ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0025.1—2018

中国金融集成电路（IC）卡规范 第1部分：总则

China financial integrated circuit card specifications—
Part 1: General principles

2018-11-28 发布　　2018-11-28 实施

中国人民银行　　发布

目　　次

前　言

JR/T 0025—2018《中国金融集成电路（IC）卡规范》分为14部分：

——第1部分：总则；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第10部分：借记/贷记应用个人化指南；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第18部分：基于安全芯片的线上支付技术规范。

本部分为JR/T 0025—2018的第1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、中国金融电子化公司、中国银联股份有限公司、中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国邮政储蓄银行、银行卡检测中心、中金金融认证中心有限公司、北京中金国盛认证有限公司。

本部分主要起草人：李伟、李兴锋、宋汉石、渠韶光、杨倩、聂丽琴、邵阔义、周玥、张宏基、程胜、黄本涛、汤沁莹、李春欢、张永峰、洪隽、胡吉晶、吴潇、魏猛、雷斌、邓少峰、林发全、陈文博、张萌、吴雪艳、谭培强、郑元龙、尚可、刘文其、章盼。

引　言

为满足社会公众对安全、便捷、多元化支付工具的创新需求，适应“互联网+”时代下银行卡应用可持续发展的需要，加强个人信息保护和资金安全防范能力，体现金融IC卡的层次性、规范性和可扩展性特点，特制定本标准。

为促进基于金融IC卡及安全芯片的线上支付业务的健康发展，JR/T 0025—2018将线上线下支付应用进行了统一整合，规定了基于安全芯片及借记/贷记应用的线上支付应用流程及安全功能要求，同时按照“简化流程、便捷体验”的原则对近场支付非接受理流程进行了优化。

为满足新型支付产品对通讯技术提出的多元化需求，JR/T 0025—2018明确了13.56MHz为金融IC卡非接近场通讯方式的一种具体实现，对未来多种新兴通讯技术向后兼容。

为强化金融IC卡支付业务的整体安全性，JR/T 0025—2018对借记/贷记应用的安全功能进行了优化加固，将SM算法引入通用安全功能、机制及算法要求，提高金融IC卡线上线下渠道整体风险防控能力，进一步加强和保障持卡人隐私信息安全，推动金融IC卡支付应用、设备及系统全业务链的安全发展。

中国金融集成电路（IC）卡规范
第1部分：总则

1 范围

本部分规定了JR/T 0025—2018的整体技术架构、基本特点以及整套规范中各个部分之间的关系和主要内容。本部分为其余各部分的使用提供了指南。

本部分适用于金融集成电路（IC）卡及终端制造商、支付系统或应用开发商及检测认证机构等。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 32918—2016 信息安全技术 SM2椭圆曲线公钥密码算法

JR/T 0025—2018（所有部分） 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融IC卡 financial integrated circuit(s) card

符合JR/T 0025—2018要求，并由商业银行发行的集成电路（IC）卡。

3.2

集成电路卡（IC卡） integrated circuit(s) card (ICC)

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.3

集成电路（IC） integrated circuit (IC)

用于执行处理和/或存储功能的电子器件。

3.4

终端 terminal

在交易点安装、用于与IC卡配合共同完成金融交易的设备。应包括接口设备，也可包括其他的部件和接口（如与主机的通讯）。

3.5

金融交易 financial transaction

由于持卡者和商户之间的商品或服务交换行为而在持卡者、发卡机构、商户和收单行之间产生的信息交换、资金清算和结算行为。

3.6

接口设备 interface device

终端上插入IC卡的部分，包括其中的机械和电气部分。

3.7

命令 command

终端向IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.8

响应 response

IC卡处理完成收到的命令报文后，返回给终端的报文。

3.9

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.10

脚本 script

发卡行向终端发送的命令或命令序列，目的是向IC卡连续输入命令。

3.11

密码算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.12

非对称密码技术 asymmetric cryptographic technique

采用两种相关变换的密码技术：公开变换（由公钥定义）和私有变换（由私钥定义）。这两种变换具有在获得公开变换的情况下无法通过计算得出私有变换的特性。

3.13

对称密码技术 symmetric cryptographic technique

发送方和接收方使用相同保密密钥进行数据变换的密码技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.14

