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 0025.1—201x
代替JR/T 0025.1—2010

中国金融集成电路（IC）卡规范 第1部分：电子钱包/电子存折应用卡片规范

China financial integrated circuit card specifications—
Part 1: Electronic purse/electronic deposit application card specification

（送审稿）

201x-xx-xx 发布　　201x-xx-xx 实施

中国人民银行 发布

目　　次

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为17个部分：

——第1部分：电子钱包/电子存折应用卡片规范；

——第2部分：电子钱包/电子存折应用规范；

——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9部分：电子钱包扩展应用指南；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——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17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第1部分。

本部分代替JR/T 0025.1—2010《中国金融集成电路（IC）卡规范　第1部分：电子钱包/电子存折卡片规范》。

本部分与JR/T 0025.1-2010相比主要变化如下：

——修订了标准的前言。

本部分与JR/T 0025.1—2005相比主要变化如下：

——名称由“电子钱包/电子存折卡片规范”更改为“电子钱包/电子存折应用卡片规范”；

——重新起草标准的前言及引言；

——对“术语和定义”及“符号和缩略语”在正文中的出现的情况做了核对，对于没有出现的直接予以删除，对于出现的进行了修改和完善，并同步修改正文；

——对“规范性引用文件”在正文中的引用情况做了核对，对正文中引用到的文件根据标准编写要求进行重新编排和规范，将参考到的文件归集到参考文献，将没有引用也没有参考的文件予以剔除；

——根据当前先进技术的发展趋势及主流标准的应用情况，对本部分进行了补充完善；

——为保证标准的适用性，根据中国银行卡产业的实际需求，针对原标准在使用过程中发现的问题进行修订；

——JR/T0025.1中机电特性、逻辑接口与传输协议、文件和应用选择内容与JR/T0025.3中等同的内容直接引用JR/T0025.3；

——删除了资料性附录“目录结构实例”和“使用T=0协议交换的示例”（2005年版的附录A和附录C）；

——将“卡片结构示例”调整为资料性附录（2005 年版的 6.1.1.5，本版的附录 B）。

本部分的附录 A 和附录 B 为资料性附录。

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归口。

本部分主要起草单位：中国人民银行、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、上海浦东发展银行、中国银联股份有限公司、中国印钞造币总公司、中国金融电子化公司和银行卡检测中心。

本部分主要起草人：

本部分所代替标准的历次版本发布情况为：

——《中国金融集成电路（IC）卡规范》（V1.0）卡片规范；

——JR/T 0025.1—2005；

——JR/T 0025.1—2010。

引　言

本部分为JR/T 0025的第1部分，与JR/T 0025的第2部分一起构成电子钱包/电子存折规范。

电子钱包/电子存折应用为同一类应用，两者在卡片和终端的处理流程上基本相同，主要区别有：电子钱包应用支持消费、圈存等交易，消费无须提交个人识别码，卡片中的消费明细记录功能为可选；电子存折应用支持消费、取现、圈存、圈提、修改透支限额等功能，消费必须提交个人识别码，卡片中的消费明细功能为必选。两者在银行后台的账户处理流程由各个发卡机构决定，不在JR/T 0025范围之内。电子钱包/电子存折应用的密钥管理系统在中国人民银行统一管理下建设，相关密钥管理办法及流程（包括相关PSAM卡部分）不在JR/T 0025范围之内。

中国金融集成电路（IC）卡规范
第1部分：电子钱包/电子存折应用卡片规范

1 范围

JR/T 0025的本部分规定了电子钱包/电子存折卡片方面的内容，包括卡片的机电特性、逻辑接口和传输协议，文件和命令，应用选择及电子钱包/电子存折卡的安全机制，其中：

——机电接口、逻辑接口和传输协议。用于卡和终端间的信息交换。

——文件和命令集。定义了金融应用中所使用的文件、命令集和对终端响应的基本要求。金融应用中所需的专用命令在JR/T 0025.2中定义。

——应用选择。定义了卡和终端完成应用选择的处理过程，并规定了与卡中此过程相关的数据文件的逻辑结构。

——安全机制。定义了金融应用中有关安全的总体要求、加密算法和安全机制。应用安全特征和设备要求在JR/T 0025.2中定义。

本部分适用于由银行发行或受理的金融IC卡。其使用对象主要是与金融IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位），也可以作为其他行业IC卡应用的参考。

