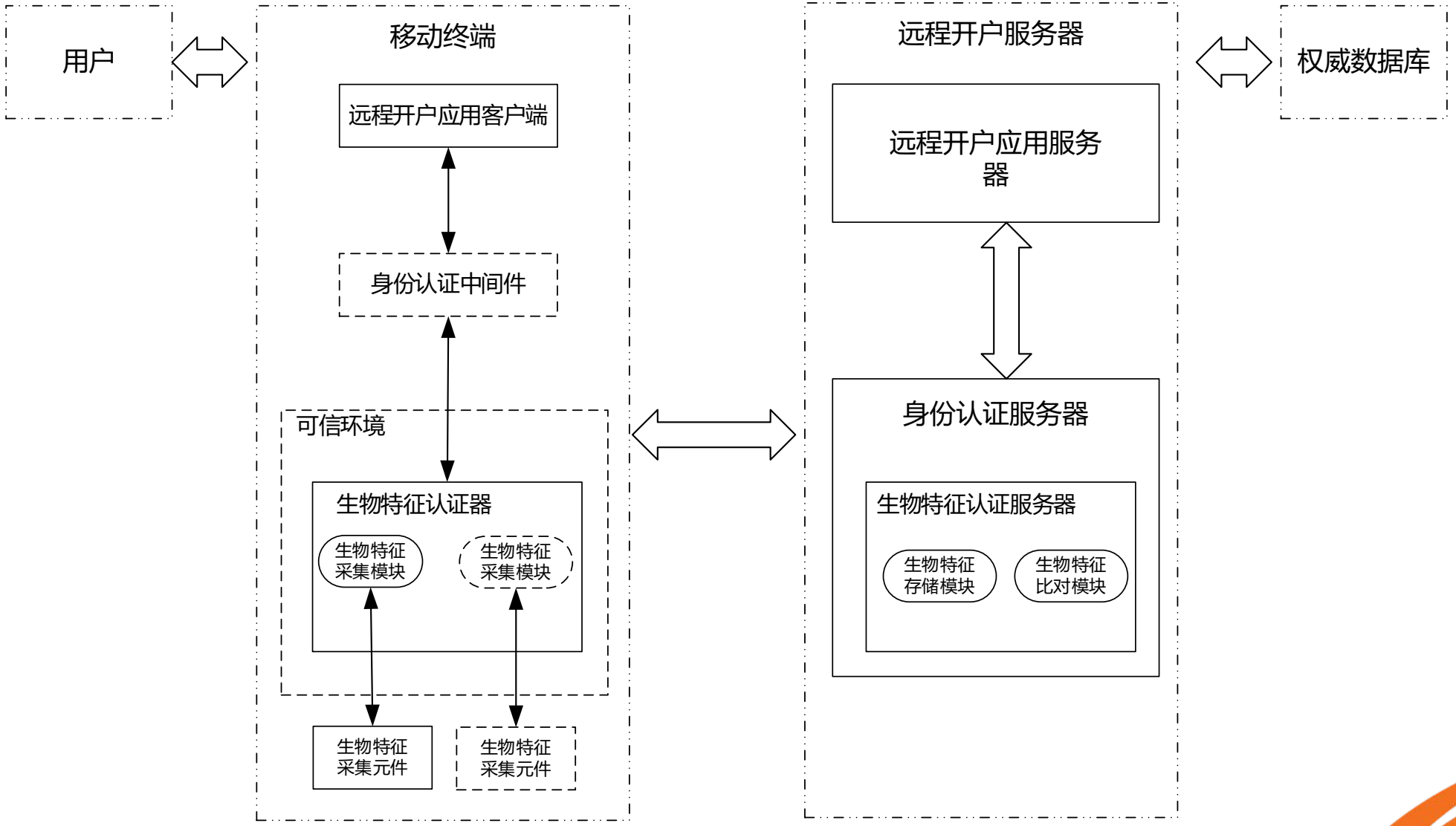


远程模式

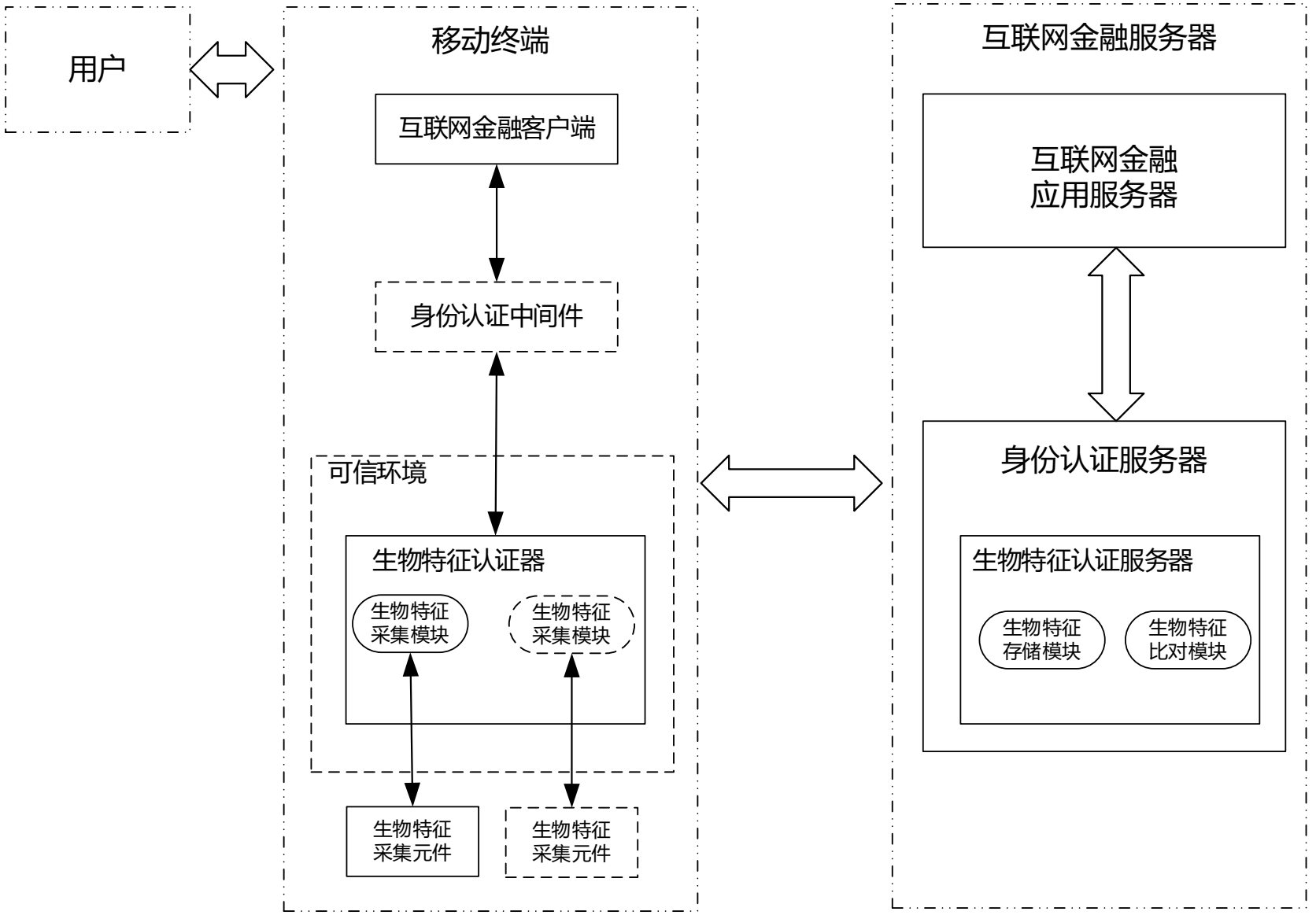


本地模式

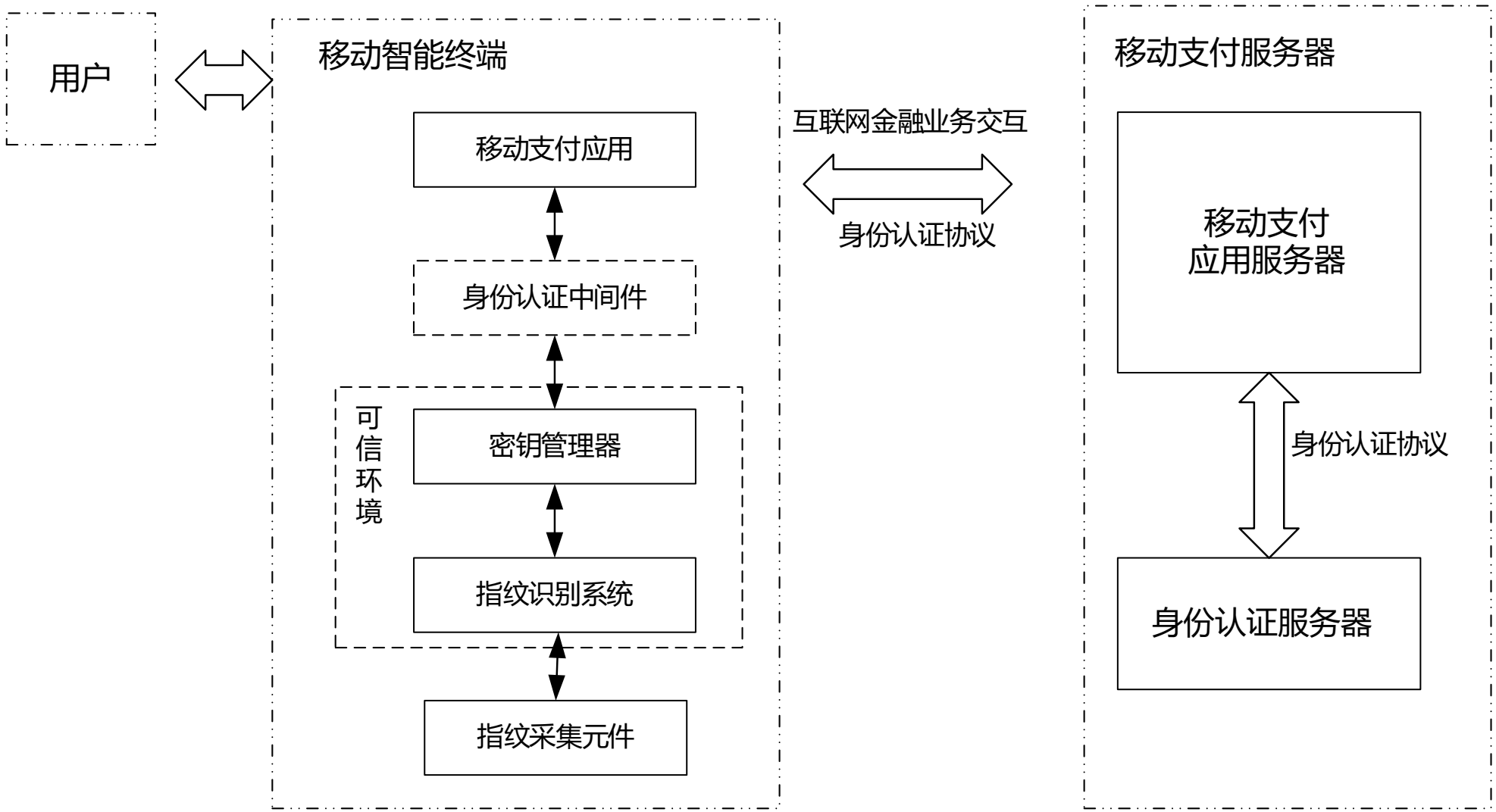
应用场景 – 远程开户


用户
移动终端
远程开户应用客户端
身份认证中间件
可信环境
生物特征认证器
生物特征采集模块
生物特征采集模块
生物特征采集元件
生物特征采集元件
远程开户服务器
远程开户应用服务器
身份认证服务器
生物特征认证服务器
生物特征存储模块
生物特征比对模块
权威数据库

