



中华人民共和国城镇建设行业标准

CJ/T 166—2006
代替 CJ/T 166—2002

建设事业集成电路(IC)卡应用技术

Integrated circuit card application technology of construction cause

2006-06-26 发布

2006-11-01 实施

中华人民共和国建设部 发 布

目 次

前言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语和符号	5
5 卡片技术要求	6
5.1 接触式 IC 卡	6
5.2 非接触式 IC 卡	6
5.3 双界面 IC 卡	6
5.4 CPU 卡的数据元和文件结构	6
5.5 IC 卡应用文件结构	10
5.6 CPU 卡的命令	30
5.7 PSAM 卡专用指令	35
5.8 SAM 卡通用指令说明	37
6 消费类及服务类 IC 卡终端技术要求	41
6.1 基本性能要求	41
6.2 IC 卡终端的一般要求	41
6.3 IC 卡终端的多应用要求	41
6.4 IC 卡终端的功能要求	41
6.5 IC 卡终端的数据安全要求	42
6.6 黑名单管理	43
6.7 IC 卡终端交易流程	44
6.8 IC 卡终端安全要求	48
7 表具类 IC 卡终端技术要求	50
7.1 表具类 IC 卡终端的定义和分类	50
7.2 表具类 IC 卡终端的基本性能要求	50
7.3 表具类 IC 卡终端的功能要求	51
7.4 表具类 IC 卡终端的数据安全要求	53
7.5 表具类 IC 卡终端交易流程	53
7.6 安全认证流程	57
8 密钥系统和安全技术要求	57
8.1 密钥系统	57
8.2 密钥管理的安全要求	57
8.3 安全存取模块	58
8.4 安全加密设备的安全要求	59
9 安全机制及安全要求	59
9.1 基本安全要求	59
9.2 密钥和个人密码的存放	60

9.3 安全报文传送	60
10 应用系统要求	64
10.1 应用系统总体架构	64
10.2 发卡系统技术要求	65
10.3 中央清算系统技术要求	65
10.4 数据采集技术要求	66
10.5 互联互通基本要求	67
10.6 应用系统安全要求	67
11 卡应用系统验收要求	68
11.1 验收基本流程	68
11.2 专用 IC 卡产品验收要求	69

图表索引

图 1 CPU 卡的文件结构(详细)	8
图 2 接触式、非接触式 CPU 卡应用文件结构	22
图 3 表具类 CPU 卡应用文件结构	25
图 4 非接触式逻辑加密卡与消费终端的交易流程	45
图 5 CPU 卡与消费终端的交易流程图	47
图 6 CPU 卡消费的详细交易流程图	48
图 7 CPU 卡消费交易安全认证流程	49
图 8 非接触式逻辑加密卡消费交易安全认证流程	49
图 9 CPU 卡充值交易安全认证流程	50
图 10 非接触式逻辑加密卡充值交易安全认证流程	50
图 11 逻辑加密卡表具交易流程	55
图 12 CPU 卡表具交易流程	56
图 13 表具类终端消费安全认证流程图	57
图 14 单长度 DEA 密钥的 MAC 算法	61
图 15 双长度 DEA Key 的 MAC 算法	61
图 16 单长度 DEA 密钥的数据加密	62
图 17 使用双长度 DEA 密钥的数据加密	63
图 18 使用单长度 DEA 密钥的数据解密	63
图 19 使用双长度 DEA 密钥的数据解密	64
图 20 IC 卡应用系统总体架构	65
表 1 CPU 卡电子存折/电子钱包应用的基本数据文件	9
表 2 CPU 卡电子存折/电子钱包应用的持卡人基本数据文件	9
表 3 CPU 卡电子存折/电子钱包应用的交易明细文件	9
表 4 消费类逻辑加密卡应用文件结构	10
表 5 消费类逻辑加密卡目录区结构	11
表 6 消费类逻辑加密卡分区编码	11
表 7 消费类逻辑加密卡发行区结构	12
表 8 消费类逻辑加密卡卡号、认证码数据结构	12
表 9 消费类逻辑加密卡应用代码	13

