附件

ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0092—2019
代替 JR/T 0092—2012

移动金融客户端应用软件安全管理规范

Financial mobile application software security management specification

2019－09－27 发布　　2019－09－27 实施

中国人民银行　　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替JR/T 0092—2012《中国金融移动支付 客户端技术规范》，与JR/T 0092—2012相比，主要技术变化如下：

——修改了范围描述（见第1章，2012年版第1章）；

——增加了术语和定义（见第2章）；

——删除了规范性引用文件（2012年版第2章）；

——删除了“应用场景”（2012版第3章）；

——删除了“客户端软件系统架构”（2012年版第4章）；

——删除了“客户端基本功能及流程”（2012年版第5章）；

——增加了总体要求（见第4章）；

——全面梳理完善客户端应用软件安全要求，区分基本要求和增强要求（见第5、6章，2012年版第6、7章）；

——将“人机交互安全”改为“身份认证安全”，包括身份认证、认证信息安全（安全输入、敏感数据显示、认证失败处理）、密码的设定与重置三部分安全要求（见5.1，2012年版6.1）；

——增加了逻辑安全，包括逻辑安全设计、软件权限控制、风险控制、回退处理、异常处理等安全要求（见5.2）；

——增加了安全功能设计，包括组件安全、接口安全、抗攻击能力、客户端环境检测安全（见5.3）；

——增加了密码算法及密钥管理（见5.4）；

——修改了数据安全要求，在数据获取、数据访问控制、数据传输、数据存储、数据销毁等方面提出具体安全要求（见5.5，2012年版6.3）；

——修改了客户端应用软件管理要求，增加了设计、开发、发布等环节的要求（见第6章，2012年版第7章）；

——增加了不收集与所提供服务无关的个人金融信息、收集个人金融信息前需经用户的明示同意、不得变相强迫用户授权、不得违反约定收集使用个人金融信息的要求（见6.1）；

——客户端软件发布环节明确了由客户端应用软件所有方进行签名的要求（见6.3，2012年版7.4）；

——增加了以SDK等形式对外提供金融交易类服务时对于信息记录的要求（见6.4）；

——增加了敏感数据的相关描述（见资料性附录A）；

——增加了客户端应用软件应用智能语音交互技术（见资料性附录B）。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国金融电子化公司。

本标准参加起草单位：中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国邮政储蓄银行股份有限公司、中国银联股份有限公司、中国民生银行股份有限公司、中信银行股份有限公司、中移电子商务有限公司、天翼电子商务有限公司、联通支付有限公司、浙江蚂蚁小微金融服务集团股份有限公司、财付通支付科技有限公司、京东数字科技控股有限公司、拉卡拉支付股份有限公司、北京中金国盛认证有限公司、北京银联金卡科技有限公司、中金金融认证中心有限公司、

信息产业信息安全测评中心、工业和信息化部计算机与微电子发展研究中心、北京软件产品质量检测检验中心、科大讯飞股份有限公司。

本标准主要起草人：李伟、李兴锋、杨倩、聂丽琴、王晓燕、程胜、汤沁瑩、关晓辉、刘雨露、郭栋、刘运、刘力慷、付小康、张行、高志民、高强裔、黄本涛、王飞宇、吴永强、陈伟、宋立国、黄江、张健、高原、陈龙、周思捷、周小淋、李宇、朱克雷、韩璐、刘健松、刘宪伟、赵亮、姚建伟、黄晓培、刘磊、曹炜、孙朝阳、宋铮、邓凡平、赖穆彬、史立龙、王鸿娴、王冠华、王秀君、马洪涛、孙款、纪崇廉、马松松、胡一鸣、于泉、吴振宇、吕坤、马万钟、蒯天祥、张文博、曹小龙、李盛昌、任旭龙、陕晨阳、杨银鹏、刘婷、刘琼瑶。