2 规范性引用文件

下列文件中的条款通过JR/T 0025的本部分的引用而成为本部分的条款。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部分，然而，鼓励根据本部分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部分。

GB/T 18238.3 信息技术 安全技术 散列函数 第3部分：专用散列函数（GB/T 18238.3—2002，ISO/IEC 10118-1:1994，IDT）

JR/T 0025.2 中国金融集成电路（IC）卡规范 第2部分：电子钱包/电子存折应用规范

ISO/IEC 7816-4:2005 识别卡 带触点的集成电路卡 第4部分：行业间交换用命令

ISO 8731-1 银行业 批准的报文鉴别算法 第1部分：DEA

ISO 8732 信息处理 64位块加密算法的运算方法

ISO/IEC 10116:1993 信息技术 安全技术 n位块密码算法的操作方式

3 术语和定义

下列术语和定义适用于JR/T 0025的本部分。

3.1

块 block

包含两个或三个域（头域、信息域和尾域）的字符组。

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

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。它应包括接口设备，也可包括其它的部件和接口（如与主机的通讯）。

3.4

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。

3.5

串联 concatenation

通过把第二个元素的字节添加到第一个元素的结尾将两个元素连接起来。每个元素中的字节在结果串中的顺序和原来从 IC 卡发到终端时的顺序相同，即高位字节在前。在每个字节中位按由高到低的顺序排列。

3.6

触点 contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.7

响应 response

IC 卡处理完成收到的命令报文后，返回给终端的报。

3.8

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支持个人识别码（PIN）保护的金融IC卡应用。它支持圈存、圈提、消费和取现等交易。

3.9

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。它支持圈存、消费等交易。消费不支持个人识别码（PIN）保护。

3.10

头域 prologue field

块的第一部分，包括节点地址（NAD）、协议控制字节（PCB）和长度（LEN）。

3.11

尾域 epilogue field

块的最后一部分，包括错误校验码（EDC）。

3.12

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。

3.13

函数 function

由一个或多个命令及其合成的行为实现的一个处理过程，这些命令及其合成的行为用于完成全部或部分交易。

3.14

哈希函数 hash function

将位串映射为定长位串的函数，它满足以下两个条件：

——对于一个给定的输出，不可能推导出与之相对应的输入数据；

——对于一个给定的输入，不可能通过计算得到具有相同的输出的另一个输入。

另外，如果要求哈希函数具备防冲突功能，则还应满足以下条件：

——不可能通过计算找到两个不同的输入具有相同的输出。

3.15

集成电路 integrated circuit(IC)

具有处理和/或存储功能的电子器件。

3.16

集成电路卡（IC卡） integrated circuit(s) card

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。

3.17

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。

3.18

报文鉴别码 message authentication code

对交易数据及其相关参数进行运算后产生的代码，主要用于验证报文的完整。

3.19

半字节 nibble

一个字节的高四位或低四位。

3.20

明文 plaintext

未被加密的信息。

3.21

密文 ciphertext

加密运算的结果。

3.22

密钥 key

控制加密转换操作的符号序列。

3.23

数字签名 digital signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.24

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.25

认证中心 certification authority

证明公钥和其它相关信息同其拥有者相关联的可信的第三方机构。

3.26

对称加密技术 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加密技术。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。