应用场景 – 账户管理



应用场景 – 指纹支付



3 技术研究

技术研究 – 术语区分

身份证明：proofing

提供“证件”证明实体身份的过程，是个“举证的过程”
关键技术：身份标识技术、安全协议等关键点

身份核验：verification

身份的核查验证过程，是“身份查验的过程”，
关键技术：生物特征识别，安全协议，身份标识的查询验证，数据库的快速查询等；

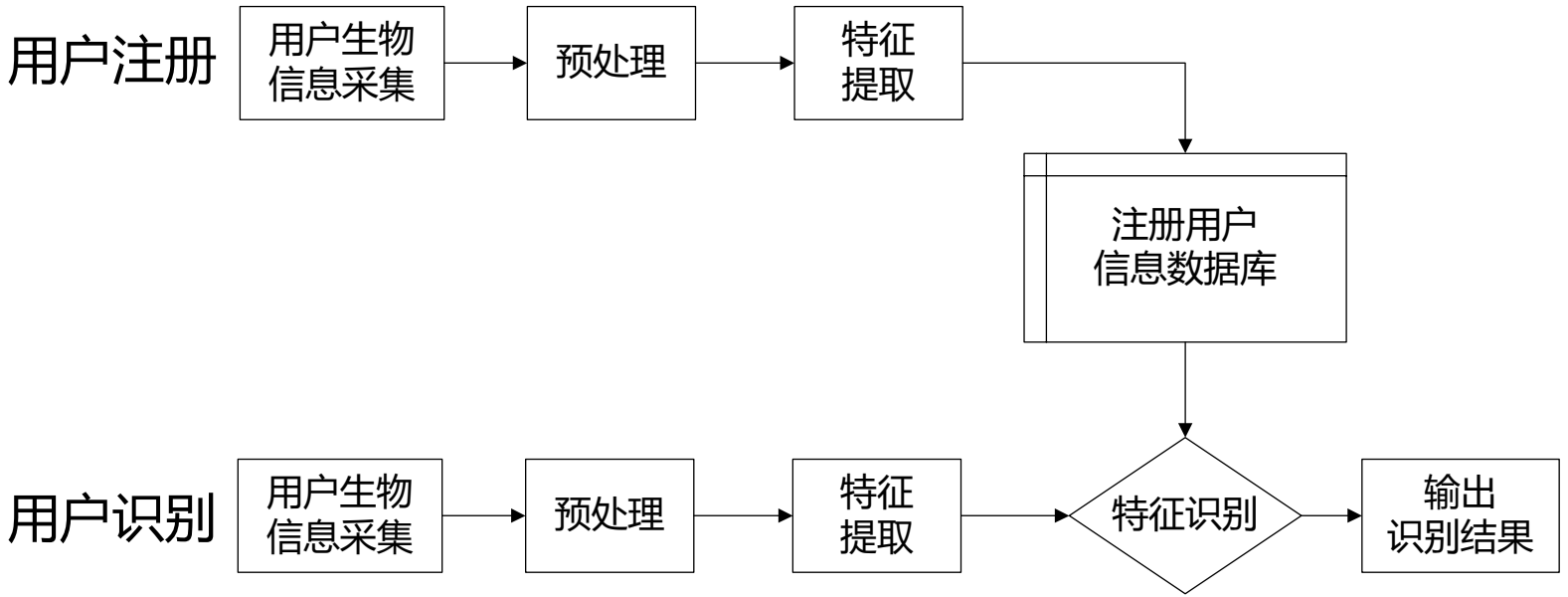
身份鉴别：authentication

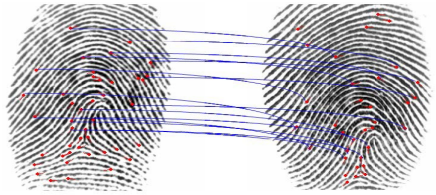
用户提交相关凭证、标识、口令、生物特征等内容，系统判断用户身份及权限的过程。
关键技术：安全协议、身份鉴别协议、生物特征识别、电子凭证技术等；