本标准所代替标准的历次版本发布情况为：

——JR/T 0092—2012，JR/T 0092—2012于2012年12月首次发布，本次为第1次修订。

移动金融客户端应用软件安全管理规范

1 范围

本标准规定了移动金融客户端应用软件的安全要求，以及客户端应用软件设计、开发、维护和发布的管理要求。

本标准适用于移动金融客户端应用软件的设计、开发、维护及发布过程，也适用于评估机构对相关应用进行安全性和标准符合性评估。

2 术语和定义

下列术语和定义适用于本文件。

2.1

移动金融客户端应用软件 financial mobile application software

在移动终端上为用户提供金融交易服务的应用软件。

注：包括但不限于可执行文件、组件等。

2.2

资金交易类客户端应用软件 capital transaction client application software

直接面向用户提供资金交易服务的移动金融客户端应用软件。

注：包括但不限于手机银行、支付APP等。

2.3

信息采集类客户端应用软件 information collection client application software

不直接向用户提供资金交易服务，但需采集个人敏感信息的移动金融客户端应用软件。

2.4

资讯查询类客户端应用软件 information query client application software

仅提供金融产品推介、信息查询、资讯推送等服务的移动金融客户端应用软件。

2.5

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注1：包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

注2：改写 GB/T 35273—2017，定义 3.1。

2.6

支付敏感信息 payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

2.7

语音识别 automatic speech recognition

将人类语音中的词汇内容转换为计算机可读的输入。

示例：按键、二进制编码或者字符序列。

2.8

语音合成 text to speech

将文本信息转化为语音数据的技术，涉及声学、语言学、数字信号处理、多媒体等多种前沿的高新科技。

2.9

自然语言理解 natural language processing

使用自然语言同计算机进行通讯的技术。

2.10

第三方信源 the third party source

客户端应用软件调用语音能力时可以接入的第三方服务。

3 缩略语

下列缩略语适用于本文件。

APP：客户端应用软件（Application software）

URI：统一资源标识符（Uniform Resource Identifier）

TEE：可信执行环境（Trusted Execution Environment）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

4 总体要求

客户端应用软件分为资金交易类、信息采集类和资讯查询类。资金交易类客户端应用软件应符合资金交易、信息保护等所有技术及管理安全要求。信息采集类客户端应用软件应重点符合信息保护相关技术及管理安全要求。资讯查询类客户端应用软件参照执行相关客户端应用软件安全和管理要求。

本标准安全要求分为基本要求和增强要求两个层次，基本要求是针对客户端应用软件应该具有的基本保护能力提出的安全要求，增强要求为推荐要求。

5 客户端应用软件安全要求

5.1 身份认证安全

5.1.1 认证方式

基本要求：

a） 客户端应用软件登录时应采用适宜的验证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别等方式。

b） 应确保采用的身份验证要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露，如：用于登录验证的口令和用于交易的口令不能一致。

c） 客户端应用软件交易时应按照相关业务管理要求对用户身份进行认证，如：对于大额资金交易，客户端应采用两种或两种以上要素对用户身份进行认证等。

d） 对于手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：

- 若采用手势密码作为验证要素，手势密码应至少设置连续不间断的 4 个点；
- 若采用短信验证码作为验证要素，短信验证码应仅使用一次，仅限于在规定时间内使用，短信验证码应具备长度和随机性的要求，短信验证码所在的短信内容中，告知用户短信验证码的用途；
- 若采用生物特征识别作为验证要素，应当符合国家、金融行业标准和相关信息安全管理要求，防止非法存储、复制和重放。

e） 若采用图形验证码作为验证的辅助要素，图形验证码应具有使用时间限制并仅能使用一次，图形验证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容。

