



中华人民共和国城镇建设行业标准

CJ/T 304—2017
代替 CJ/T 304—2008

建设事业智能卡操作系统技术要求

Technical requirement for chip operating system of
smart card in construction cause

2017-09-30 发布

2018-05-01 实施

中华人民共和国住房和城乡建设部 发布

目 次

前言 I

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语和符号 2

5 文件和命令 4

6 应用选择..... 23

7 安全机制及安全要求..... 26

8 电子存折/电子钱包应用 26

附录 A（规范性附录） 算法标识文件 ADEE 说明 93

附录 B（规范性附录） 数据元解释 94

附录 C（规范性附录） ED/EP 应用的密钥关系 96

附录 D（资料性附录） 应用密钥说明 98

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 CJ/T 304—2008《建设事业 CPU 卡操作系统技术要求》，与 CJ/T 304—2008 相比较，主要技术变化包括：

- 删除机电特性、逻辑接口与传输协议(2008 年版中第 5 章)；
- 删除密钥的推导方法和过程密钥的产生方法等相关内容(2008 年版中附录 C、E、F)；
- 增加记录格式说明(见 6.4)；
- 增加状态命令表(见 8.3.1)；
- 完善了相关指令的参数定义。

本标准做了下列编辑性修改：

- 修改了标准名称。

本标准由住房和城乡建设部标准定额研究所提出。

本标准由住房和城乡建设部信息技术应用标准化技术委员会归口。

本标准主编单位：中外建设信息有限责任公司。

本标准参编单位：住房和城乡建设部 IC 卡应用服务中心、北京亿速码数据处理有限责任公司、深圳市华旭科技开发有限公司、大唐微电子有限公司、武汉天喻信息产业股份有限公司、上海华虹集成电路有限责任公司、东信和平科技股份有限公司、捷德(中国)信息科技有限公司、上海复旦微电子集团股份有限公司、英飞凌科技(中国)有限公司、北京中电华大电子设计有限责任公司、上海雅斯拓智能卡技术有限公司、金邦达有限公司、北京中科软件有限公司、国民技术股份有限公司、广东楚天龙智能卡有限公司、河北一卡通电子支付服务有限公司、上海公共交通卡股份有限公司、郑州城市一卡通有限责任公司、南通公共交通总公司、青岛市琴岛通卡股份有限公司、深圳欧贝特卡系统科技有限公司。

本标准主要起草人：张永刚、尚治宇、樊静静、殷骏、张昕、王猛、张志红、李玉华、吴思凯、黄小鹏、丁晓明、段永刚、黄显明、刘觅、常小争、徐木平、刘春晓、柳建勇、刘典清、霍立民、胡振清、刘广乐、陆流、李妍、张鲲鹏。

本标准所代替标准的历次版本发布情况为：

- CJ/T 304—2008。

建设事业智能卡操作系统技术要求

1 范围

本标准规定了建设事业智能卡文件和命令、应用选择、安全机制及安全要求、电子存折/电子钱包应用和相应的定义符号等。

本标准适用于建设事业智能卡操作系统的设计、管理以及应用。

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。

CJ/T 166 建设事业集成电路(IC)卡应用技术

JR/T 0025 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

智能卡 smart card

一种具有微处理器芯片的 IC 卡,本文件中提到的 IC 卡特指智能卡。

3.2

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。

3.3

响应 response

IC 卡处理完终端收到的命令报文后,返回给终端的报文。

3.4

电子存折 electronic deposit

一种为持卡人进行消费、取现等交易而设计的使用个人密码(PIN)保护的金融 IC 卡应用。

注:它支持圈存、圈提、消费、取现等交易。

3.5

电子钱包 electronic purse

一种为方便持卡人小额消费而设计的金融 IC 卡应用。

注:它支持圈存、消费等交易。除圈存交易外,使用电子钱包进行的其他交易均无需提交个人密码(PIN)。

3.6

哈希函数 hash function

将位串映射为定长位串的函数。

3.7

报文 message

由终端向卡或卡向终端发出的,不含传输控制字符的字节串。