身份认证：certification

通过了身份验证，发放“证件”的过程。
关键技术：公钥密码技术、数字签名、安全协议等。

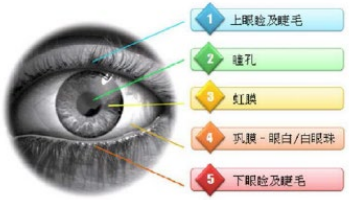
技术研究 – 基本原理





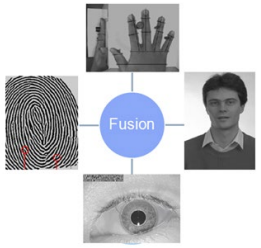
指纹识别

人脸识别



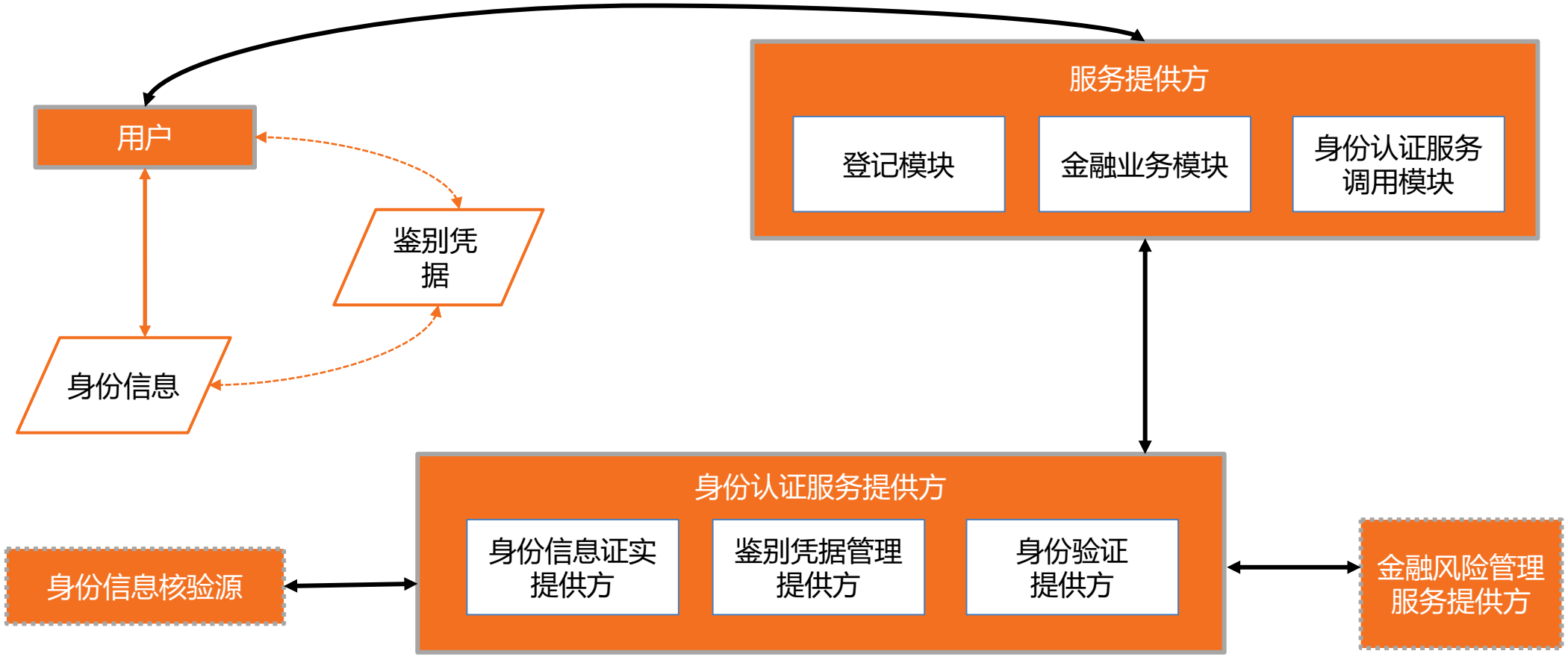
虹膜识别

…



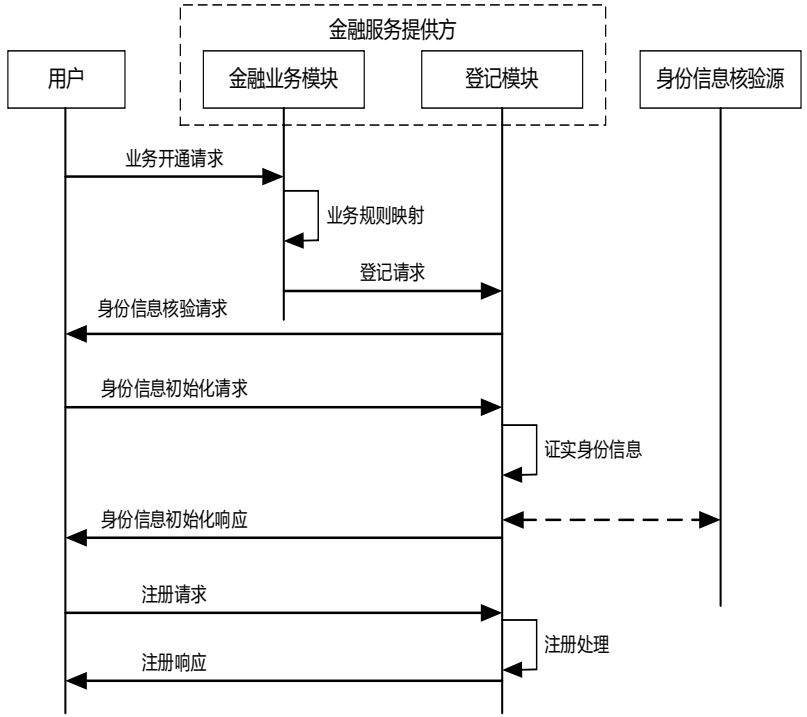
多模态识别

技术研究 – 金融服务网络身份认证系统架构

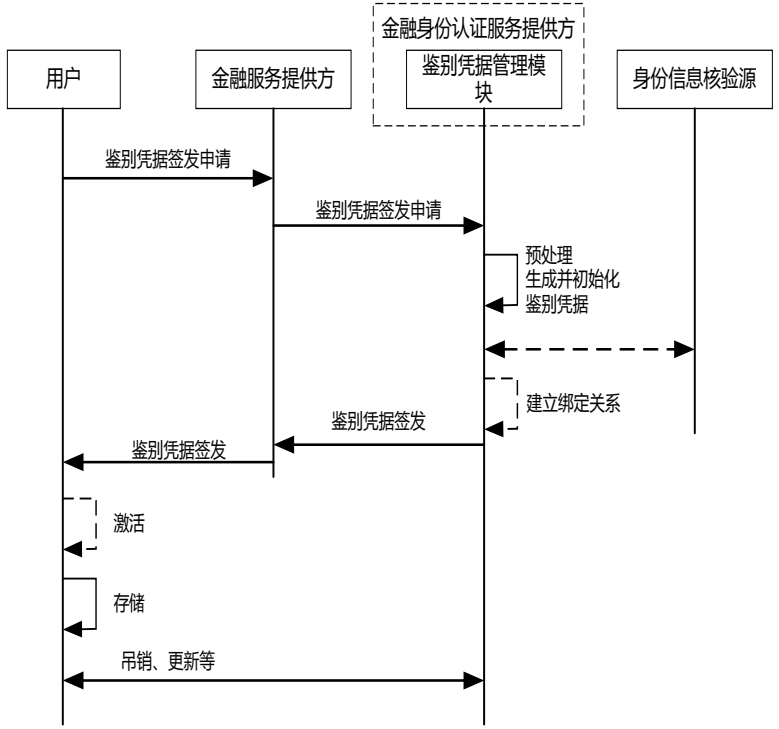


技术研究 –金融服务网络身份认证业务流程

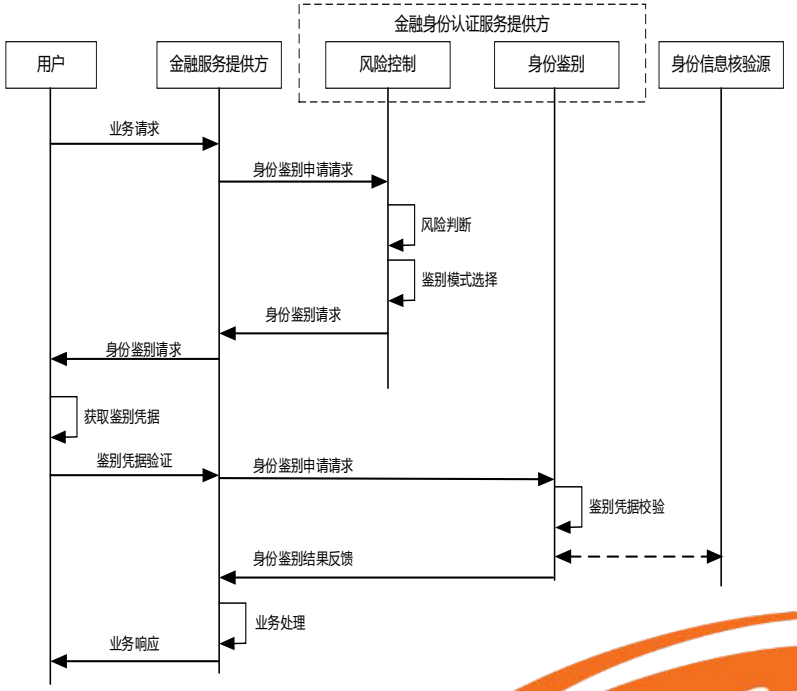
登记（身份信息证实及注册）



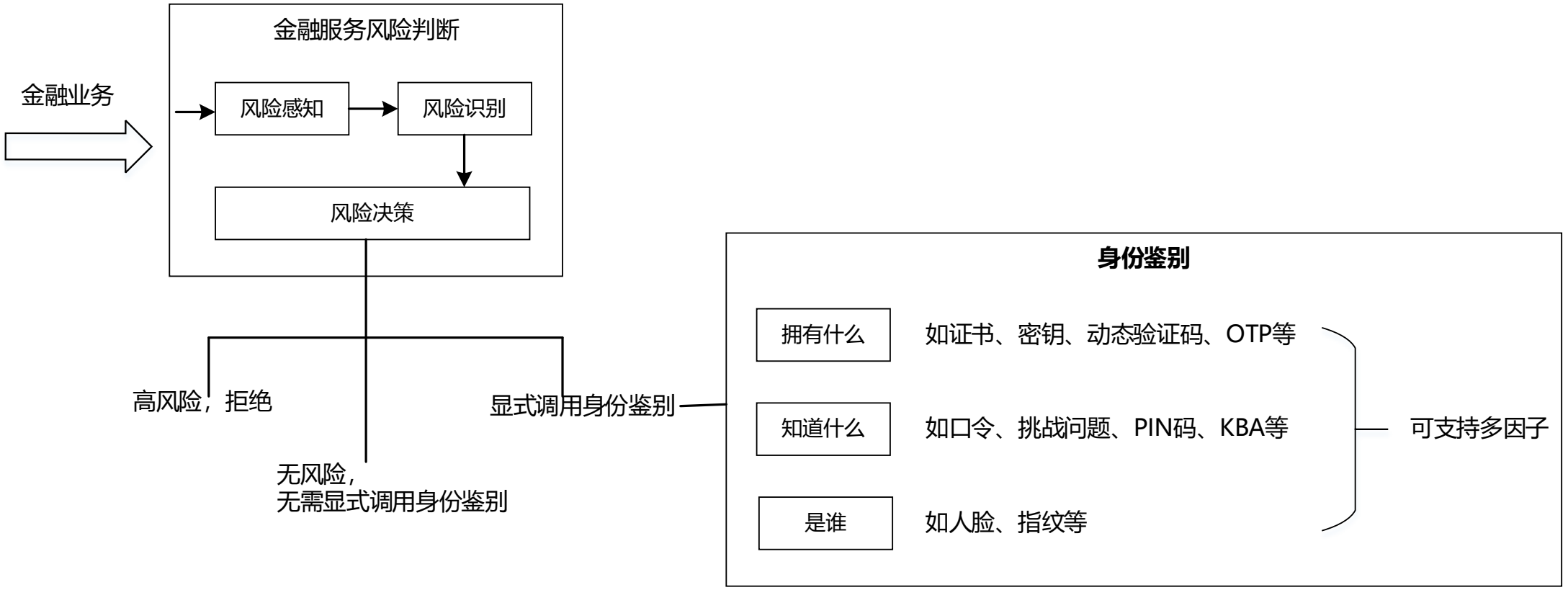
鉴别凭据签发及管理