f） 图形验证码不得作为独立的身份验证要素。

增强要求：

a） 客户端应用软件登录应采用两种或两种以上的要素对用户身份进行认证。

b） 在用户身份认证后，客户端应用软件进入终端系统后台时，如果超过设定时限后被唤醒切换到前台，应采取措施对用户身份重新认证。

5.1.2 认证信息安全

5.1.2.1 安全输入

基本要求：

客户端应用软件应提供客户输入银行卡支付密码和网络支付交易密码的即时防护功能，客户端应提供以下安全控制措施，或其他经攻击测试无法获取明文的安全防护措施。

a） 采取替换输入框原文。

b） 逐字符加密、字符加密。

c） 防范键盘窃听。

d） 采用自定义软键盘。

增强要求：

客户端应用软件应提供客户输入信息的即时防护功能，如：卡片验证码、卡片有效期、银行卡账号、身份证号码、手机号码等信息。

5.1.2.2 个人金融信息展示

基本要求：

a） 客户端应用软件的口令框应默认屏蔽显示，屏蔽显示时应使用同一特殊字符（例如*或•）代替。

b） 客户端应用软件不应明文显示银行卡密码和网络支付交易密码。

c） 客户端应用软件展示个人金融信息时，应符合以下要求：

- 处于未登录状态时，不应展示与个人信息主体相关的用户鉴别信息（如：卡片验证码、卡片有效期、登录密码、支付密码等）；
- 处于已登录状态时，个人金融信息展示的技术要求如下：
  - ♦ 除银行卡有效期外，用户鉴别信息（如：卡片验证码、登录密码、支付密码等）不应明文展示；
  - ♦ 对于银行卡号、客户法定名称、手机号码、证件类或其他识别标识信息等可以直接或组合后确定信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应履行客户端身份验证，并做好此类信息管理，防范此类信息泄露风险；
  - ♦ 涉及其他信息主体的信息时，宜进行屏蔽展示，当满足如下条件之一时可不脱敏：
    - ■ 其他方主动发起的活动包含的信息，如其他方发起交易、收付款；
    - ■ 与其他方已建立信任关系（间接授权），如向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人；
    - ■ 其他法律法规要求的情况。

5.1.3 认证失败处理

基本要求：

a) 客户端应用软件应提供认证失败处理功能，可采取结束会话、限制失败登录次数和自动退出等措施。

b) 在提示客户认证失败时，应模糊错误提示信息，防止错误提示信息中泄露用户全部账号、交易金额等敏感数据。

注：关于敏感数据类型和范围参见附录A。

5.1.4 密码的设定与重置

基本要求：

a) 客户端应用软件应配合服务端提供密码复杂度校验功能，保证用户设置的密码达到一定的强度，避免采用简单交易密码或与客户个人信息相似度过高的交易密码。

b) 应严格限制使用初始登录密码与初始交易密码，若设置初始密码，应强制用户在首次登录后修改初始密码。

c) 在修改密码前，应对用户身份进行重新验证。

d) 修改密码时应对原密码输入错误次数进行限制。

e) 修改密码时新密码不应与原密码相同。

f) 在密码重置时，应使用短信验证码、用户注册信息校核等方式，对用户身份进行校验。

增强要求：

a) 在进行修改密码或密码重置时，应采用两种或两种以上要素进行身份认证，如：数字证书、生物特征信息等。

b) 应采取有效措施提醒客户避免设置与常用软件、网站相同或相似的用户名和密码组合，并采取有效措施引导客户设置独立的支付密码。

5.2 逻辑安全

5.2.1 逻辑安全设计

基本要求：

a) 对于认证、校验等安全保证功能的流程设计应充分考虑其合理性，避免逻辑漏洞的出现，确

保认证流程无法被绕过。

b） 对于交易处理功能逻辑设计应充分考虑其合理性，避免逻辑漏洞的出现，保证资金交易安全。

c） 客户端代码实现应尽量避免调用存在安全漏洞的函数，避免敏感数据硬编码。

5.2.2 软件权限控制

基本要求：

客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。

5.2.3 风险控制

基本要求：

a） 应设计合理的登录风险控制策略，包括但不限于：

- 当用户闲置在线状态超出时限时，应设计合理的账户登录超时控制策略；
- 合理的多点登录策略，如：提示登录信息或退出先登录的账户等策略；
- 合理的长期未登录控制策略，当用户长时间未登录时，应综合考虑风险情况，增大认证强度。