3.27

非对称加密技术 asymmetric cryptographic technique

采用两种相关变换进行加密的技术，一种是公开变换（由公钥定义）；另一种是私有变换（由私钥

定义)。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.28

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，在数字签名方案中，私钥用于签名。

3.29

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。在数字签名方案中，公钥用于验证。

3.30

保密密钥 secret key

对称加密技术中仅供指定实体所用的密钥。

3.31

数据完整性 data integrity

数据不受未经许可的方法变更或破坏的属性。

4 符号和缩略语

下列符号和缩略语适用于 JR/T 0025 的本部分。

ADF	应用定义文件（Application Definition File）
AEF	应用基本文件（Application Elementary File）
AID	应用标识符（Application Identifier）
APDU	应用协议数据单元（Application Protocol Data Unit）
C-APDU	命令APDU（Command APDU）
CLA	命令报文的类别字节（Class Byte of the Command Message）
DDF	目录定义文件（Directory Definition File）
DEA	数据加密算法（Data Encryption Algorithm）
DES	数据加密标准（Data Encryption Standard）
DF	专用文件（Dedicated File）
EDC	错误校验码（Error Detection Code）
EF	基本文件（Elementary File）
EMV	Europay、Mastercard和VISA
FCI	文件控制信息（File Control Information）
FIPS	联邦信息处理标准（Federal Information Processing Standard）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
IEC	国际电工委员会（International Electrotechnical Commission）
IFD	接口设备（Interface Device）
INS	命令报文的指令字节（Instruction Byte of Command Message）
ISO	国际标准化组织（International Organization for Standardization）
Lc	终端应用层（TAL）在情况3或情况4命令中发出数据的实际长度（Exact Length of Data Sent by the TAL IN A Case 3 or 4 Command）
Le	在情况2或情况4命令中返回给终端应用层(TAL)的数据最大期望长度(Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command）
LEN	长度（Length）
Lr	响应数据域的长度（Length of Response Data Field）
M	必备 （Mandatory）

MAC	报文鉴别码（Message Authentication Code）
MF	主文件（Master File）
n	数字型（Numeric）
N_{CA}	认证中心公钥模长（Length of the Certification Authority Public Key Modulus）
N_I	发卡行公钥模长（Length of the Issuer Public Key Modulus）
N_{IC}	IC卡公钥模长（Length of the ICC Public Key Modulus）
O	可选（Optional）
P1	参数1（Parameter 1）
P2	参数2（Parameter 2）
PCB	协议控制字节（Protocol Control Byte）
PIN	个人识别码（Personal Identification Number）
PSE	支付系统环境（Payment System Environment）
R-APDU	响应APDU（Response APDU）
RFU	预留（Reserved for Future Use）
RSA	Rivest、Sharmir和Adleman提出的一种非对称密钥算法
SAM	安全存取模块（Secure Access Module）
SFI	短文件标识符（Short File Identifier）
SHA	安全哈希算法（Secure Hash Algorithm）
SW1	状态字1（Status Word One）
SW2	状态字2（Status Word Two）
TAL	终端应用层（Terminal Application Layer）
$X:=ALG^{-1}(K)[Y]$	用密钥K，通过64位分组加密方法，对64位数据块Y进行解密
X:=Recover(PK)[Y]	用公钥PK，通过非对称可逆算法，对数据块Y进行恢复
xx	任意值
Y:=Sign(SK)[X]	用私钥SK，通过非对称可逆算法，对数据块X进行签名
Y:=ALG(K)[X]	用密钥K，通过64位分组加密方法，对64位数据块X进行加密
（X|n）	整数X和整数n（n=pq，p和q为素数）的Jacobi值，有如下定义：J:=（X（p-1）/2 mod p）（X（q-1）/2 mod q） 如果J=1或j=（pq-p-q+1），则：（X|n）=1，否则（X|n）=-1 注：整数X的Jacobi值在没有n素数因子时，也可计算。
[ ]	可选部分
|n|	整数n的位长
H:=Hash[MSG]	用160位的HASH函数对任意长度的报文MSG进行HASH运算。
C:=(A||B)	将m位数字B和n位数字A进行链接，定义为：$C=2^m A+B$
Abs（n）	n的绝对值
A=B	数值A等于数值B
A≡B mod n	整数A与B对于模n同余，即存在一个整数d，使得(A－B)=dn
A mod n	A整除n的余数，即：唯一的整数r，$1 \leq r < n$，存在一个整数d，使得A=dn+r
A:=B	A被赋予数值B

5 机电特性、逻辑接口与传输协议

机电特性、逻辑接口与传输协议见JR/T 0025.3第5章、第6章、第7章、第8章和第9章。

6 文件和命令

6.1 文件

文件见JR/T 0025.3第10章。

6.2 命令

6.2.1 C-APDU 格式

C-APDU由4字节长的必备头后跟一个可变长的条件体组成，见图1。

CLA	INS	P1	P2	Lc	Data	Le
←必备头→				←条件体→		

图1 C-APDU 格式

C-APDU中发送的数据字节数用Lc（命令数据域的长度）表示。

R-APDU中期望返回的数据字节数用Le（期望数据长度）表示。当Le存在且值为0时，表示需要最大字节数（256字节）。在命令报文需要时，Le可始终被设为'00'。