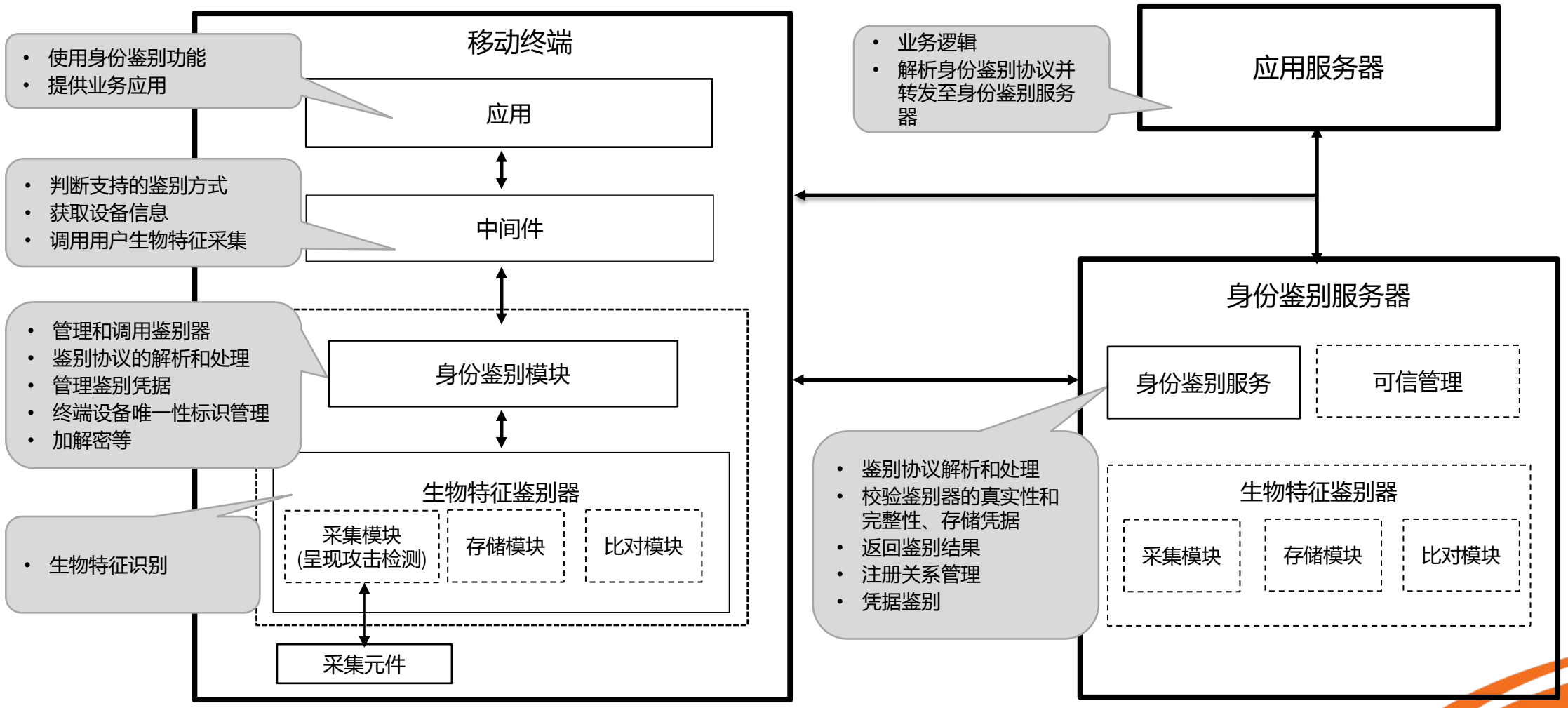
身份鉴别



技术研究 – 结合风险控制的金融服务网络身份鉴别

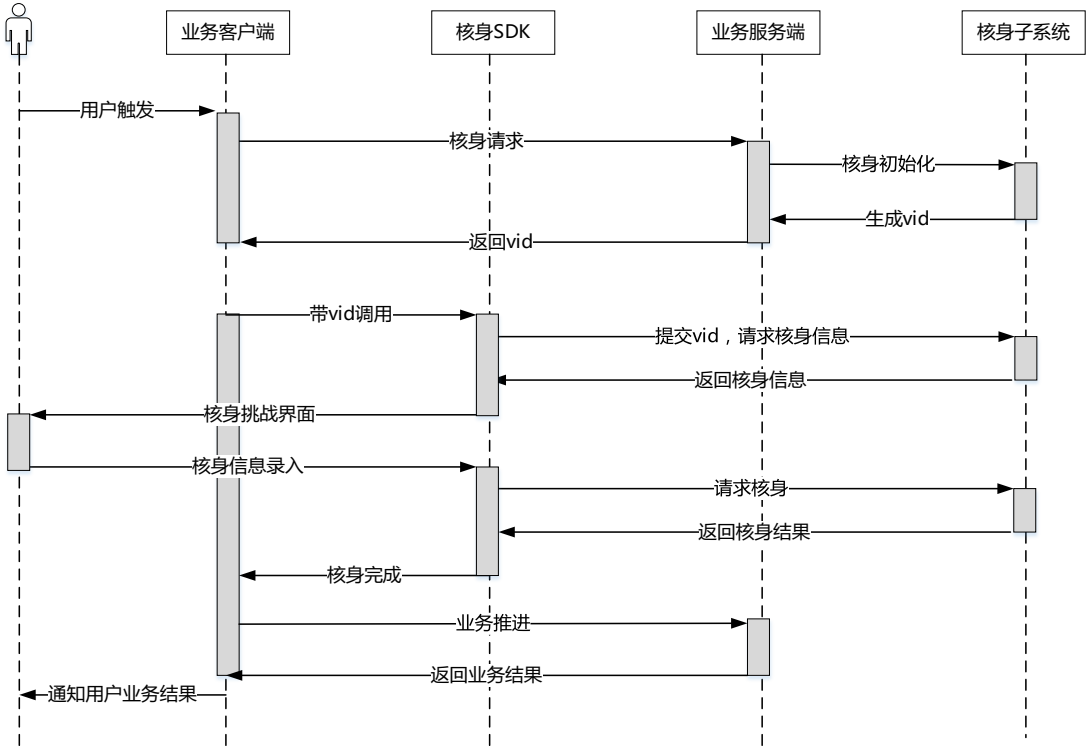


技术研究 – 本地免密

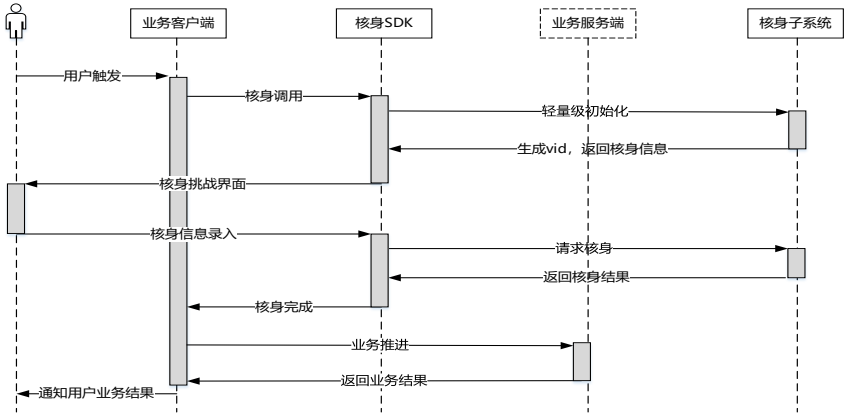


技术研究 - 协议设计

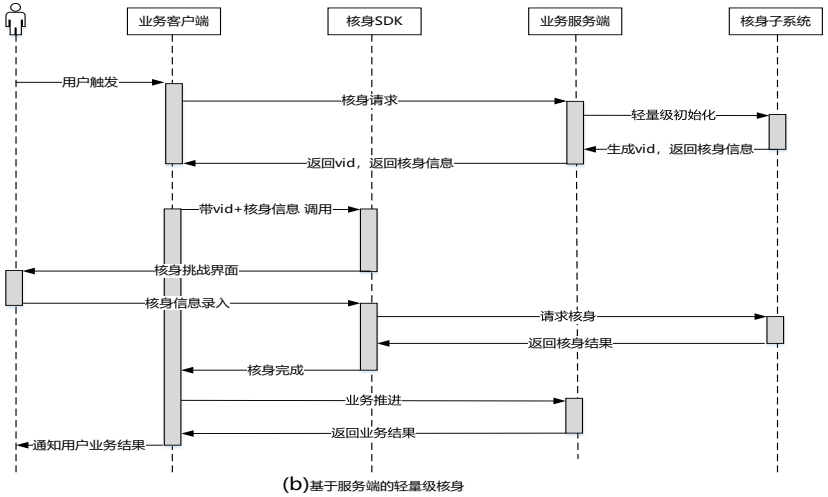
弱网环境下，4次RPC失败概率会严重影响用户体验和身份认证成功率，因此设计了轻量级模式，合并初始化和渲染RPC，提升用户体验，并保证对大规模并发业务的良好支持



基础的核身服务调用时序
(4个RPC过程)



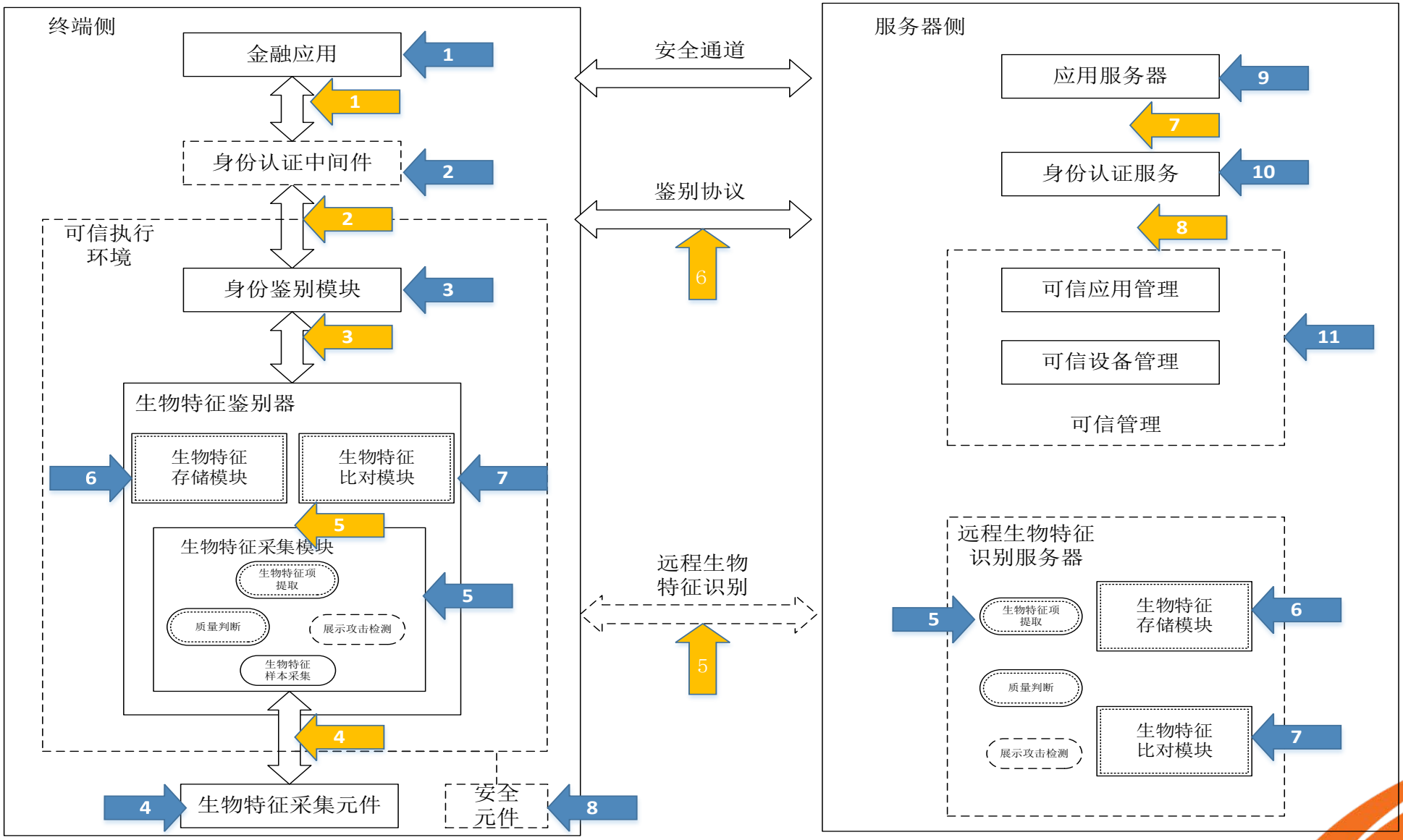
(a)基于客户端的轻量级核身



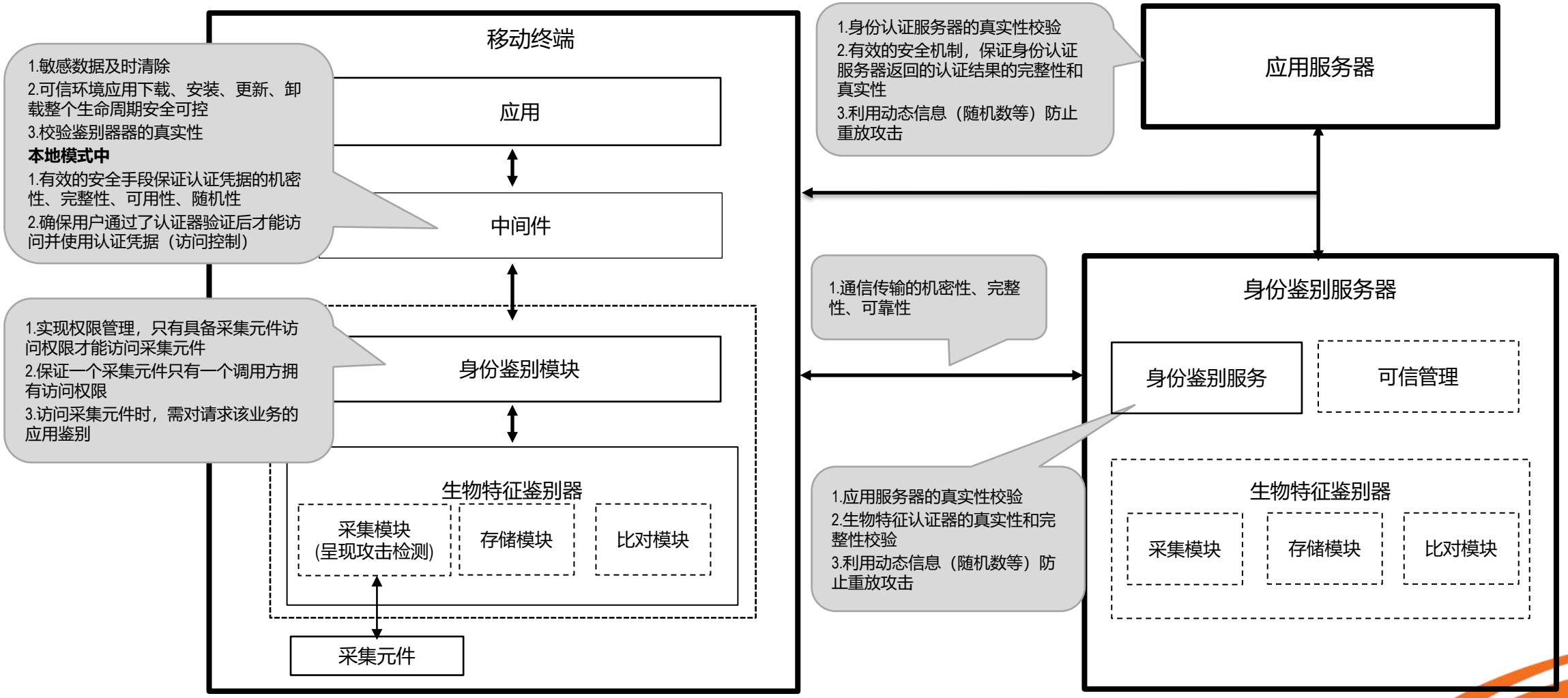
(b)基于服务端的轻量级核身

改进的轻量级核身服务调用时序
(a：基于客户端的模式)
(b：基于服务端的模式)