b） 应设计合理的交易风险控制策略，包括但不限于：

- 针对不同的资金交易金额，应设计合理的身份认证策略；
- 针对不同的资金交易业务场景，应设计合理的策略，如：限额控制策略、时限控制策略等。

c） 客户端应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

5.2.4 回退处理

基本要求：

交易过程中如遇交易失败或在交易完成前用户进行撤销操作，应返回到交易前的有效状态。

5.2.5 异常处理

基本要求：

a） 客户端应用软件发生故障产生的异常信息，不应泄露用户的敏感数据。

b） 当交易出现异常时，客户端应用软件应向客户提示出错等信息，但不应泄露用户的敏感数据。

5.3 安全功能设计

5.3.1 组件安全

基本要求：

a） 客户端应用软件应避免使用存在已知漏洞的系统组件与第三方组件。

b） 客户端应用软件在使用第三方组件时，应避免第三方组件未经授权收集客户端应用软件信息和个人信息。

5.3.2 接口安全

基本要求：

a） 客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。

b） 客户端应用软件应对传入的 URI 进行校验与安全处理，防止客户端应用软件运行异常或操作

异常。

c) 当客户端应用软件需要与 TEE、SE 结合使用时，应避免使用存在已知漏洞的接口。

5.3.3 抗攻击能力

基本要求：

a) 客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。

b) 客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。

c) 客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

d) 客户端应用软件如使用安全输入控件，该控件应具备抵御一定程度攻击的能力。

增强要求：

客户端应用软件如使用安全输入控件，该控件应具备检测自身是否正在被调试的能力，并采取适当的风控措施，如：给予用户风险提示。

5.3.4 客户端应用软件环境检测

基本要求：

客户端应用软件在运行时应具备对运行环境的检查能力，检查的范围可包括：系统是否被未经授权获取管理员权限、程序运行环境是否可信（如：是否运行在模拟器或虚拟机中）等，并能向后台系统反馈设备信息等。

5.4 密码算法及密钥管理

5.4.1 密码算法

基本要求：

a) 客户端应用软件应使用密码算法对资金有关交易或重要业务操作进行保护。

b) 密码算法、密钥长度及密钥管理方式应符合国家密码主管部门的要求。

5.4.2 密钥管理

基本要求：

a) 密钥在传输过程中应使用密码算法对密钥进行保护。

b) 随机生成的密钥应具有一定的随机性与不可预测性。

c) 密钥应加密存储，并确保密钥储存位置和形式的安全。

5.5 数据安全

5.5.1 数据获取

5.5.1.1 数据防窃取

基本要求：

a) 客户端应用软件应保证内存中不应存在完整的银行卡密码和网络支付交易密码明文。

b) 客户端应用软件的临时文件中不应出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等。

c) 客户端应用软件程序应禁止在身份认证结束后存储支付敏感信息，防止支付敏感信息泄露。

d) 客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。

增强要求：

a） 应采取技术手段防止内存中加密的敏感数据被还原为明文。

b） 客户端应用软件应实现身份认证过程的防截屏、录屏，如：输入手势验证码、登录口令等。

5.5.1.2 数据防篡改

基本要求：

用户输入关键交易数据时，如：收款人信息、交易金额、订单号等，应采取防篡改机制保证数据不被移动终端的其他程序篡改。

5.5.1.3 数据有效性

基本要求：

客户端应用软件在数据获取时提供有效性校验功能，确保通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求。

5.5.2 数据访问控制

基本要求：

a） 应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。

b） 客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。

5.5.3 数据传输

5.5.3.1 通讯安全

基本要求：

a） 应在客户端应用软件与服务器之间建立安全的信息传输通道，协议版本应及时更新至安全稳定版本。

b） 应确保采用的安全协议不包含已知的公开漏洞。

c） 客户端应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。

5.5.3.2 数据保密性

基本要求：

a） 敏感数据（如：登录口令、支付敏感信息等）在客户端应用软件与本地其他应用软件间传输时，应采取加密等措施确保其保密性，若本地其他应用软件不能提供与金融客户端软件相应等级的加密接口，则应评估敏感数据调用的风险，并设计补救措施。