密钥 key

控制加密转换操作的符号序列。

3.15

公钥 public key

在一个实体使用的非对称密钥对中可以公开的密钥。

3.16

私钥 private key

一个实体的非对称密钥对中含有的供实体自身使用的密钥。

3.17

密码杂凑算法 hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

——为一个给定的输出找出能映射到该输出的一个输入在计算上是困难的；

——为一个给定的输入找出能映射到同一个输出的另一个输入在计算上是困难的；

——要发现不同的输入映射到同一输出在计算上是困难的。

3.18

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。

3.19

SM3算法 SM3 algorithm

一种密码杂凑算法，其输出为256比特。

3.20

SM4算法 SM4 algorithm

一种分组密码算法，其分组长度和密钥长度均为128比特。

4 缩略语

下列缩略语适用于本文件。

DGI——数据分组标识符（Data Grouping Identifier）

IC——集成电路（Integrated Circuit）

qPBOC——快速借记/贷记应用（quick PBOC）

5 金融IC卡标准结构

5.1 概述

金融IC卡标准整体架构涉及通讯、安全和应用三个层面。包括：

——功能应用层：对借记/贷记应用卡片和终端之间的处理技术要求进行描述，包括交易流程、指令集、数据元等，全面覆盖线上线下支付应用方式；

——安全管理层：对借记/贷记应用的安全功能要求进行描述，包括安全机制、加密算法、密钥管

理等，在实现安全功能以及实现金融交易的过程中支持SM系列算法，包括但不限于GB/T 32918—2016规定的SM2算法、GB/T 32905—2016规定的SM3算法、GB/T 32907—2016规定的SM4算法；

——通讯抽象层：对通讯层信息交互模式、握手方式、通讯传输方式及链路方式等进行统一要求，支持13.56MHz近场通讯协议，同时为将来其他通讯技术的扩展预留支持空间。