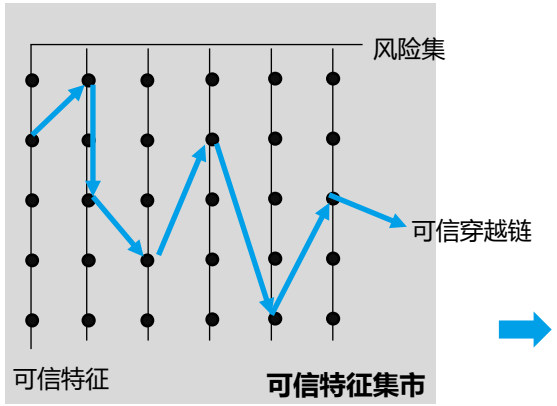
技术研究 - 安全威胁


终端侧
金融应用
身份认证中间件
可信执行环境
身份鉴别模块
生物特征鉴别器
生物特征存储模块
生物特征比对模块
生物特征采集模块
生物特征项提取
质量判断
展示攻击检测
生物特征样本采集
生物特征采集元件
安全元件
安全通道
鉴别协议
远程生物特征识别
服务器侧
应用服务器
身份认证服务
可信应用管理
可信设备管理
可信管理
远程生物特征识别服务器
生物特征项提取
生物特征存储模块
质量判断
展示攻击检测
生物特征比对模块

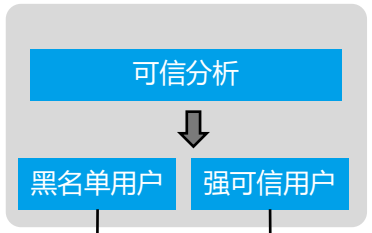
技术研究 – 安全要求


移动终端
应用
中间件
身份鉴别模块
生物特征鉴别器
采集模块
(呈现攻击检测)
存储模块
比对模块
采集元件
1.敏感数据及时清除
2.可信环境应用下载、安装、更新、卸载整个生命周期安全可控
3.校验鉴别器器的真实性
本地模式中
1.有效的安全手段保证认证凭据的机密性、完整性、可用性、随机性
2.确保用户通过了认证器验证后才能访问并使用认证凭据（访问控制）
1.实现权限管理，只有具备采集元件访问权限才能访问采集元件
2.保证一个采集元件只有一个调用方拥有访问权限
3.访问采集元件时，需对请求该业务的应用鉴别
1.身份认证服务器的真实性校验
2.有效的安全机制，保证身份认证服务器返回的认证结果的完整性和真实性
3.利用动态信息（随机数等）防止重放攻击
应用服务器
1.通信传输的机密性、完整性、可靠性
身份鉴别服务器
身份鉴别服务
可信管理
生物特征鉴别器
采集模块
存储模块
比对模块
1.应用服务器的真实性校验
2.生物特征认证器的真实性和完整性校验
3.利用动态信息（随机数等）防止重放攻击