表 10	消费类逻辑加密卡卡类别编码表	13
表 11	消费类逻辑加密卡的发行/有效/启用日期数据结构	13
表 12	消费类逻辑加密卡启用标志	14
表 13	消费类逻辑加密卡充值记录数据结构	14
表 14	消费类逻辑加密卡钱包文件数据结构	15
表 15	消费类逻辑加密卡交易记录数据结构	15
表 16	消费类逻辑加密卡交易类型编码	16
表 17	消费类逻辑加密卡交易记录区数据定义	16
表 18	消费类逻辑加密卡公共信息区数据结构	17
表 19	消费类逻辑加密卡交易过程标志编码表	17
表 20	消费类逻辑加密卡公共信息区数据定义	17
表 21	表具类逻辑加密卡分区结构	18
表 22	消费类 CPU 用户卡文件详细信息	22
表 23	消费类 CPU 用户卡 MF 的 KEY 文件内容	22
表 24	消费类 CPU 用户卡 MF 的基本信息文件	23
表 25	消费类 CPU 用户卡 ADF1 的 KEY 文件内容	23
表 26	消费类 CPU 用户卡 ADF1 的公共基本信息文件	23
表 27	消费类 CPU 用户卡卡类别标识	24
表 28	消费类 CPU 用户卡卡类别编码	24
表 29	消费类 CPU 用户卡个人基本信息文件	24
表 30	消费类 CPU 用户卡公共电子钱包	24
表 31	消费类 CPU 用户卡交易记录文件	25
表 32	表具类 CPU 用户卡文件详细信息	26
表 33	表具类 CPU 用户卡 MF 的 KEY 文件内容	26
表 34	表具类 CPU 用户卡 MF 的公共信息文件	26
表 35	表具类 CPU 用户卡卡类别标识	27
表 36	表具类 CPU 用户卡卡类别编码	27
表 37	表具类 CPU 用户卡 ADF 的 KEY 文件内容	27
表 38	表具类 CPU 用户卡 ADF 的基本信息文件	27
表 39	表具类 CPU 用户卡计量文件	28
表 40	表具类 CPU 用户卡设置信息文件	28
表 41	表具类 CPU 用户卡返回信息文件	29
表 42	CPU 卡命令 APDU 的内容及格式	30
表 43	CPU 卡响应 APDU 的内容及格式	30
表 44	CPU 卡命令集	30
表 45	CPU 卡 PULL 命令报文	31
表 46	CPU 卡 PULL 命令报文数据域	31
表 47	CPU 卡 PULL 命令响应报文数据域	32
表 48	CPU 卡 PULL 命令错误状态	32
表 49	CPU 卡 CHARGE 命令报文	32
表 50	CPU 卡 CHARGE 命令报文数据域	32
表 51	CPU 卡 CHARGE 命令响应报文数据域	33
表 52	CPU 卡 CHARGE 命令错误状态	33

表 53	CPU 卡 INITIALIZE FOR CHARGE 命令报文	33
表 54	CPU 卡 INITIALIZE FOR PULL 命令报文	33
表 55	CPU 卡 INITIALIZE FOR CHARGE/PULL 命令报文数据域	34
表 56	CPU 卡 INITIALIZE FOR CHARGE/PULL 命令充值响应报文数据域	34
表 57	CPU 卡 INITIALIZE FOR CHARGE/PULL 命令消费响应报文数据域	34
表 58	CPU 卡 INITIALIZE FOR CHARGE/PULL 命令错误状态	34
表 59	CPU 卡 GET SPECIAL _ TRAN PROOF 命令报文	35
表 60	CPU 卡 GET SPECIAL _ TRAN PROOF 命令错误状态	35
表 61	CPU 卡 INIT _ SAM _ FOR _ PURCHASE 命令报文	36
表 62	CPU 卡 CREDIT _ SAM _ FOR _ PURCHASE 命令报文	37
表 63	CPU 卡 INIT _ FOR _ DEACRYPT 命令报文	38
表 64	CPU 卡 DES CRYPT 命令报文	39
表 65	CPU 卡 DES CRYPT 命令引用控制参数	39
表 66	逻辑加密卡扇区密钥计算命令报文	40
表 67	逻辑加密卡扇区密钥计算命令响应报文状态码	40
表 68	IC 卡终端交易上传数据格式要求	43

前 言

本标准是对 CJ/T 166—2002《建设事业 IC 卡应用技术》的修订。

本标准与 CJ/T 166—2002 相比修订的主要内容包括：

1. 补充完善表具类 IC 卡终端的技术要求；
2. 补充完善 IC 卡的安全机制和安全要求；
3. 补充完善 IC 卡应用系统要求；
4. 补充完善 IC 卡应用系统验收要求；
5. 修订了卡片技术要求；
6. 修订了消费类及服务类 IC 卡终端技术要求。