本规范各部分之间的关系结构如图1所示。

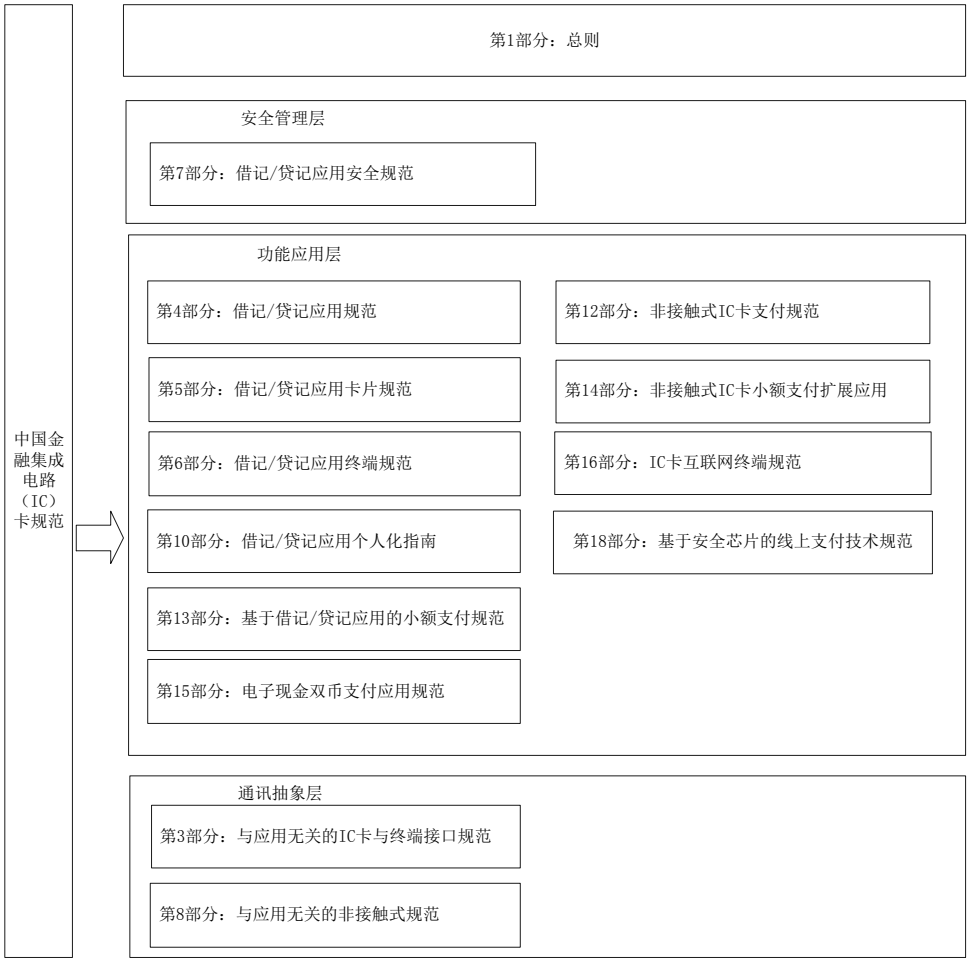

图1　规范结构图

5.2　金融IC卡标准组成

5.2.1　总则

第1部分《总则》：该部分描述了规范整体技术架构、基本特点以及整套规范中各个部分之间的关系和主要内容。

5.2.2　安全管理层

本层包括：

第7部分《借记/贷记应用安全规范》：该部分描述了借记/贷记应用安全功能方面的要求以及为实现这些安全功能所涉及的安全机制和获准使用的加密算法，包括：IC卡脱机数据认证方法、IC卡和发卡行之间的通讯安全、以及相关的对称及非对称密钥的管理。此外，还包括为实现这些安全功能所涉及的安全机制和获准使用的加密算法的规范。

5.2.3 功能应用层

本层包括：

——第 4 部分《借记/贷记应用规范》：该部分主要描述了借记/贷记应用卡片和终端之间处理的技术概要，提出了对基于 IC 卡借记/贷记项目的最低要求；

——第 5 部分《借记/贷记应用卡片规范》：该部分从卡片的角度描述了借记/贷记交易流程，包括卡片内部的处理细节、卡片所使用的数据元、卡片所支持的指令集等；

——第 6 部分《借记/贷记应用终端规范》：该部分从终端的角度描述了借记/贷记交易流程，包括终端的硬件需求、终端内部的处理细节、终端所使用的数据元、终端所支持的指令集等；

——第 10 部分《借记/贷记应用个人化指南》：该部分描述了 IC 卡借记/贷记应用特有的个人化指令、特有的数据分组标识（DGI）的定义及个人化时有关安全方面的规定；

——第 12 部分《非接触式 IC 卡支付规范》：该部分描述了非接触式 IC 卡应用，在快速借记/贷记非接触式支付应用（qPBOC）方面制定相关要求和规定；

——第 13 部分《基于借记/贷记应用的小额支付规范》：该部分描述了关于如何在借记/贷记卡上实现小额支付功能（即电子现金）的相关信息，并提供了电子现金的功能概述，包括卡片应用程序、终端功能与发卡行系统的示例等，发卡行后台的账户处理不在本部分范围之内；

——第 14 部分《非接触式 IC 卡小额支付扩展应用》：该部分对基于非接触式 IC 卡小额支付的扩展应用做出了相关要求和规定，主要应用于分段扣费、脱机预授权、单次扣款优惠等特定的小额支付场景；

——第 15 部分《电子现金双币支付应用规范》：该部分描述了关于如何在 PBOC 借记/贷记卡上实现电子现金双币支付功能（以下简称双币电子现金）的相关信息。此外还提供了双币电子现金支付中各个组成部分的不同于单币电子现金功能的概述，包括卡应用程序、终端功能等；

——第 16 部分《IC 卡互联网终端规范》：该部分描述了 IC 卡互联网终端在硬件需求、接口协议、命令集、个人化以及安全体系方面的相关要求和规定；

——第 18 部分《基于安全芯片的线上支付技术规范》：该部分规定了个人移动智能终端如何基于借记/贷记应用和安全芯片，通过移动互联网，采取后台账户限额控制和线上支付密码等持卡人身份认证保护措施，实现安全的个人线上支付，仅适用于个人支付。

5.2.4 通讯抽象层

本层包括：

——第 3 部分《与应用无关的 IC 卡与终端接口规范》：该部分规定了与应用无关的 IC 卡与终端接口方面的内容，包括卡片的机电接口、卡片操作过程、字符的物理传输、复位应答、传输协议、文件、命令及应用选择机制；

——第 8 部分《与应用无关的非接触式规范》：该部分描述了物理特性、射频功率和信号接口、初始化和防冲突、传输协议以及数据元和命令集等。