

ICS

备案号: PXX

CJ

中华人民共和国城镇建设行业标准

CJ/T ××××—××××

建设事业 CPU 卡操作系统技术要求

Technical requirement for chip operate system of CPU card in construction case

(报批稿)

发布

实施

中华人民共和国住房和城乡建设部 发布

目 次

前言.....	VII
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 缩略语和符号表示.....	3
5 机电特性、逻辑接口与传输协议.....	4
5.1 接触式 CPU 卡的机电特性、逻辑接口与传输协议.....	4
5.2 非接触式 CPU 卡机电特性、逻辑接口与传输协议.....	4
5.3 CPU 卡的机械特性.....	4
6 文件和命令.....	4
6.1 说明.....	4
6.2 文件.....	4
6.3 命令.....	5
7 应用选择.....	20
7.1 一般要求.....	20
7.2 应用标识符的编码.....	21
7.3 支付系统环境结构.....	21
7.4 支付系统目录编码.....	21
7.5 目录入口中执行命令的使用.....	21
7.6 其他目录的编码.....	22
7.7 终端的应用选择.....	22
8 安全机制及安全要求.....	23
8.1 安全机制.....	23
8.2 安全要求.....	23
8.3 加密算法.....	23
9 电子存折/电子钱包应用.....	23
9.1 应用说明.....	23
9.2 文件.....	24
9.3 命令.....	24
9.4 交易流程.....	47
9.5 防拔.....	77
9.6 交易处理性能.....	78
附录 A（规范性附录）数据元解释.....	79
附录 B（规范性附录）ED/EP 应用的密钥关系.....	81
B.1 说明.....	81
B.2 密钥关系.....	81
附录 C（资料性附录）密钥的推导方法和过程密钥的产生方法.....	82
C.1 子密钥推导方法.....	82
C.1.1 DPK 左半部分的推导方法.....	82

C.1.2 DPK 右半部分的推导方法	82
C.2 过程密钥的产生	83
C.3 MAC/TAC 的计算	83
附录 D (资料性附录) 应用密钥说明	85
D.1 密钥存储说明见表 D.1。	85
D.2 主密钥存放位置说明:	85
附录 E (资料性附录) 电子钱包应用的基本数据文件	86
E.1 MF 下文件信息	86
E.2 KEY 文件信息	86
E.3 目录信息文件	86
E.4 发行基本信息文件	86
E.5 公用钱包应用目录	87
E.5.1 KEY 文件	87
E.5.2 公共应用基本信息文件 (0015)	88
E.5.3 持卡人基本信息文件	88
E.5.4 电子钱包文件	88
E.5.5 复合交易记录文件	89
附录 F (资料性附录) 复合应用说明	90
F.1 一般要求	90
F.2 基础定义	90
F.3 交易流程	90
F.3.1 消费开始	90
F.3.2 消费结束	92

图表索引

图 1 命令 APDU 结构	6
图 2 响应 APDU 的结构	6
图 3 加入灰锁机制的交易预处理流程	48
图 4 圈存交易处理流程	49
图 5 圈提交易处理流程	52
图 6 消费交易处理流程	56
图 7 复合应用消费交易	59
图 8 修改透支限额交易	62
图 9 灰锁消费交易流程	65
图 10 联机解扣交易流程	69
图 11 补扣交易流程	73
图 12 补充交易流程	75
图 C.1 推导 DPK 左半部分	82
图 C.2 推导 DPK 右半部分	83
图 C.3 过程密钥的产生	83
图 C.4 MAC 和 TAC 的单倍长 DEA 密钥算法	84
图 F.1 消费开始示意图	92
图 F.2 消费结束示意图	93
表 1 命令 APDU 的内容	6