C-APDU报文的内容见表1。

表1 C-APDU 的内容

代码	描述	长度
CLA	命令类别	1
INS	指令字节	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据位串（=Lc）	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

6.2.2 R-APDU 格式

R-APDU格式由一个变长的条件体和后随两字节长的必备尾组成，见图2。

Data	SW1	SW2
条件体	←必备尾→	

图2 R-APDU 的结构

表2 R-APDU 的内容

代码	描述	长度
Data	响应中接收的数据位串（=Lr）	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

当使用T=1协议时，对于所有Le=’00’的命令，状态字SW1 SW2=“90 00”或“61 La”均表示命令的成功执行。但由于可读性的需要，这两种应答码只用了“90 00”作为参考。

本条描述了以下的C-APDU/R-APDU：

——APPLICATION BLOCK（应用锁定）；

——APPLICATION UNBLOCK（应用解锁）；

——CARD BLOCK（卡片锁定）；

——EXTERNAL AUTHENTICATION（外部认证）；

——GET RESPONSE（取响应）；

——GET CHALLENGE（产生随机数）；

——INTERNAL AUTHENTICATION（内部认证）；

——PIN CHANGE/UNBLOCK（个人识别码修改/解锁）；

——READ BINARY（读二进制）；

——READ RECORD（读记录）；

——SELECT（选择）；

——UPDATE BINARY（修改二进制）；

——UPDATE RECORD（修改记录）；

——VERIFY（校验）。

如果在应用规范使用了本条中定义的命令，执行该命令所需的附加信息见JR/T 0025.2。

6.2.3 APPLICATION BLOCK 命令

6.2.3.1 定义和范围

APPLICATION BLOCK命令使当前选择的应用失效。

当APPLICATION BLOCK命令成功地完成应用临时锁定后，用SELECT命令选择已临时锁定的应用，将回送状态字“选择文件无效”（SW1 SW2=“6283”）。同时回送FCI（对于T=0卡片，需要用GET RESPONSE指令取回）。

当APPLICATION BLOCK命令成功完成应用永久锁定后，此后执行所有命令，卡片将回送状态字“应用永久锁定”（SW1 SW2=“9303”）。

对其他命令的影响根据不同应用而定。

6.2.3.2 命令报文

APPLICATION BLOCK命令报文编码见表3。

表3 APPLICATION BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘1E’
P1	‘00’，其他值预留
P2	‘00’或’01’
Lc	数据字节数
Data	报文鉴别码（MAC）数据元，根据第 8 章的规定编码
Le	不存在

P2=’00’：此命令执行成功后可锁定应用，但该应用可以用APPLICATION UNBLOCK命令解锁。

P2=’01’：此命令执行成功后将永久锁定应用。

6.2.3.3 命令报文数据域

命令报文数据域包括根据第8章的规定编码的报文鉴别码（MAC）数据元。

6.2.3.4 响应报文数据域

响应报文数据域不存在。

6.2.3.5 响应报文状态字

无论应用是否已经失效，此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表4。

表4 APPLICATION BLOCK 警告状态

SW1	SW2	含　义
‘62’	‘00’	无信息提供
‘62’	‘81’	回送数据可能出错
‘62’	‘83’	选择文件无效

‘6A’	‘81’	不支持此功能
‘93’	‘03’	应用永久锁定

IC卡可能回送的错误状态字见表5。

表5 APPLICATION BLOCK 错误状态

SW1	SW2	含 义
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1 和 P2 错误
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.4 APPLICATION UNBLOCK 命令