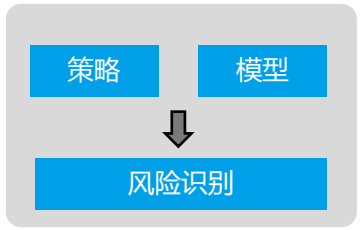
技术研究 – 风险控制



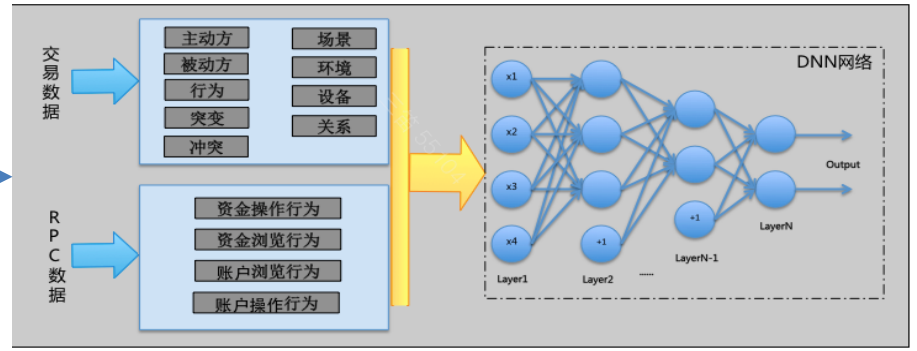
快速识别



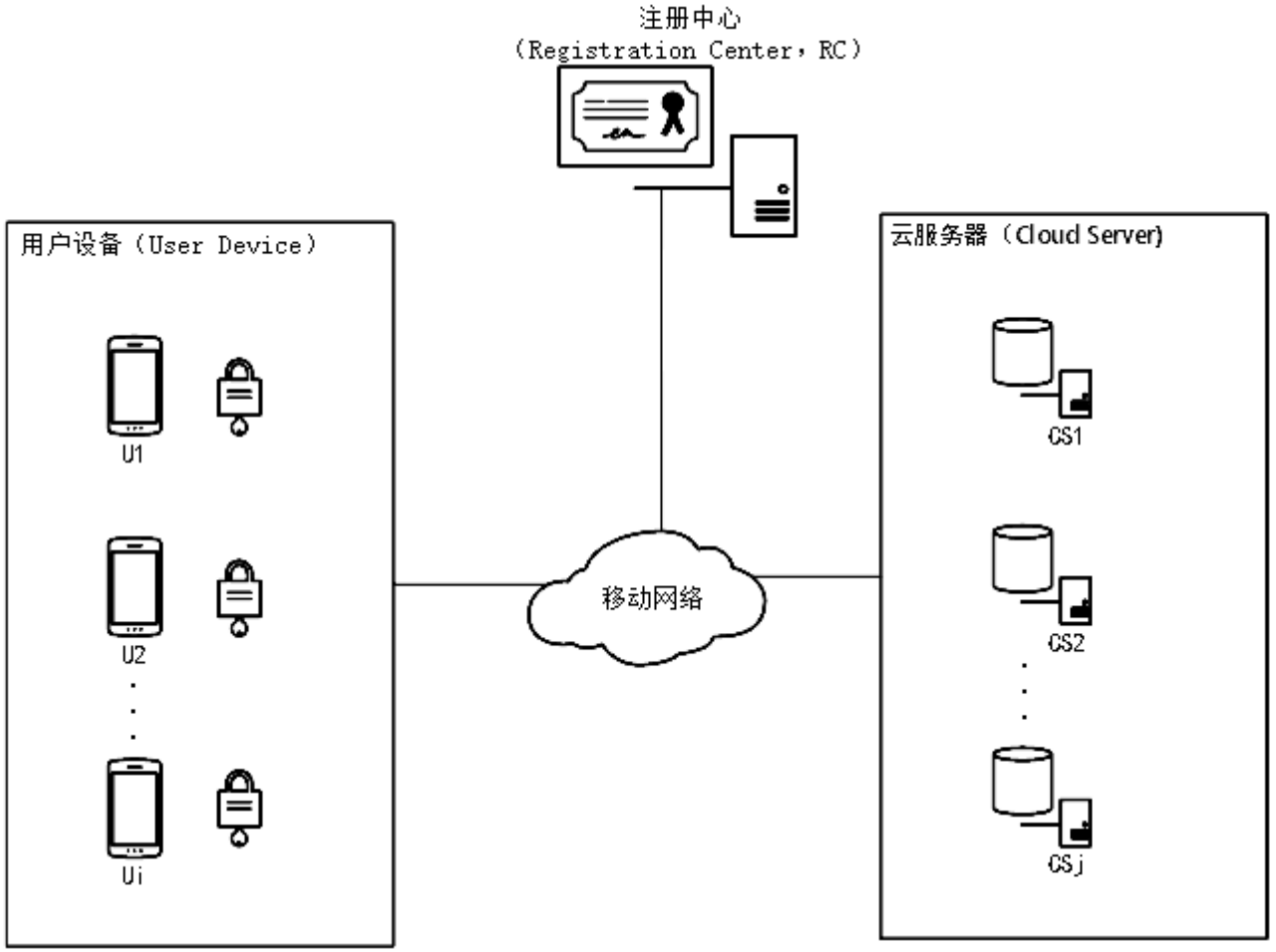
深度识别



深度识别模型（DNN）



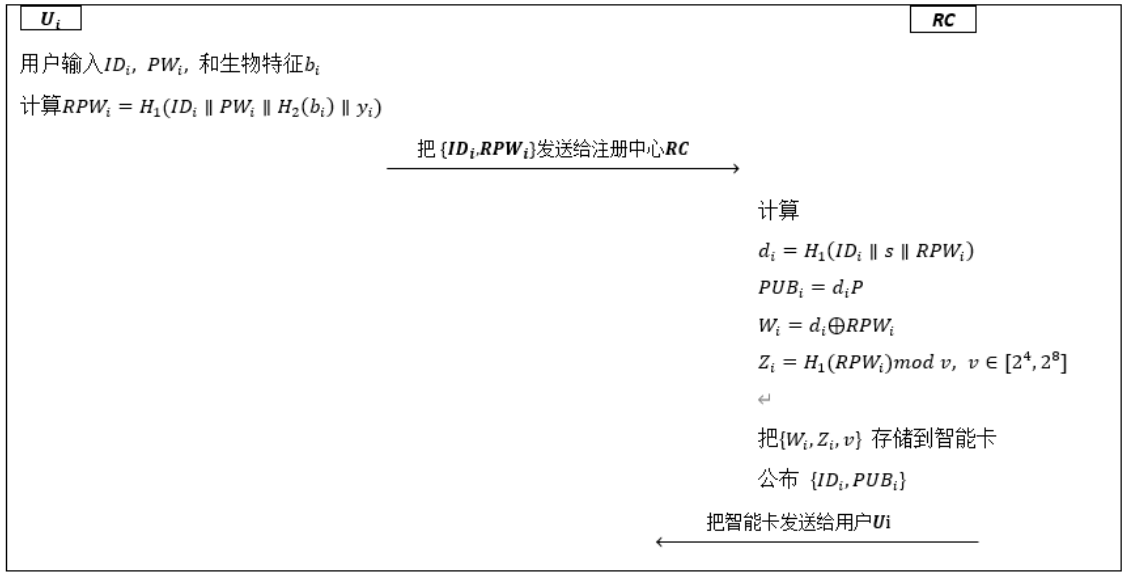
技术研究 – 协议研究案例

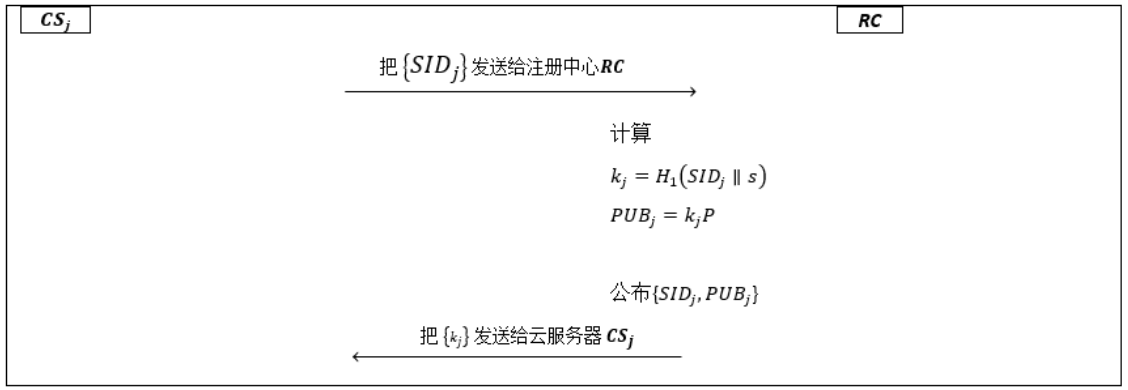


面向移动云计算的基于三因素的身份认证方法

用于在不传递用户隐私情况下，实现用户设备和云服务器的双向认证，同时实现会话密钥的协商生成；注册中心仅仅负责注册，不参与后续认证，保证用户设备和云服务器双向认证的性能。此外，还支持智能卡远程撤销、口令和生物特征更新等功能，能够满足用户使用中的各种需求。

技术研究 – 协议研究案例





预部署阶段：

由注册中心*RC*执行，其旨在生成所述认证系统的相关参数，以用于后续的注册、认证等步骤。具体的，注册中心*RC*在一素域F_p中选定椭圆曲线群E_q，并确定所述素域E_q的一个生成元P。此外，注册中心还确定主密钥s，安全哈希函数H_1（）和生物哈希函数H_2（），并公布{E_q，P}。

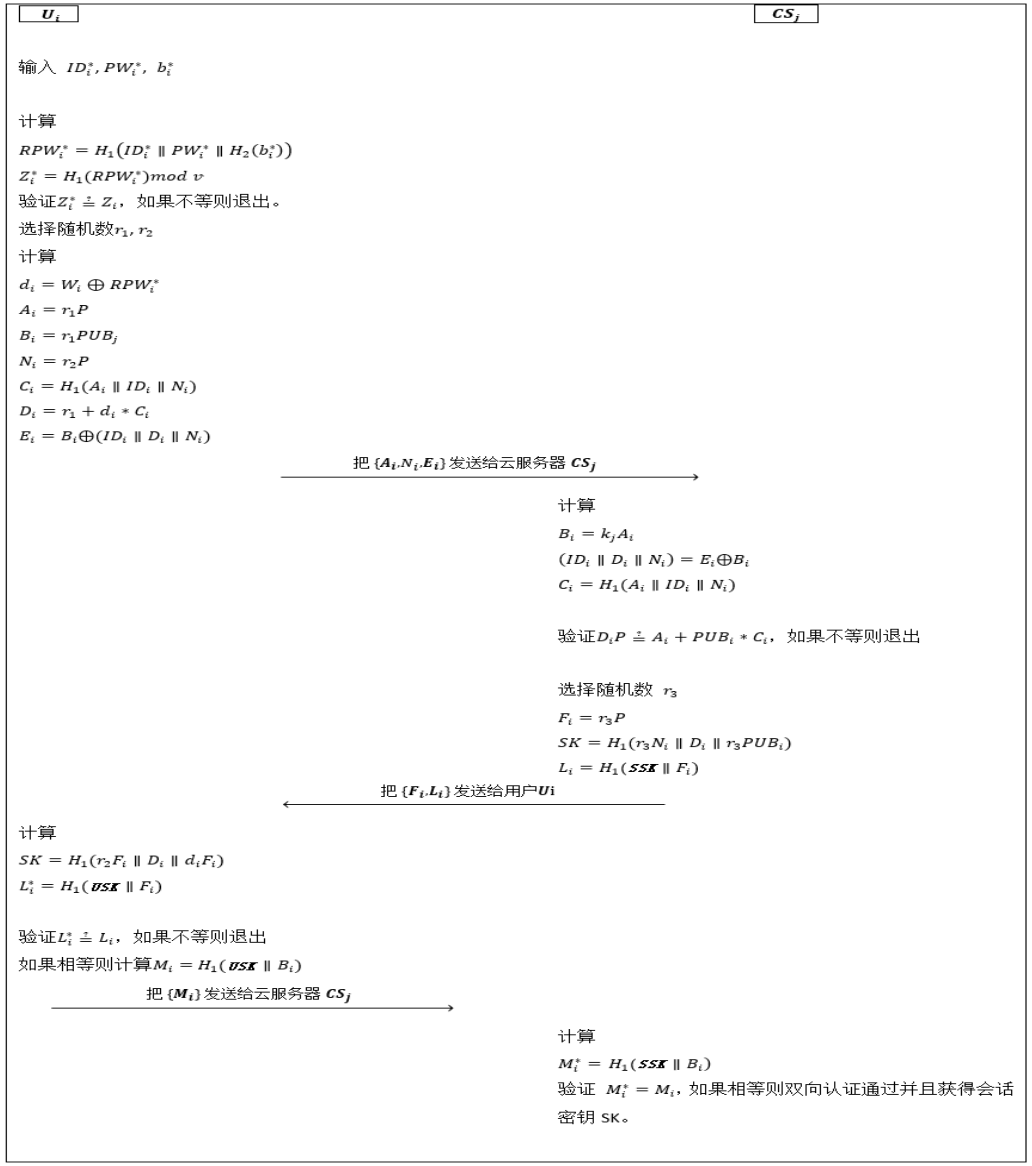
用户设备注册阶段：

用户设备U_i向注册中心*RC*进行注册，以获得智能卡。智能卡作为由用户设备U_i保存的数字凭证，存储有用于后续与云服务器CS_j认证用的验证信息，以及能够使用户设备U_i计算获得用户设备私钥。

云服务器注册阶段：

云服务器CSj向注册中心RC进行注册，以获得云服务器私钥kj。

技术研究 – 协议研究案例



身份认证阶段：

步骤1：用户U_i 输入ID_i^*、PW_i^*和生物特征b_i^*，并且计算$RPW_i^* = H_1(ID_i^* \| PW_i^* \| H_2(b_i^*) \| y_i)$，$Z_i^* = H_1(RPW_i^*) mod\ v$。验证$Z_i^* \stackrel{?}{=} Z_i$，如果等式不成立则协议终止；如果相等，用户$U_i$选择随机数$r_1$和$r_2$，计算$d_i = W_i \oplus RPW_i^*$，$A_i = r_1 P$，$B_i = r_1 PUB_j$，$N_i = r_2 P$，$C_i = H_1(A_i \| ID_i \| N_i)$，$D_i = r_1 + d_i * C_i$，$E_i = B_i \oplus (ID_i \| D_i \| N_i)$。用户$U_i$通过可靠信道将消息$\{A_i, N_i, E_i\}$发送给云服务器$CS_j$。

步骤2：收到$\{A_i, N_i, E_i\}$以后，云服务器CS_j计算$B_i = k_j A_i$，$(ID_i \| D_i \| N_i) = E_i \oplus B_i$，$C_i = H_1(A_i \| ID_i \| N_i)$。检查$D_i P \stackrel{?}{=} A_i + PUB_i * C_i$，如果等式不成立则协议终止；如果相等，选择随机数 r_3，计算$F_i = r_3 P$，$SK = H_1(r_3 N_i \| D_i \| r_3 PUB_i)$，$L_i = H_1(SK \| F_i)$。云服务器$CS_j$把消息$\{\boldsymbol{F_i, L_i}\}$发送给用户$U_i$。

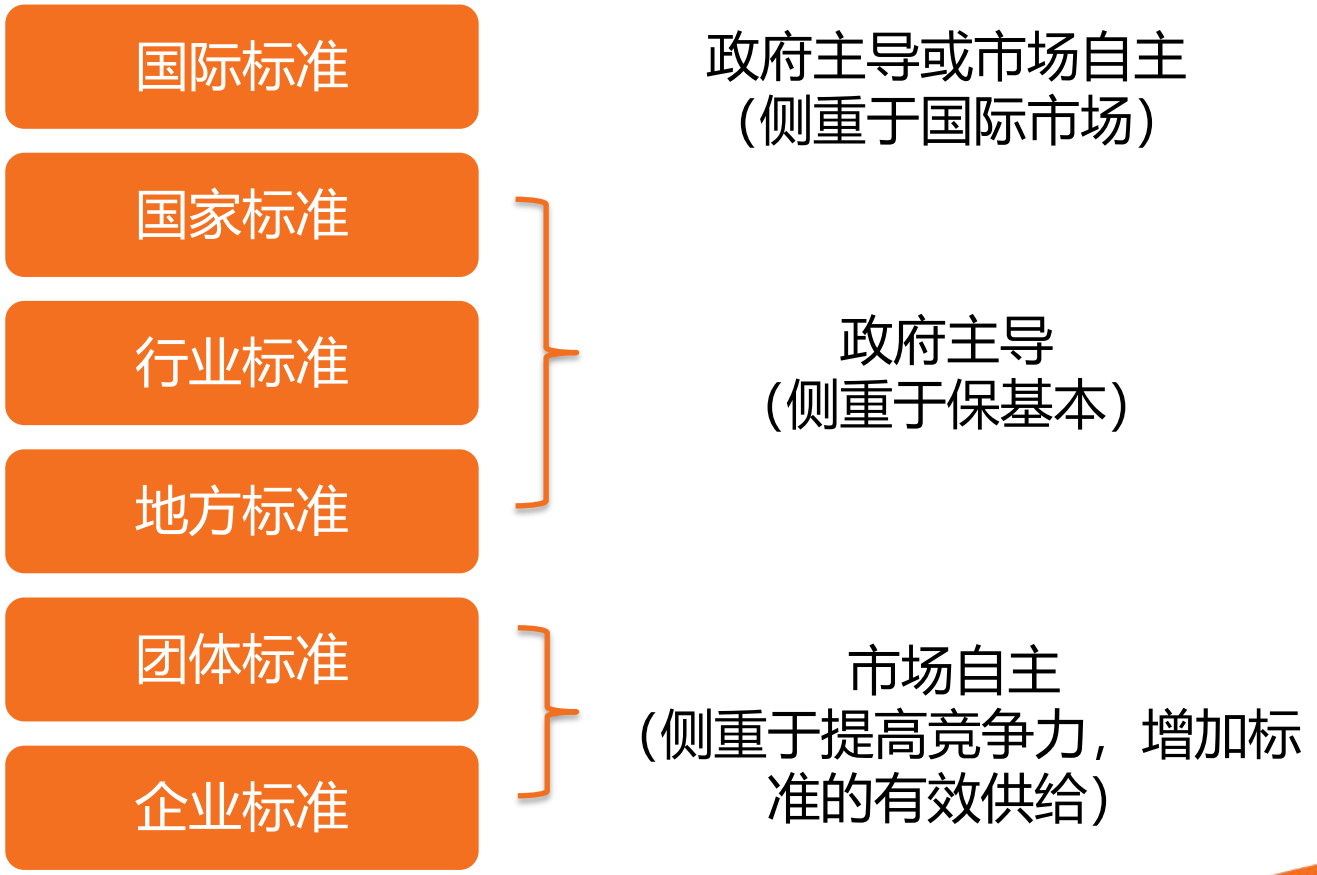
步骤3：收到消息$\{\boldsymbol{F_i, L_i}\}$以后，智能卡计算$SK = H_1(r_2 F_i \| D_i \| d_i F_i)$，$L_i^* = H_1(SK \| F_i)$。验证$L_i^* \stackrel{?}{=} L_i$，如果等式不成立则协议终止；如果相等则计算$M_i = H_1(SK \| B_i)$。用户$U_i$把消息$\{M_i\}$发送到云服务器$CS_j$。