表 2 响应 APDU 的内容	6
表 3 APPLICATION BLOCK 命令报文	7
表 4 APPLICATION BLOCK 警告状态	7
表 5 APPLICATION BLOCK 错误状态	7
表 6 APPLICATION UNBLOCK 命令报文	8
表 7 APPLICATION UNBLOCK 错误状态	8
表 8 CARD BLOCK 命令报文	9
表 9 CARD BLOCK 错误状态	9
表 10 EXTERNAL AUTHENTICATION 命令报文	9
表 11 EXTERNAL AUTHENTICATION 警告状态	10
表 12 EXTERNAL AUTHENTICATION 错误状态	10
表 13 GET CHALLENGE 命令报文	10
表 14 GET CHALLENGE 错误状态	10
表 15 GET RESPONSE 命令报文	11
表 16 GET RESPONSE 正确响应命令报文	11
表 17 GET RESPONSE 警告状态	11
表 18 GET RESPONSE 错误状态	11
表 19 INTERNAL AUTHENTICATION 命令报文	12
表 20 INTERNAL AUTHENTICATION 警告状态	12
表 21 INTERNAL AUTHENTICATION 错误状态	12
表 22 PIN CHANGE/UNBLOCK 命令报文	12
表 23 PIN CHANGE/UNBLOCK 警告状态	13
表 24 PIN CHANGE/UNBLOCK 错误状态	13
表 25 READ BINARY 命令报文	13
表 26 READ BINARY 命令引用控制参数	14
表 27 READ BINARY 警告状态	14
表 28 READ BINARY 错误状态	14
表 29 READ RECORD 命令报文	15
表 30 READ RECORD 命令引用控制参数	15
表 31 READ RECORD 警告状态	15
表 32 READ RECORD 错误状态	15
表 33 SELECT 命令报文	16
表 34 SELECT 命令引用控制参数	16
表 35 SELECT PSE 的响应报文 (FCI)	16
表 36 SELECT DDF 的响应报文 (FCI)	16
表 37 SELECT ADF 的响应报文 (FCI)	16
表 38 SELECT 警告状态	17
表 39 SELECT 错误状态	17
表 40 UPDATE BINARY 命令报文	17
表 41 UPDATE BINARY 命令引用控制参数	18
表 42 UPDATE BINARY 警告状态	18
表 43 UPDATE BINARY 错误状态	18
表 44 UPDATE RECORD 命令报文	18
表 45 UPDATE RECORD 命令引用控制参数	19

表 46 UPDATE RECORD 警告状态	19
表 47 UPDATE RECORD 错误状态	19
表 48 VERIFY 命令报文	20
表 49 VERIFY 警告状态	20
表 50 VERIFY 错误状态	20
表 51 CHANGE PIN 命令报文	25
表 52 CHANGE PIN 错误状态	25
表 53 CREDIT FOR LOAD 命令报文	25
表 54 CREDIT FOR LOAD 命令报文数据域	25
表 55 CREDIT FOR LOAD 响应报文数据域	26
表 56 CREDIT FOR LOAD 错误状态	26
表 57 GET MESSAGE 命令	26
表 58 GET MESSAGE 命令响应报文数据	26
表 59 GET MESSAGE 命令错误状态码	27
表 60 DEBIT FOR PURCHASE/CASH WITHDRAW 命令报文	27
表 61 DEBIT FOR PURCHASE/CASH WITHDRAW 命令报文数据域	27
表 62 DEBIT FOR PURCHASE/CASH WITHDRAW 响应报文数据域	27
表 63 DEBIT FOR PURCHASE/CASH WITHDRAW 错误状态	27
表 64 DEBIT FOR UNLOAD 命令报文	28
表 65 DEBIT FOR UNLOAD 命令报文数据域	28
表 66 DEBIT FOR UNLOAD 响应报文数据域	28
表 67 DEBIT FOR UNLOAD 错误状态	28
表 68 GET BALANCE 命令报文	29
表 69 GET BALANCE 响应报文数据域	29
表 70 GET BALANCE 错误状态	29
表 71 GET TRANSACTION PROVE 命令报文	29
表 72 GET TRANSACTION PROVE 命令报文数据域	30
表 73 GET TRANSACTION PROVE 响应报文数据域	30
表 74 GET TRANSACTION PROVE 错误状态	30
表 75 INITIALIZE FOR CASH WITHDRAW 命令报文	30
表 76 INITIALIZE FOR CASH WITHDRAW 命令报文数据域	31
表 77 INITIALIZE FOR CASH WITHDRAW 响应报文数据域	31
表 78 INITIALIZE FOR CASH WITHDRAW 错误状态	31
表 79 INITIALIZE FOR LOAD 命令报文	31
表 80 INITIALIZE FOR LOAD 命令报文数据域	32
表 81 INITIALIZE FOR LOAD 响应报文	32
表 82 INITIALIZE FOR LOAD 错误状态	32
表 83 INITIALIZE FOR PURCHASE 命令报文	32
表 84 INITIALIZE FOR PURCHASE 命令报文数据域	33
表 85 INITIALIZE FOR PURCHASE 响应报文数据域	33
表 86 INITIALIZE FOR PURCHASE 错误状态	33
表 87 INITIALIZE FOR UNLOAD 命令报文	33
表 88 INITIALIZE FOR UNLOAD 命令报文数据域	34
表 89 INITIALIZE FOR UNLOAD 响应报文数据域	34
表 90 INITIALIZE FOR UNLOAD 错误状态	34