6.2.4.1 定义和范围

APPLICATION UNBLOCK命令用于恢复当前应用。

当APPLICATION UNBLOCK命令成功地完成后，由APPLICATION BLOCK命令产生的对应用命令响应的限制将被取消。

6.2.4.2 命令报文

APPLICATION UNBLOCK命令报文编码见表6。

表6 APPLICATION UNBLOCK 命令报文

代码	值
CLA	‘84’
INS	‘18’
P1	‘00’，其他值预留
P2	‘00’，其他值预留
Lc	数据字节数
Data	报文鉴别码（MAC）数据元，根据第 8 章的规定编码
Le	不存在

6.2.4.3 命令报文数据域

命令报文数据域的内容包括根据第8章的规定编码的报文鉴别码（MAC）数据元。

6.2.4.4 响应报文数据域

响应报文数据域不存在。

6.2.4.5 响应报文状态字

当应用被临时锁定时，此命令执行成功的状态字是 “9000”。

当应用未被临时锁定，此命令执行返回的状态字是使用条件不满足（SW1 SW2=“6985”）。

IC卡可能回送的错误状态字见表7。

表7 APPLICATION UNBLOCK 错误状态

SW1	SW2	含 义

‘64’	‘00’	标志状态位未变
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 错误
‘69’	‘82’	不满足安全状态
‘69’	‘84’	未取随机数
‘69’	‘85’	使用条件不满足
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘82’	文件未找到
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用已被永久锁定

6.2.5 CARD BLOCK 命令

6.2.5.1 定义和范围

CARD BLOCK命令使卡中所有应用永久失效。

当CARD BLOCK命令成功地完成后，所有后续的命令都将回送状态字“不支持此功能”（SW1 SW2=“6A81”），且不执行任何其他操作。

6.2.5.2 命令报文

CARD BLOCK命令报文编码见表8。

表8 CARD BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘16’
P1	‘00’，其他值预留
P2	‘00’，其他值预留
Lc	数据字节数
Data	报文鉴别码（MAC）数据元，根据第 8 章的规定编码
Le	不存在

6.2.5.3 命令报文数据域

命令报文数据域包括根据第8章的规定编码的报文鉴别码（MAC）数据元。

6.2.5.4 响应报文数据域

响应报文数据域不存在。

6.2.5.5 响应报文状态字

此命令执行成功的状态字是 “9000”。

IC卡可能回送的错误状态字见表9。

表9 CARD BLOCK 错误状态

SW1	SW2	含　　义
‘64’	‘00’	标志状态位没变
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 错误
‘69’	‘87’	安全报文数据项丢失

‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.6 EXTERNAL AUTHENTICATION 命令

6.2.6.1 定义和范围

EXTERNAL AUTHENTICATION命令要求IC卡中的应用验证密码。

IC卡的响应包括命令处理状态的回送。

6.2.6.2 命令报文

EXTERNAL AUTHENTICATION命令报文编码见表10。

表10 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8-16
Data	发卡方认证数据
Le	不存在

EXTERNAL AUTHENTICATION命令使用的算法参考值（P1）编码为’00’表示无信息。算法参考值在命令发出之前是已知的，或者在数据域中提供。

EXTERNAL AUTHENTICATION命令的参数P2为’00’时的含义是无信息。P2的值可事先得到，也可以在数据域中提供。

6.2.6.3 命令报文数据域

命令报文数据域中包含8-16字节的数据：

——前 8 个必备型字节包含密码；

——可选的 1-8 个附加字节是专用的信息。

6.2.6.4 响应报文数据域

响应报文数据域不存在。

6.2.6.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表11。

表11 EXTERNAL AUTHENTICATION 警告状态

SW1	SW2	含　义
‘63’	‘00’	认证失败

IC卡可能回送的错误状态字见表12。

表12 EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	含　义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误

‘6E’	‘00’	CLA 不支持或错误

6.2.7 GET CHALLENGE 命令

6.2.7.1 定义和范围

GET CHALLENGE命令请求一个用于安全相关过程（如安全报文）的随机数。

该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

6.2.7.2 命令报文

GET CHALLENGE命令报文编码见表13。

表13 GET CHALLENGE 命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’或’08’

6.2.7.3 命令报文数据域

命令报文数据域不存在。

6.2.7.4 响应报文数据域

响应报文数据域包括随机数，长度为4字节或8字节。

6.2.7.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字见表14。

表14 GET CHALLENGE 错误状态

SW1	SW2	含 义
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.8 GET RESPONSE 命令