步骤4：收到消息$\{M_i\}$以后，云服务器CS_j计算$M_i^* = H_1(SK \| B_i)$。验证$M_i^* = M_i$，如果相等则用户和云服务器完成相互认证，并且获得会话密钥SK。

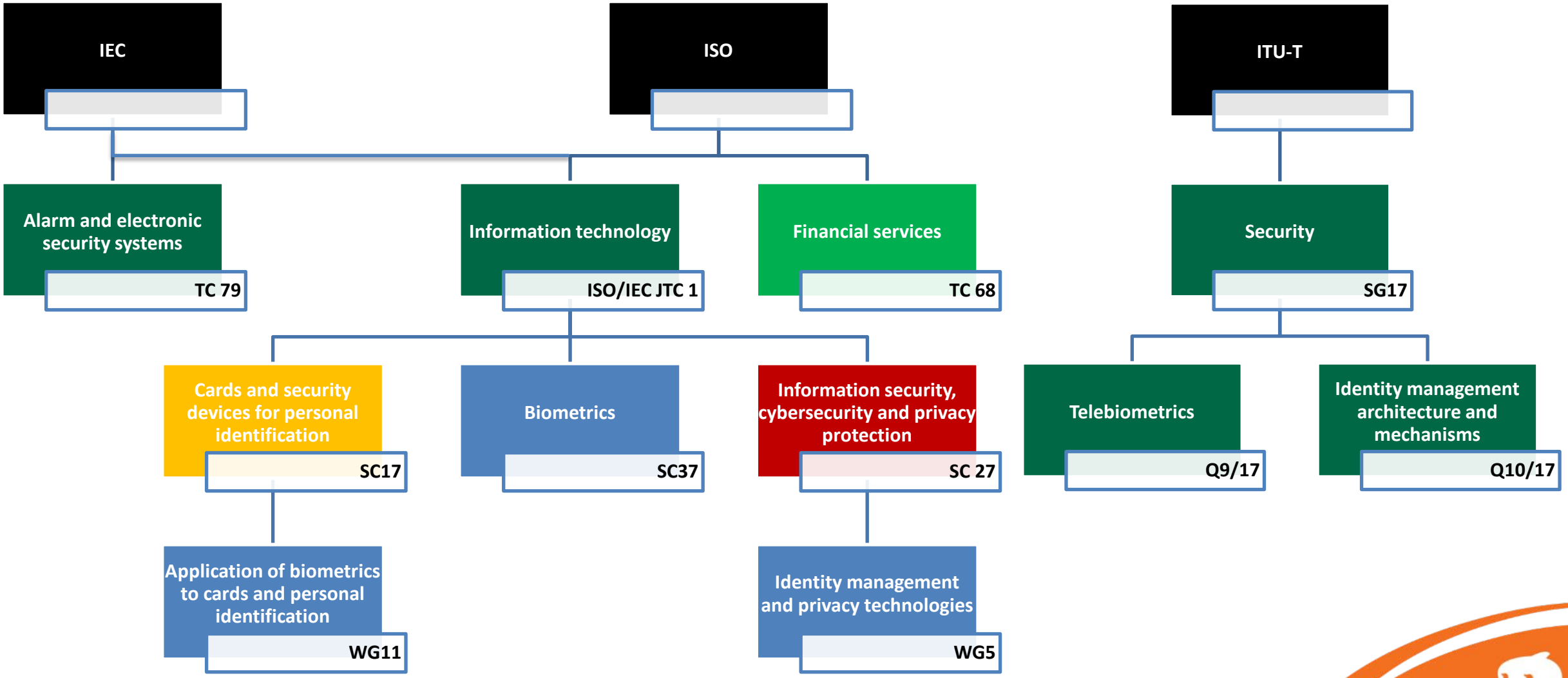
4 标准介绍

标准介绍 – 基本概念

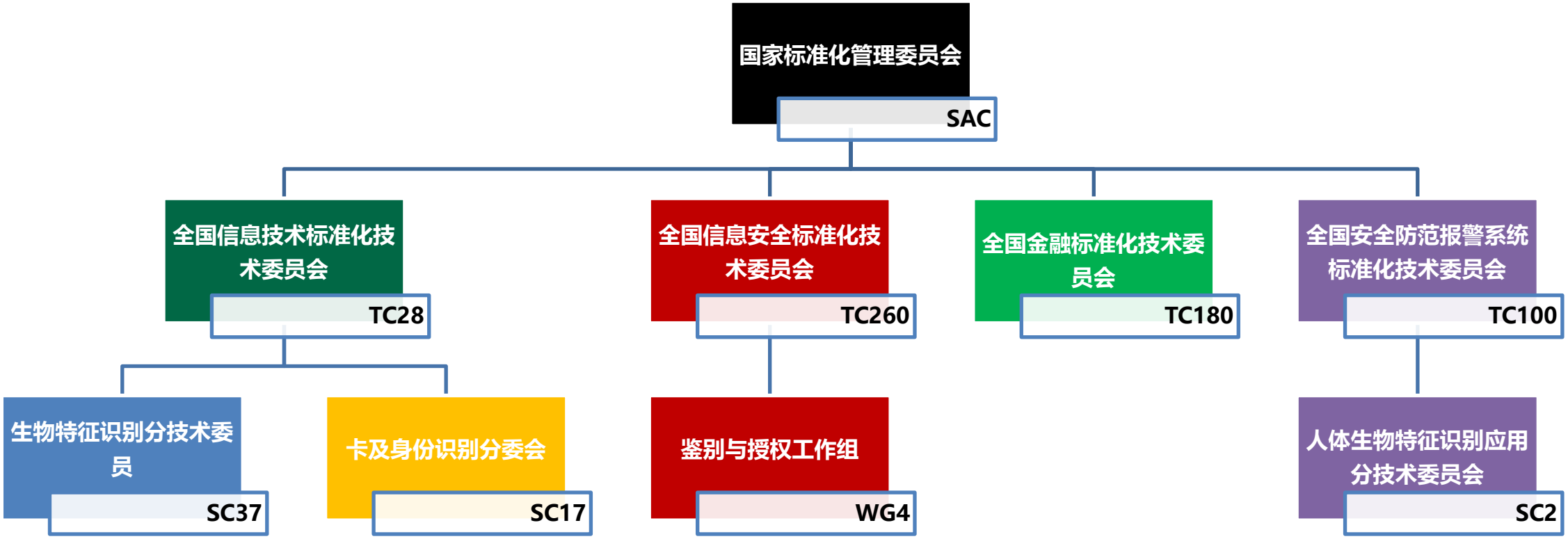
定义：为在**一定范围**内获得最佳秩序，对活动或其结果规定**共同的和重复使用**的规则、导则或特性的文件。该文件经**协商一致**制定并经一个**公认机构**的批准。它以科学、技术和实践经验的综合成果为基础，以促进最佳社会效益为目的。



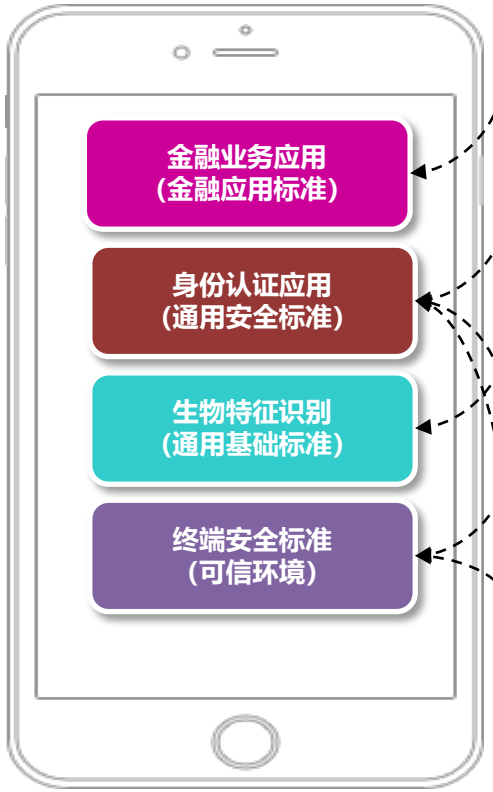
标准介绍 – 相关国际标准组织



标准介绍 – 相关国家标准组织



标准介绍 – 标准体系



1. ISO TC68 2. 全国金融标准化技术委员会 3. 互联网金融协会	金融业务应用（金融应用标准）	1. ISO 19092 Financial services -- Biometrics -- Security framework 2. GB/T 27912-2011 金融服务 生物特征识别 安全框架
1. ISO/IEC JTC1 SC27 2. 全国信息安全标准化技术委员会	身份认证应用（通用安全标准）	1. ISO/IEC 24745:2011 Information technology -- Security techniques -- Biometric information protection 2. ISO/IEC 27553 Security requirements authentication using biometrics on mobile devices 3. GB/T 38542-2020 基于生物特征识别的移动智能终端身份鉴别技术框架 4. GB/T 38671-2020 信息安全技术 远程人脸识别系统技术要求
1. ISO/IEC JTC1 SC37 2. 全国信息技术标准化技术委员会	生物特征识别（通用基础标准）	1. ISO/IEC 30107 Information technology -- Biometric presentation attack detection 2. ISO/IEC TR 30125 Information technology -- Biometrics used with mobile devices 3. GB/T 37036.1 技术要求 第1部分：通用要求 4. GB/T 37036.2 移动设备生物特征识别技术要求 第2部分：指纹 5. GB/T 37036.3 移动设备生物特征识别技术要求 第3部分：人脸 6. GB/T 37036.4 移动设备生物特征识别技术要求 第4部分：虹膜
1. ITU-T SG17 2. 中国通信标准化协会		
IFAA / Sorter/ FIDO	终端安全标准（可信环境）	1. JR/T 0156-2017 移动终端支付可信环境技术规范 2. 移动设备可信执行环境技术要求 3. GP TEE Specs 4. IFAA 2.0协议 5. FIDO UAF Spec ...
GlobalPlatform		
国家密码行业标准化委员会		