b） 敏感数据（如：登录口令、支付敏感信息等）在通过公共网络传输时，应采取加密等措施确保其保密性。

5.5.3.3 数据完整性

基本要求：

a） 关键的交易数据，如：收款人信息、交易金额、订单号等，在客户端应用软件与本地其他应用软件间传输时，应采取措施（如：数字签名、MAC 等）确保其完整性，若本地其他应用软件不能提供与金融客户端软件相应等级的数据完整性保护措施，则应评估关键数据传输的风险，并设计补救措施。

b) 关键的交易数据、个人身份信息，如：收款人信息、交易金额、订单号、身份证号码等，在通过公共网络传输时，应采取措施（如：数字签名、MAC 等）确保其完整性。

5.5.3.4 数据抗抵赖

基本要求：

通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。

5.5.3.5 数据防重放

基本要求：

通过客户端应用软件发起的身份认证或资金类交易报文，应能够防止重放攻击。

5.5.4 数据存储

5.5.4.1 个人金融信息存储

基本要求：

a) 客户端应用软件不应以任何形式存储用户的支付敏感信息与金融业务查询口令。

b) 在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量。

5.5.4.2 加密密钥存储

基本要求：

客户端应用软件应确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

5.5.5 数据展示

基本要求：

除交易对账、转账收款方确认等必须由用户确认的情况外，客户端应用软件在显示个人信息，如：银行账号、身份证号码、手机号码、姓名等时应屏蔽关键字段。

5.5.6 数据销毁

5.5.6.1 残余信息保护

基本要求：

a) 客户端应用软件应在敏感数据使用完毕后，对其立即进行清除。

b) 客户端应用软件进程被结束时，应清除非业务功能运行所必需留存的业务数据，保证客户信息的安全性。

c) 客户端应用软件卸载完成后，文件系统中不应残留任何个人金融信息。

增强要求：

客户端应用软件应确保无法通过技术手段恢复已清除的敏感数据。

5.5.6.2 页面返回保护

基本要求：

客户端应用软件应支持页面返回后自动清除银行卡密码、网络支付交易密码、登录口令等支付敏感信息的机制。

增强要求：

a） 客户端应用软件应对后台任务列表中的预览界面采取模糊或其他防护措施。

b） 当客户端应用软件从前台进入后台时，超过设定时限后应清除页面中已输入的敏感数据。

5.5.6.3 会话失效

基本要求：

客户端应用软件在安全退出登录时，应向服务器发送会话结束请求，使当前会话状态失效。

6 客户端应用软件管理要求

6.1 设计要求

基本要求：

a） 客户端应用软件设计应遵循安全、可靠、易用、可维护和可扩展等原则，制定用于指导客户端应用软件设计与开发的总体方案。

b） 客户端应用软件应提供易用、风格统一、体验良好的用户界面。

c） 客户端应用软件应遵循合法、正当、必要的原则，不收集与所提供服务无关的个人金融信息。

d） 客户端应用软件收集个人金融信息或用户授权等操作前，要以通俗易懂、简单明了的方式展示个人金融信息收集使用规则，并经个人金融信息主体自主选择同意。

e） 客户端应用软件不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反与用户的约定收集使用个人金融信息。

增强要求：

a） 客户端应用软件设计在遵循易用性原则的基础上，应采用人工智能技术，其中智能语音交互技术实例参见附录 B。

b） 客户端应用软件应提供访问、更正个人金融信息，以及授权撤销、账户注销等功能。

6.2 开发要求

基本要求：

a） 客户端应用软件开发过程中应遵守严格的开发流程、项目管理流程和编码安全规范，进行完整的测试，避免在请求、响应、存储、配置等功能中存在漏洞。

b） 客户端应用软件开发过程中应建立并维护开发文档。

c） 客户端应用软件开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明功能。

d） 客户端应用软件的每次重要更新、升级，都必须经过严格归档、源代码扫描、发布审核等步骤。

6.3 发布要求

基本要求：

a） 客户端应用软件应有规范的上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源和发布者，提供安全可靠的应用软件下载、发布、升级渠道。

b） 客户端应用软件应当删除调试或测试中存留的敏感数据。

c） 客户端应用软件安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其他软件。

d） 客户端应用软件有新版本时，不能未经用户允许自动安装新版本。

e) 若客户端应用软件支持动态模块更新，应使用加密信道与服务端通信传输更新模块或对更新模块进行签名校验；动态模块更新后不得影响用户使用，不得修改用户已有的安全配置。