6.2.8.1 定义和范围

该指令只用于T=0协议卡片。

当APDU不能用现有协议传输时，GET RESPONSE命令提供了一种从卡片向接口设备传送APDU（或APDU的一部分）的传输方法。

6.2.8.2 命令报文

GET RESPONSE命令报文编码见表15。

表15 GET RESPONSE 命令报文

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’

Lc	不存在
Data	不存在
Le	响应的期望数据最大长度

6.2.8.3 命令报文数据域

命令报文数据域不存在。

6.2.8.4 响应报文数据域

响应报文数据域的长度由Le的值决定。

如果Le的值为零，在附加数据有效时，卡片必须回送状态字“6CXX”，否则回送状态字“6F00”。

6.2.8.5 响应报文状态字

此命令执行成功的状态字是“9000”。

表16列出正常处理情况。

表16 GET RESPONSE 正常状态

SW1	SW2	含　　义
‘61’	‘XX’	表示正常处理，‘XX’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度

IC卡可能回送的警告状态字见表17。

表17 GET RESPONSE 警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

IC卡可能回送的错误状态字见表18。

表18 GET RESPONSE 错误状态

SW1	SW2	含　义
‘67’	‘00’	长度错误（Le 不正确）
‘6A’	‘86’	P1 和 P2 错误
‘6C’	‘XX’	长度错误（Le 不正确，’XX’表示实际长度）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘6F’	‘00’	数据无效

6.2.9 INTERNAL AUTHENTICATION 命令

6.2.9.1 定义和范围

INTERNAL AUTHENTICATION命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

6.2.9.2 命令报文

INTERNAL AUTHENTICATION命令报文编码见表19。

表19 INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	‘00’
Lc	认证数据的长度
Data	认证数据
Le	‘00’

INTERNAL AUTHENTICATION命令的参数P1为'00'时的含义是无信息。P1的值可事先得到，也可以在数据域中提供。

INTERNAL AUTHENTICATION命令的参数P2为'00'时的含义是无信息。P2的值可事先得到，也可以在数据域中提供。

6.2.9.3 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

6.2.9.4 响应报文数据域

响应报文数据域内容是相关认证数据，其格式和定义不在JR/T 0025的范围之内。

6.2.9.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表20。

表20 INTERNAL AUTHENTICATION 警告状态

SW1	SW2	含 义
'62'	'81'	回送的数据可能有错

IC卡可能回送的错误状态字见表21。

表21 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
'64'	'00'	标志状态位未变
'67'	'00'	Lc 域不存在
'68'	'82'	不支持安全报文
'69'	'85'	不满足使用条件
'6A'	'80'	数据域参数不正确
'6A'	'86'	P1 和 P2 错误
'6D'	'00'	INS 不支持或错误

6.2.10 PIN UNBLOCK 命令

6.2.10.1 定义和范围

PIN UNBLOCK命令为发卡方提供了解锁个人识别码的功能。

当PIN UNBLOCK命令成功完成后，卡将执行以下功能：

——重置个人识别码尝试计数器的值。

命令中个人识别码的传递采用加密方式。

6.2.10.2 命令报文

PIN UNBLOCK命令报文编码见表22。

表22 PIN UNBLOCK 命令报文

代码	值
CLA	'84'，根据第 8 章的规定编码
INS	'24'
P1	'00'
P2	'00'
Lc	数据字节数
Data	加密的个人识别码数据元和报文鉴别码（MAC）数据元，根据第 8 章的规定编码
Le	不存在

P2='00'，表示解锁个人识别码。此时应重置尝试计数器，但不更改个人识别码。

当P2='00'时，Lc应包括MAC数据元的长度。

6.2.10.3 命令报文数据域

命令报文数据域中个人识别码数据元（如果存在）和其后的MAC数据元组成。个人识别码和MAC数据元根据第8章的规定编码。

6.2.10.4 响应报文数据域

响应报文数据域不存在。

6.2.10.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表23。

表23 PIN UNBLOCK 警告状态

SW1	SW2	含 义
‘62’	‘00’	无信息提供
‘62’	‘81’	数据或能出错

IC卡可能回送的错误状态字见表24。

表24 PIN UNBLOCK 错误状态

SW1	SW2	含 义
‘64’	‘00’	标志状态位没变
‘65’	‘81’	内存失败
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘85’	使用条件不满足（PIN 未锁定）
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1 和 P2 错误
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用被永久锁定