5 标准思路

标准思路 – 标准价值

标准价值：基于用户应用场景需求，围绕产业痛点，通过标准联盟连接产业伙伴，提供中立、安全并具有更优秀用户体验的认证方式，为迅速发展的业务提供支持。

产业链路长，效能低下
碎片化严重，安全风险高

建立标准
生态合作

IIFAA：建立标准形成全链路安全
解决方案

打穿标准体系
赢得市场主动

国际标准

- ISO 27553 移动设备生物特征识别身份鉴别安全要求
- ISO 5158 移动金融服务客户身份鉴别指南
- IEEE P2790 活体检测
- IEEE P2859 多模态融合

国家标准

- GBT 37036.XX 移动设备生物特征识别系列国家标准
- GBT 38542-2020 基于生物特征识别的移动智能终端身份鉴别技术框架

联盟标准

- IFAA本地免密技术规范2.0
- IFAA本地免密检测规范

- 接入速度
- 场景覆盖
- 设备覆盖
- 用户覆盖

标准思路 – 标准解读

《基于生物特征识别的移动智能终端身份鉴别技术框架》(GB/T 38542-2020)：规范通用的基于生物特征识别的移动智能终端身份鉴别技术框架。

- 为移动智能终端上基于生物特征识别技术的身份鉴别相关应用的设计、开发、使用提供统一的基础技术架构。
- 以此技术框架为基准，为身份鉴别的相关功能单元、接口、协议的规范化建立功能和安全性方面的基本要求。

标准思路 – 标准解读

01

统一技术架构

系统研究业界已有技术成果，参考国际国内标准，结合实际应用，形成统一的技术架构

02

规范功能要求

结合实际应用，规范技术框架各功能单元的基本功能要求

03

规范信息安全要求

结合已有标准和现实情况保障移动智能终端生物特征识别信息安全

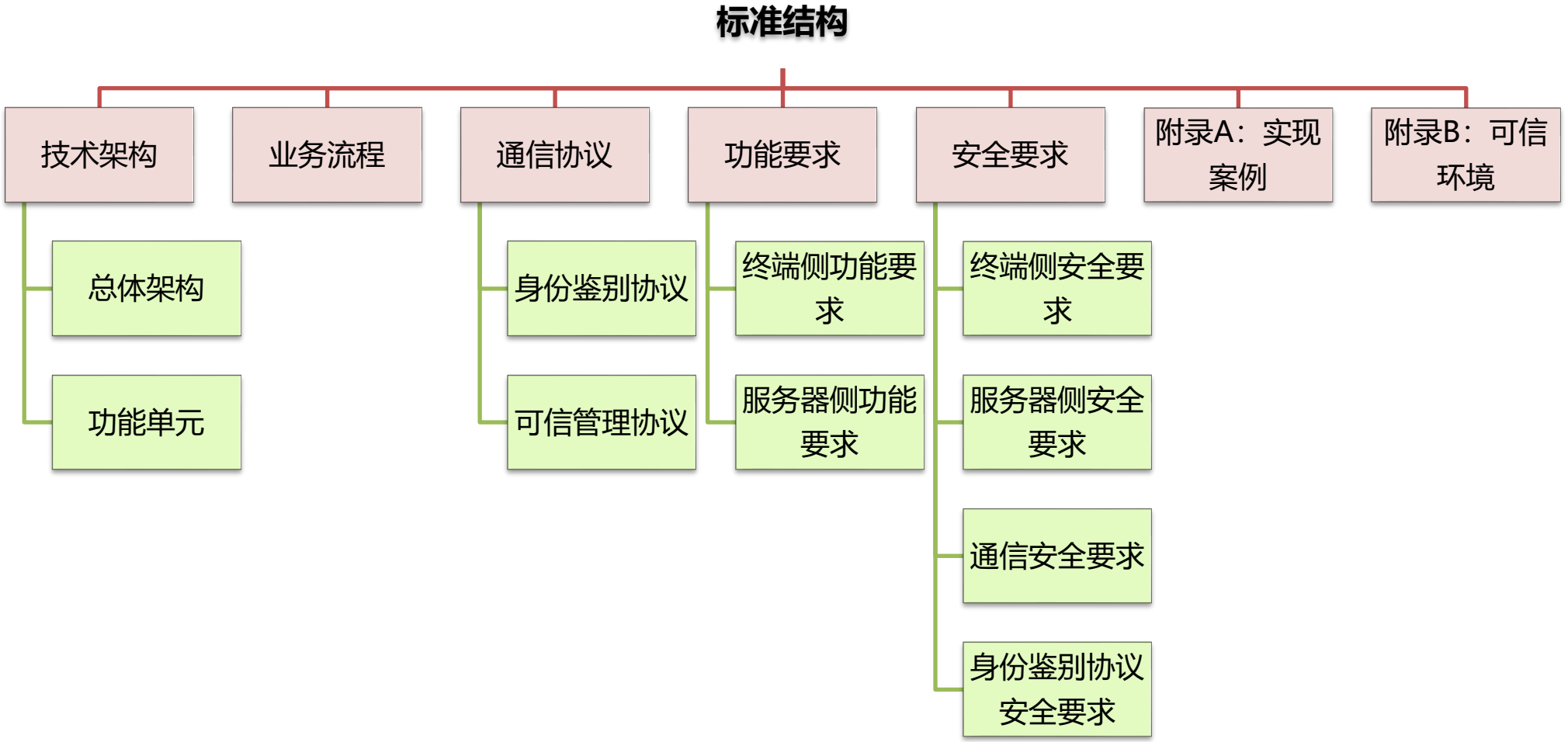
04

规划标准体系

以技术框架为基础，规划基于生物特征识别技术移动智能终端身份认证标准体系

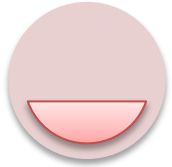
实现安全、便捷、统一的智能终端生物识别身份认证技术框架，降低集成成本，提高安全性，更好的服务用户，促进产业持续发展和创新。

标准思路 – 标准解读


标准结构
技术架构
业务流程
通信协议
功能要求
安全要求
附录A：实现案例
附录B：可信环境
总体架构
功能单元
身份鉴别协议
可信管理协议
终端侧功能要求
服务器侧功能要求
终端侧安全要求
服务器侧安全要求
通信安全要求
身份鉴别协议安全要求

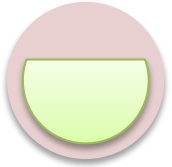
标准思路 – 标准解读

附录A：基于指纹识别的身份鉴别应用主要可分为注册、鉴别和注销三个流程。



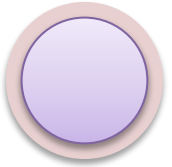
注册

第三方应用获取当前的指纹认证数据信息（主要是Authenticator ID、Fingerprint ID），使指纹认证与第三方应用的业务或账户关联。



鉴别

由指纹认证模块进行指纹认证，第三方应用在得到认证结果后，再根据结果授权相应业务或者账号。

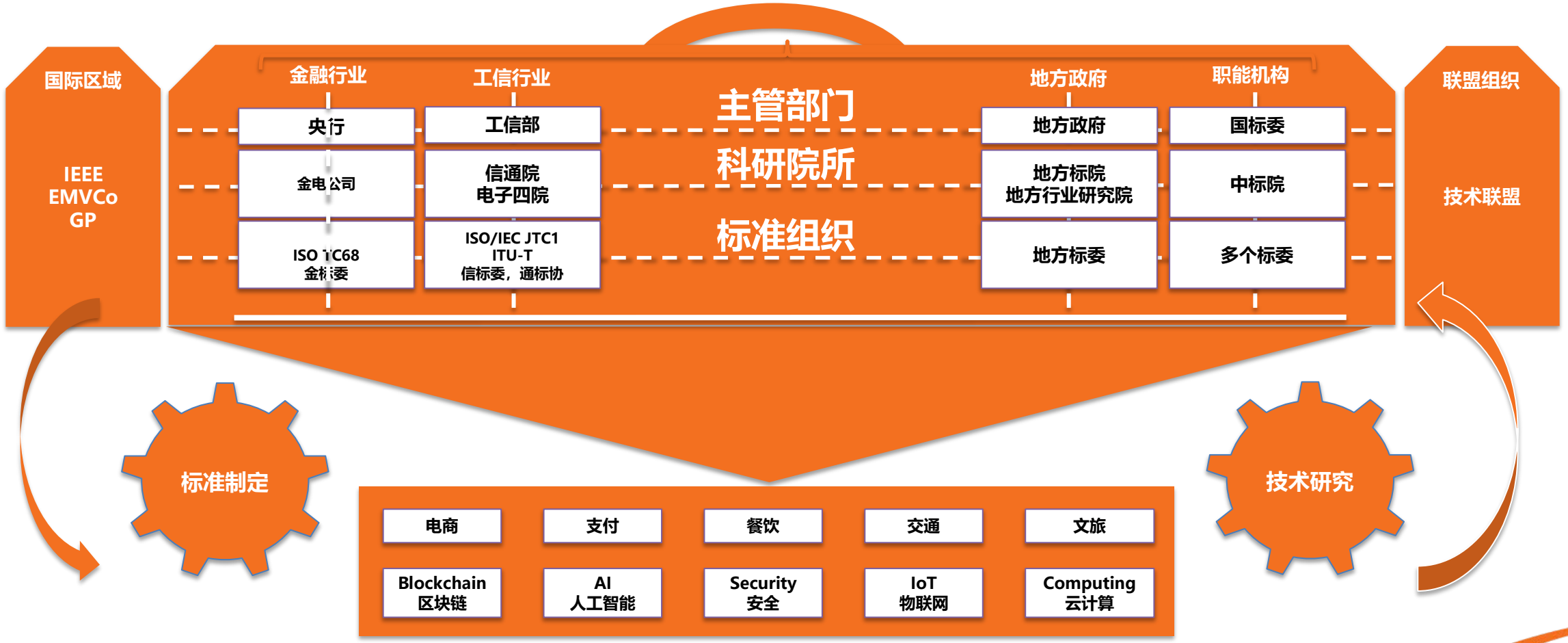


注销

身份鉴别服务器删除对应鉴别公钥，指纹认证模块删除相应的鉴别私钥。

6 梳理总结

梳理总结


国际区域
IEEE
EMVCo
GP
金融行业
工信行业
地方政府
职能机构
主管部门
科研院所
标准组织
央行
工信部
地方政府
国标委
金电公司
信通院
电子四院
地方标院
地方行业研究院
中标院
ISO TC68
金标委
ISO/IEC JTC1
ITU-T
信标委，通标协
地方标委
多个标委
联盟组织
技术联盟
标准制定
技术研究
电商
支付
餐饮
交通
文旅
Blockchain
区块链
AI
人工智能
Security
安全
IoT
物联网
Computing
云计算

Alibaba Group
阿里巴巴集团

阿里巴巴标准化

谢 谢

Thank You