6.4 维护要求

基本要求：

a) 应制定科学、合理的管理策略和执行制度，指导各类角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程。

b) 客户端应用软件应具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在安全隐患时，应及时进行修复更新。

c) 以 SDK 等形式对外提供金融交易类服务时，应记录 SDK 信息及引用本 SDK 的外部应用软件信息。

附 录 A
（资料性附录）
敏感数据

本标准中的敏感数据是指移动金融客户端应用软件在运行过程中通过用户输入、客户端自动获取或通过算法计算出的，需要客户端应用软件重点保护的信息。

在移动金融应用场景中，需要客户端应用软件重点保护的敏感数据通常包括支付敏感信息、个人身份信息、财产信息、账户信息、信用信息、金融交易信息等个人金融信息。客户端应用软件应在数据输入、使用、传输以及存储过程中，采用加密、完整性校验、屏蔽掩盖等技术措施，对敏感数据进行安全防护，保护其机密性、完整性及可用性。客户端应用软件需要重点保护的敏感数据包括但不限于以下内容：

a) 客户端应用软件采集与处理的支付敏感信息，包含但不限于：
   - 银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码。

b) 客户端应用软件采集与处理的除支付敏感信息外的用户鉴别（如：身份鉴别等）信息，包含但不限于：
   - 用于身份鉴别的个人生物特征模板或特征值等信息；
   - 账户（包括但不限于支付账号、网络支付业务系统中个人金融信息主体登录用户、证券账户、 保险账户）登录密码、交易密码，账户查询密码，以及用户鉴别（或辅助用户进行身份鉴别）相关的个人生物特征模板或特征值。

c) 客户端应用软件采集与处理的可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及金融消费者用于金融产品与服务的关键信息，包含但不限于：
   - 支付账号及其等效信息，如：支付账号、证件类识别标识与证件（身份证、护照等）信息、手机号码；
   - 账户（包括但不限于支付账号、网络支付业务系统中个人金融信息主体登录用户、证券账户、 保险账户）登录的用户名；
   - 用户鉴别辅助信息，如：动态口令、短信验证码、密码提示问题答案；
   - 直接反映个人金融信息主体金融状况的信息，如：个人财产信息（包括网络支付账号余额）、借贷信息等；
   - 其他能够识别出特定主体的信息，如：账单寄送地址等。