本标准由建设部标准定额研究所提出并归口。

本标准负责起草单位：建设部 IC 卡应用服务中心。

本标准参编单位：中外建设信息有限责任公司、北京江南歌盟科技有限公司、北京捷德智能卡系统有限公司、北京融通高科科技发展有限公司、北京握奇数据系统有限公司、朝阳华龙电子仪表有限公司、成都前锋电子仪器厂、大连世达科技有限公司、丹东思凯电子发展有限责任公司、飞利浦(中国)投资有限公司、杭州先锋电子技术有限公司、宁波东海集团有限公司、上海华虹集成电路有限责任公司、深圳市华旭科技开发有限公司、深圳市明华澳汉科技股份有限公司、索尼(中国)有限公司、天津环球磁卡股份有限公司、武汉蓝焰自动化应用技术有限责任公司、武汉天喻信息产业股份有限公司、亚太安讯网络电子技术有限公司、浙江威星电子系统软件有限公司、重庆明光燃气设备有限公司、珠海东信和平智能卡股份有限公司、珠海亿达科技电子工业有限公司。

本标准主要起草人：马虹、申绯斐、王辉、杜昊、赵海波、周欣、王毅(以下按姓氏笔画排序)丁晓明、丹明波、刘贤斌、孙立颖、朱树兴、朱洲、汤天顺、闫廷辉、张大群、张汉就、张驰、张松林、张继中、李中华、李之明、李锦铭、杨德强、汪有余、周天宝、周承平、林立峰、欧阳由、钟健、钱维钧、陶坚、高林洪、常波、章曙、黄铁军、蒋海、谢文录、谢骏、靳宇华。

CJ/T 166—2002《建设事业 IC 卡应用技术》于 2002 年 6 月首次发布，本次为第一次修订。本标准自实施之日起代替 CJ/T 166—2002。

建设事业集成电路(IC)卡应用技术

1 范围

本标准规定了建设事业应用 IC 卡的卡片技术要求、消费类及服务类 IC 卡终端技术要求、表具类 IC 卡终端技术要求、密钥系统和安全技术要求、安全机制及安全要求、应用系统要求、应用系统验收要求和相应的定义、符号等。

本标准适用于使用建设行业发行或接受的 IC 卡及其产品的相关组织。其使用对象主要是与建设事业 IC 卡应用相关的卡片和终端设计、制造、管理、发行以及应用系统的研制、开发、集成、维护和监理的部门(单位)。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 2260—1995 中华人民共和国行政区划代码

GB/T 2828.1—2003 计数抽样检验程序 第 1 部分:按接收质量限(AQL)检索的逐批检验抽样计划

GB/T 2887—2000 电子计算机场地通用规范

GB 4943—2001 信息技术设备的安全

GB/T 4754—1994 国民经济行业分类与代码

GB/T 7408—1994 数据源:日期表示方法

GB/T 9361—1988 计算机场地安全要求

GB/T 14916 识别卡 物理特性

GB/T 16649.1 识别卡 带触点的集成电路卡 第 1 部分:物理特性

GB/T 16649.2 识别卡 带触点的集成电路卡 第 2 部分:触点的尺寸与位置

GB/T 16649.3 识别卡 带触点的集成电路卡 第 3 部分:电信号和传输协议

GB/T 16649.4 识别卡 带触点的集成电路卡 第 4 部分:用于交换的行业间命令

GB/T 16649.5 识别卡 带触点的集成电路卡 应用标识符的编号系统和登记规程

GB/T 17554.1 识别卡 测试方法 第 1 部分:通用性能测试

GB/T 18239—2000 集成电路(IC)卡读写机通用规范

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第 1 部分:简介和一般模型

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第 2 部分:安全功能要求

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第 3 部分:安全保证要求

ISO/IEC 7811-1:1995 识别卡 记录技术 第一部分:凸印文字

ISO/IEC 7811-3:1995 识别卡 记录技术 第三部分:凸印在 ID-1 型卡字符位置

ISO/IEC 7812-1:2000 识别卡 发行者标识 第 1 部分:编号系统

ISO/IEC 14443-1:2000 识别卡 无触点集成电路卡 接近式卡 第 1 部分:物理特性