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 0109.3-2015

智能电视支付应用规范
第3部分：数据安全传输控制规范

Smart TV payment application specification—
Part 3: Data secure transmission control 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3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3部分：数据安全传输控制规范

1 范围

JR/T 0109的本部分规定了智能电视支付交易网络中安全传输数据信息应达到的要求，包括数据传输安全要求、密钥管理方法和加密方法。

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。

GM/T 0003-2012 SM2椭圆曲线公钥密码算法（所有部分）

GM/T 0002-2012 SM4分组密码算法

3 术语和定义

下列术语和定义适用于本文件。

3.1

硬件加密机 Hardware and Security Machine (HSM)

对传输的数据进行加密的外围硬件设备，用于 PIN 的加密和解密、验证报文和文件来源的正确性以及存储密钥。

3.2

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。

3.3

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。

3.4

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。请见GM/T 0003-2012规范。

3.5

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。请见GM/T 0002-2012规范。

4 符号和缩略语

下列符号和缩略语适用于本部分。

3DES	三重数据加密标准（Triple Data Encryption Standard）
AES	高级加密标准（Advanced Encryption Standard）
CBC	密码分组链接（Cipher-block chaining）
DES	数据加密标准（Data Encryption Standard）
RSA	Rivest、Sharmir和Adleman提出的一种非对称密码算法
ECC	椭圆曲线密码（Elliptic Curve Cryptography）
CVN2	安全码（Card Verification Number）

5 密钥管理与控制

5.1 安全管理的基本要求

5.1.1 概述

整个智能电视支付交易网络的数据安全保密，不仅仅需要技术上的支持，更需要在业务上制定和贯彻严格的密钥管理制度。基本要求如下：

——应采用安全、可靠、成熟的加密算法；

——密钥的生成、存贮、销毁和交易信息的加密 / 解密应在硬件加密设备中进行；

——应遵循金融业有关数据安全保密的国家标准和国际标准；

——应加强对操作人员的管理要求。

5.1.2 数据传输安全控制的基本要求

智能电视支付体系应技术上保证账户信息、持卡人密码、卡有效期、CVN2、交易金额、交易日期时间等在传输过程中的安全性，应能防止其在传输过程中被破解、篡改或仿造。数据传输安全控制要求包括以下几个方面：

——密钥管理机制：在技术上应实施严格和可靠的密钥分发过程；

——个人标识码（PIN）的加密及转换机制：不允许 PIN 以明文的形式在通信线路上传输，同时任何情况下均不应储存 PIN（即使已经加密）；

——应保证交易报文的完整性和报文来源的真实有效性；

——点对点的数据加解密网络机制，防止交易数据被破解、篡改和仿造。

5.1.3 数据加密传输环境的基本要求

交易敏感数据应由智能电视支付应用终端加密处理后方可进入智能电视支付及账户管理系统。

支付密码等交易敏感数据应达到端到端加密。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应达到端到端防止篡改。

5.2 密钥管理的安全要求

5.2.1 对称密钥管理要求

对称密钥可用于对智能电视支付应用终端和智能电视支付及账户管理系统之间交易报文来源的真实有效性进行检验。

对称密钥应由硬件加密机的随机发生器产生。密钥产生后，硬件加密机应检查密钥的有效性。弱密钥和半弱密钥应被剔除。

对称密钥应保存在硬件加密机内，如果出现在硬件加密机外，则应以密文方式出现。

当新密钥产生后，生命期结束的旧密钥应从数据库和内存中清除，防止被替换使用；同时所有可能重新构造此密钥的信息也应清除。新密钥成功启用和旧密钥自动销毁的记录将被更新。

对称密码算法宜使用AES 128位及以上密钥长度算法、3DES 128位及以上密钥长度算法，可选择使用SM4算法，不应使用DES算法。

5.2.2 非对称密钥管理要求

非对称密钥（公私钥对）可用于对用户输入的交易敏感信息进行加解密。

公私钥对由硬件加密机生成，为保证密钥安全建议生成不同索引、不同使用年限和不同长度的多把公私钥对。为保证密钥安全，建议至少安装三把不同索引、长度和时间周期的公钥。

私钥应存储在智能电视支付及账户管理系统的硬件加密机内。公钥应存储在智能电视支付应用客户端中，该存储区内的数据不应被外界偶然或蓄意的删除、修改、伪造、乱续、重放、插入等行为造成破坏和丢失。

当旧密钥对被撤销或失效时，应通过重复适当的密钥生成、传输、分发和加载程序来实现密钥更换。在更换密钥的情况下，密钥对的公钥与私钥均应进行更换。被更换的密钥不应再激活使用，并应将私钥进行安全销毁。

非对称密码算法宜使用RSA 2048位及以上公钥长度算法，可选择使用ECC、SM2算法，不应使用RSA 1024位及以下公钥长度的算法。

6 数据的安全保护要求

6.1 交易敏感数据的加密要求

智能电视支付应用客户端应对持卡人输入的交易敏感数据进行非对称密钥加密，确保其数据信息的保密性。

智能电视支付客户端应提取持卡人输入的交易敏感数据，按照与智能电视支付及账户管理系统约定的公钥加密算法，使用保存在客户端的指定密钥索引的公钥进行加密；智能电视支付及账户管理系统收到交易报文后，应提取交易敏感数据密文传入硬件加密机进行相关密文处理。

6.2 交易关键数据的安全保护要求

智能电视支付系统应采用相关机制确保商户编号、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的完整性。