表 91 INITIALIZE FOR UPDATE 命令报文	34
表 92 INITIALIZE FOR UPDATE 命令报文数据域	35
表 93 INITIALIZE FOR UPDATE 响应报文数据域	35
表 94 INITIALIZE FOR UPDATE 错误状态	35
表 95 RELOAD PIN 命令报文	35
表 96 RELOAD PIN 命令报文数据域	36
表 97 RELOAD PIN 错误状态	36
表 98 INITIALIZE FOR CAPP PURCHASE 命令报文格式	36
表 99 INITIALIZE FOR CAPP PURCHASE 命令报文的的数据域定义	37
表 100 INITIALIZE FOR CAPP PURCHASE 命令执行成功的响应报文数据域	37
表 101 INITIALIZE FOR CAPP PURCHASE 命令可能回送的错误状态	37
表 102 UPDATE CAPP DATA CACHE 命令报文	37
表 103 UPDATE CAPP DATA CACHE 命令报文中的引用控制参数 P2 定义	38
表 104 UPDATE CAPP DATA CACHE 可能回送的错误状态码	38
表 105 DEBIT FOR CAPP PURCHASE 命令报文	38
表 106 DEBIT FOR CAPP PURCHASE 命令报文的的数据域定义	39
表 107 DEBIT FOR CAPP PURCHASE 命令执行成功的响应报文数据域	39
表 108 DEBIT FOR CAPP PURCHASE 可能回送的错误状态	39
表 109 DEBIT FOR UNLOCK 命令报文	39
表 110 DEBIT FOR UNLOCK 命令报文的的数据域定义	40
表 111 DEBIT FOR UNLOCK 命令执行成功的响应报文数据域	40
表 112 DEBIT FOR UNLOCK 错误状态	40
表 113 GET LOCK PROOF 命令报文	40
表 114 参数、状态与 GET LOCK PROOF 响应报文数据域的关系	41
表 115 正常状态 GET LOCK PROOF 命令执行成功的响应报文数据域	41
表 116 灰锁状态 GET LOCK PROOF 命令执行成功的响应报文数据域	41
表 117 TAC 未读时 GET LOCK PROOF 命令执行成功的响应报文数据域	41
表 118 GET LOCK PROOF 错误状态	42
表 119 GREY LOCK 命令报文	42
表 120 GREY LOCK 命令报文的的数据域定义	42
表 121 GREY LOCK 命令执行成功的响应报文数据域	43
表 122 GREY LOCK 错误状态	43
表 123 GREY UNLOCK 命令报文	43
表 124 GREY UNLOCK 命令报文的的数据域定义	43
表 125 GREY UNLOCK 命令执行成功的响应报文数据域	43
表 126 GREY UNLOCK 错误状态	44
表 127 INITIALIZE FOR GREY LOCK 命令报文	44
表 128 INITIALIZE FOR GREY LOCK 命令报文的的数据域定义	44
表 129 INITIALIZE FOR GREY LOCK 命令执行成功的响应报文数据域	44
表 130 INITIALIZE FOR GREY LOCK 错误状态	45
表 131 INITIALIZE FOR GREY UNLOCK 命令报文	45
表 132 INITIALIZE FOR GREY UNLOCK 命令报文的的数据域定义	45
表 133 INITIALIZE FOR GREY UNLOCK 命令执行成功的响应报文数据域	45
表 134 INITIALIZE FOR GREY UNLOCK 错误状态	46

表 135 UPDATE OVERDRAW LIMIT 命令报文	46
表 136 命令报文的的数据域	46
表 137 UPDATE OVERDRAW LIMIT 响应报文数据域	46
表 138 UPDATE OVERDRAW LIMIT 错误状态	46
表 A.1 数据元解释	79
表 B.1 共用于电子存折和电子钱包应用的密钥	81
表 B.2 用于电子存折应用的密钥	81
表 D.1 密钥存储说明	85
表 E.1 文件结构列表	86
表 E.2 KEY 文件	86
表 E.3 目录信息文件	86
表 E.4 发行基本信息文件	87
表 E.5 1001 目录下文件信息	87
表 E.6KEY 文件	87
表 E.7 公共应用基本信息文件	88
表 E.8 持卡人基本信息文件	88
表 E.9 电子钱包文件	89
表 E.10 复合交易记录文件	89
表 F.1 复合应用专用文件	90