ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0109.5-2015

智能电视支付应用规范
第5部分：终端规范

Smart TV payment application specification—
Part 5: Terminal specification

2015-11 -30 发布　　2015-11 -30 实施

中国人民银行　发布

目　次

前　言

JR/T 0109《智能电视支付应用规范》分为五个部分：

——第1部分：交易处理说明；

——第2部分：报文接口规范；

——第3部分：数据安全传输控制规范；

——第4部分：通信接口规范；

——第5部分：终端规范。

本部分为JR/T 0109的第5部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分起草单位：中国人民银行、中国邮政储蓄银行、中国银联股份有限公司、百视通信息技术有限公司、中国金融电子化公司、中钞海思信息技术（北京）有限公司、江苏省广播电视信息网络股份有限公司。

本部分主要起草人：吴潇、张雯华、刘冰、朱婧、徐燕军、李伟、李洁、谭颖、金正博、郭延斌、周砺锋、海涛、徐蓉、倪德中、张立杰、李曙光、魏猛、关景火、胡海涛、王永军。

智能电视支付应用规范

第5部分：终端规范

1 范围

JR/T 0109的本部分规定了智能电视支付应用终端的硬件要求以及客户端软件的管理及安全要求。

本部分适用于从事智能电视支付业务相关产品的设计、制造、管理、发行、受理以及相关应用系统的研制、开发、集成和维护的相关部门（单位）。

2 规范性引用文件

下列文件对于本部分的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本部分。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本部分。

GB 15629.11-2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB/T 16649 识别卡 集成电路卡（所有部分）

JR/T 0025-2013 中国金融集成电路(IC)卡规范（所有部分）

JR/T 0089-2012 中国金融移动支付 安全单元（所有部分）

IEEE 802.3-1998 Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

3 术语和定义

下列术语和定义适用于本文件。

3.1

发卡/账户机构 card/account issuer

通过发行卡或提供账户并在支付过程中为客户提供支付款项服务的机构。

3.2

SD卡 secure digital memory card

一种基于半导体快闪记忆器的存储卡。

3.3

智能SD卡 smart SD card

集成了安全芯片并支持逻辑运算功能的SD卡。

3.4

智能电视支付应用终端 smart TV payment application terminal

具有银行卡支付及视频播放等功能的多媒体终端，主要包括数字电视机顶盒，IPTV，移动电视等。

3.5

交易敏感数据（信息） transaction sensitive data (information)

影响智能电视支付安全的密码、资金转出账户标识、卡有效期、CVN2等交易敏感数据信息，密码包括但不限于支付密码、查询密码等。

3.6

交易关键数据（信息） transaction key data (information)

商户编号、终端标识码、订单号、交易日期时间、交易金额、交易币种等交易关键数据信息。

3.7

智能电视支付应用客户端 smart TV payment application client

智能电视进行交易的核心软件，预置在智能电视支付终端中，与用户交互，获取支付相关的敏感数据信息，包括但不限于可执行文件、控件、静态链接库、动态链接库等。

4 支付应用终端硬件要求

智能电视支付应用终端作为支付应用客户端的运行平台，为支付应用客户端软件的运行提供了硬件支持，其硬件应符合以下基本要求：

——支付应用客户端应能连接到网络，终端硬件平台宜采用下列硬件方式之一：

a) 以太网卡，符合IEEE 802.3-1998的规定；

b) 无线接入，符合GB 15629.11-2003的要求；

c) 3G网络接入，支持国家相关3G网络规范要求。

——终端设备应具备USB接口或者内置卡座，支持对金融IC卡的操作，具体应满足下列要求：

a) USB接口，符合USB 2.0或者更高标准；1个（必选），2个（可选），最大电流500mA，工作电压5V，支持外接金融IC卡读卡器或者金融USBKey设备；

b) 内置金融IC卡读卡器，可选配置，读卡器满足GB/T 16649规范要求，可以对符合JR/T 0025-2013要求的金融IC卡进行操作；

c) 内置micro SD卡读卡器，可选配置。读卡器应用层接口应遵循JR/T 0025-2013、JR/T 0089-2012要求。可以对集成了符合JR/T 0025-2013、JR/T 0089-2012要求金融IC卡的micro SD卡进行操作。

5 支付应用客户端软件要求

5.1 基本要求

智能电视业务运营商应保证智能电视支付应用客户端软件下载和运行时的安全。

5.2 认证评测

支付应用客户端软件由智能电视业务运营商主导进行开发，开发完成后，应由相关机构进行安全认证，确认符合安全规范、业务要求后，才可发布到不同终端中投入使用。认证机构应对软件进行签名处理，确保软件发布过程和执行过程中不被篡改。

支付应用客户端软件由支付核心模块、管理用户界面等非核心模块组成。支付核心模块获取用户账号、支付密码等交易敏感数据，使用非对称密码算法进行加密处理，同时使用对称密码算法针对商户编号、终端标识码等交易关键数据计算报文鉴别码。

对于管理用户界面等非核心模块，不应非法保留截获交易信息，开发商或运营商应将源码提交权威的检测机构进行安全测评。

5.3 内置部署管理

支付应用客户端软件的植入和升级应由智能电视业务运营商负责。

根据不同的安全等级，支付应用客户端软件不同模块和数据文件按照下列原则进行分区保存：

——数字证书区域。该区域用于保存终端认证机构的数字证书；对于拥有安全存储区的芯片，直接使用芯片内部的安全存储区；应确保数字证书不被非法篡改和删除。

——执行文件保存区域。该区域用于保存支付应用客户端软件，普通程序应无法修改这个区域。

——安全数据存储区域。该区域用于保存支付应用客户端运行过程中生成的临时数据文件，该文件应被加密保存，普通程序应无法访问这个区域。

5.4 支付应用客户端的升级管理

智能电视业务运营商对通过终端认证机构认证的软件包进行加密签名，形成升级软件包供客户端升级使用。智能电视终端的加载模块应具有后台版本的检测功能，发现有更新的版本后，可实现自动升级。升级时加载程序应对升级包进行签名认证。加载程序有写保护，防止加载模块被破坏。智能电视终端应能拒绝非法代码下载，防止恶意写入。