附 录 B
（资料性附录）
客户端应用软件应用智能语音交互技术

B.1 应用智能语音交互技术功能架构

应用智能语音交互技术功能架构参见图B.1。

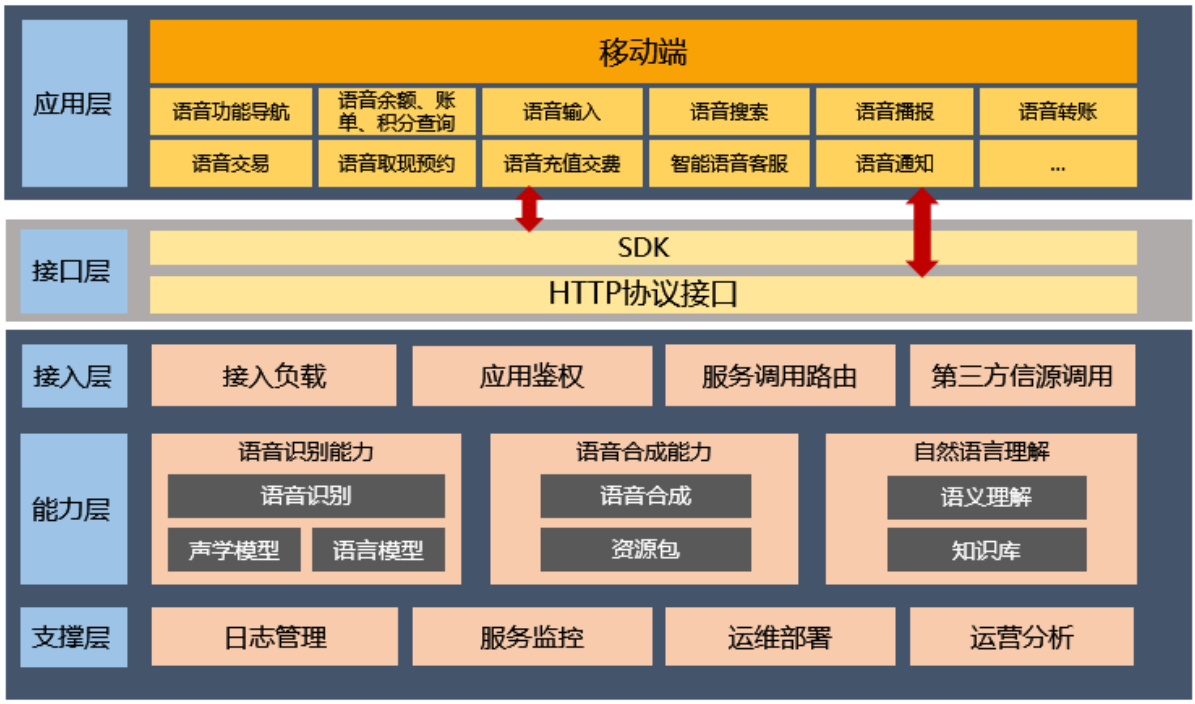

图 B.1 应用智能语音交互技术功能架构

应用层：支持客户端应用软件调用语音交互技术实用应用场景扩展和实现。
接口层：支持应用层通过标准接口调用语音交互技术。
接入层：支持接入负载、应用鉴权、服务调用路由、第三方信源调用。
能力层：支持语音识别、语音合成、自然语言理解等核心语音交互能力。
支撑层：支持对能力层的日志管理、服务监控、运维部署、运营分析功能。

部署方式：

智能语音平台采用本地化部署，以云服务的方式为客户端应用软件提供语音服务。

B.2 应用智能语音交互技术核心能力要求

基本要求：

客户端应用软件应用智能语音交互技术，可以是以下一种或多种组合：

a) 语音识别技术。
b) 语音合成技术。
c) 自然语言理解。

B.3 应用智能语音交互技术接口要求

基本要求：

a) 支持语音识别、语音合成、自然语言理解等能力的调用。
b) 支持客户端软件根据实际业务需求灵活调用接口组装能力。
c) 支持主流移动端操作系统调用标准接口。
d) 支持主流客户端开发语言调用标准接口。

B.4 应用智能语音交互技术安全要求

基本要求：

a) 只保存业务优化所必须的个人语音信息。
b) 只提取与提高语音应用效果相关的环境信息。
c) 交互数据及时保存并提供定期转存归档管理。
d) 支持安全传输协议，协议版本应及时更新至安全稳定版本，保证互联网上的传输安全。
e) 支持会话校验，为每一个应用提供唯一有效的身份校验。

参 考 文 献

[1] GB/T 25069—2010 信息安全技术 术语

[2] GB/T 35273—2017 信息安全技术 个人信息安全规范

[3] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

[4] JR/T 0156—2017 移动终端支付可信环境技术规范

[5] JR/T 0164—2018 移动金融基于声纹识别的安全应用技术规范

[6] 中国人民银行. 中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知（银发〔2011〕17号），2011-1-21

[7] 中国人民银行. 中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016-6-13

[8] 中国人民银行. 中国人民银行关于印发《中国人民银行金融消费者权益保护实施办法》的通知（银发〔2016〕314号），2016-12-14

[9] 中国人民银行. 中国人民银行办公厅关于加强条码支付安全管理的通知（银办发〔2017〕242号），2017-12-22