提供在线升级服务的服务器入口必须是唯一的，由智能电视业务运营商统一配置，支付应用客户端软件只能连入该库获取在线升级服务。

6 支付应用客户端软件用户界面要求

6.1 界面基本要求

支付应用客户端软件用户界面基本要求如下：

——应公布智能电视支付服务联系方式；

——全部交易类型的各个用户界面以及单个交易内部的各个步骤，其界面风格应保持一致；

——应包含确定按钮和取消按钮，光标默认在取消按钮；用户按确定按钮后，进入到具体支付阶段，用户按取消按钮回到订单支付前状态；

——用户输入应有删除按钮，用于更正输入信息；

——如页面提供“回退”功能，不应将输入的敏感信息重新显示在页面上；

——交易前应提示客户确认交易要素，当客户确认交易信息正确后，方可进一步支付。交易要求应尽可能详尽，包括但不限于交易账户、交易金额、交易时间、商户信息等；

——支付应用客户端同后台系统交互过程中，应提示用户交易处理状态；

——支付应用客户端同后台系统交互过程中，如果时间超过预先设定的时间，应提示用户超时，并给出交易成功与否的信息；

——交易完成后，应提示结果信息；

——当交易出现异常时，应给出相应的信息提示客户或商户；

——交易界面支持弹出式对话框；

——对于支持接触式IC卡交易的终端，用户选择使用IC卡进行交易时，应提示用户插入IC卡，交易完毕，应提示用户拔出IC卡；

——交易费用已知的，应显示实际金额，交易费用不能确定的，应提示用户根据相关发卡/账户机构规定执行；

——应尽量减少客户输入非数字字符，多以点选的方式为客户提供功能。

6.2 个人账户密码输入界面要求

个人账户密码输入界面应采用软件虚拟的软键盘技术，在电视屏幕用户界面上显示虚拟密码输入软键盘，通过电视遥控器的上下左右键和“确定”键输入数字字符。同时，智能电视支付应用客户端采用“*”号显示输入的密码具体数字。如当前交易不需输入密码，用户可以直接按“确定”键。

虚拟密码输入软键盘的具体要求如下：

——整体框架分为三个区域：密码回显框、密码数字选择键盘、“删除”和“关闭”功能按钮区；

——密码数字选择键盘应包含0-9这10个阿拉伯数字，且每次开启虚拟软键盘时数字随机排列分布；

——密码回显框需要用“*”显示输入的密码具体数字；

——删除按钮用于用户删除当前光标前的数字；

——关闭按钮用于关闭密码键盘；

——密码虚拟键盘不响应除光标移动、确认等其他按键。

6.3 交易失败提示界面要求

支付交易失败或者交易超时时，智能电视支付应用客户端应在界面显示便于用户理解的明确的提示信息。用户界面有“关闭”按钮用于关闭支付界面，回退到先前商品信息确认界面。

要求能至少显示下列几种错误：

——通讯故障

当支付应用客户端和智能电视集成播控平台之间，智能电视集成播控平台和智能电视支付及账号管理系统之间的通讯出现问题，应显示通讯故障；

——密码错

当支付密码错的时候，应提醒用户密码错及剩余可尝试输入的次数，并能引导用户再一次尝试，直至达到系统规定的输入次数；

——用户余额不足

当用户账户余额不足以支付实际金额时，应显示余额不足错误。

7 支付应用客户端安全要求

7.1 客户端数据输入安全要求

通过客户端输入银行卡卡号、银行卡个人账户密码、CVN2、卡有效期等银行卡敏感信息时，应遵循以下原则：

——对于遥控器发送模块与智能电视接收模块之间的数据传输，应采用国际通行的红外传输通讯协议，对信道进行加密，保证数据传输安全；

——支付应用客户端用户界面必须是经安全检测认证的版本，与智能电视其他客户端和集成播控平台无关，且不能被其他系统截取；

——通过支付应用客户端输入银行卡个人账户密码、CVN2、卡有效期等银行卡敏感信息时，应采用图形化的密码软键盘，键盘输入数字随机分布或混序排列，以防止红外传输过程被侦听。输入银行卡号、身份证号码和手机号码等信息时可采用遥控器键盘直接输入，应比照图形化的密码软键盘模式执行。

7.2 客户端程序安全要求

客户端程序应满足如下安全要求：

——应在上线前进行严格的代码安全测试，如果外包给第三方机构开发的，应要求进行代码安全测试；

——支付应用客户端是一个独立的软件，只能通过接口和其他模块进行通讯；

——支付应用客户端在启动时，应能自动进行自身安全性检测；

——支付应用客户端不应存储敏感信息（即使已经加密），包括PIN、卡片验证码、有效期等；

——支付应用客户端应能防范自身被恶意程序修改；

——支付应用客户端应防范恶意程序获取、篡改或窃听敏感信息；

——支付应用客户端应确保不存在内存泄漏。

7.3 客户端绑定安全

支付应用客户端应与智能电视支付应用终端以下硬件信息进行绑定：

——网卡MAC；

——CPU ID；

——终端号，即智能电视运营商分配的唯一硬件ID号，可包含运营商ID、生产厂家ID、生产序列号等信息。

客户端应与用户信息（即终端用户号）进行绑定。终端用户号是智能电视运营商分配的唯一的用户ID号。

客户端宜与终端认证机构的数字证书进行绑定。