6.2.11 READ BINARY 命令

6.2.11.1 定义和范围

READ BINARY命令用于读取二进制文件的内容（或部分内容）。

6.2.11.2 命令报文

READ BINARY命令报文编码见表25。

表25 READ BINARY 命令报文

代码	值
CLA	‘00’或’04’
INS	‘B0’
P1	见表 26
P2	从文件中读取的第一个字节的偏移地址
Lc	不存在；（CLA=’04’时除外）
Data	不存在；（CLA=’04’时，应包括 MAC）
Le	‘00’

表26定义了命令报文中的引用控制参数。

表26 READ BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X 1								读取模式： -用 SFI 方式
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI（取值范围 21-30）

6.2.11.3 命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含MAC。MAC的计算方法和长度由应用决定。

6.2.11.4 响应报文数据域

当Le的值为零时，只要文件的最大长度在256（短长度）或65536（扩展长度）之内，则其全部字节将被读出。

6.2.11.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表27。

表27 READ BINARY 警告状态

SW1	SW2	含 义
‘62’	‘81’	部分回送的数据可能有错
‘62’	‘82’	文件长度<Le

IC卡可能回送的错误状态字见表28。

表28 READ BINARY 错误状态

SW1	SW2	含 义
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（非当前 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1 和 P2 错误
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6C’	‘XX’	长度错误（Le 错误；’ XX’ 为实际长度）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.12 READ RECORD 命令

6.2.12.1 定义和范围

READ RECORD命令用于读取记录文件的内容。

IC卡的响应由回送记录组成。

6.2.12.2 命令报文

READ RECORD命令报文编码见表29。

表29 READ RECORD 命令报文

代码	值
CLA	‘00’ 或’ 04’

INS	‘B2’
P1	记录号
P2	引用控制参数（见表 30）
Lc	不存在（CLA=’04’时除外）
Data	不存在（CLA=’04’时除外）
Le	‘00’

表30定义了命令报文中的引用控制参数。

表30 READ RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X	X	X	X	X				SFI
					1	0	0	P1 为记录号

6.2.12.3 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含MAC。MAC的计算方法和长度由应用决定。

6.2.12.4 响应报文数据域

所有执行成功的READ RECORD命令的响应报文数据域由读取的记录组成。

6.2.12.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表31。

表31 READ RECORD 警告状态

SW1	SW2	含 义
‘62’	‘81’	回送的数据可能有错

IC卡可能回送的错误状态字见表32。

表32 READ RECORD 错误状态

SW1	SW2	含 义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	长度错误（Lc 域不存在）
‘69’	‘81’	命令与文件结构不相容
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.13 SELECT 命令

6.2.13.1 定义和范围

SELECT命令通过文件名或AID来选择IC卡中的PSE、DDF或ADF。应用选择见第7章。

命令执行成功后，PSE、DDF或ADF的路径被设定。

后续命令作用于与用SFI选定的PSE、DDF或ADF相联系的AEF。

从IC卡的响应报文应由回送FCI组成。

6.2.13.2 命令报文

SELECT命令报文编码见表33。

表33 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表 34）
P2	‘00’第一个或仅有一个 ‘02’下一个
Lc	‘05’-’10’
Data	文件名
Le	‘00’

表34定义了命令报文中的引用控制参数。

表34 SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0				
					1			通过文件名选择
						0	0	

6.2.13.3 命令报文数据域

命令报文数据域应包括所选择的PSE名、DF名或AID。

6.2.13.4 响应报文数据域

响应报文中数据域应包括所选择的PSE、DDF或ADF的FCI。表35和表36规定了此定义了所用的标签。本部分不规定FCI中回送的附加标志。

表35定义了成功选择PSE后回送的FCI：

表35 SELECT PSE 的响应报文（FCI）

标签	值			存在方式
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M

表36定义了成功选择DDF后回送的FCI。

表36 SELECT DDF 的响应报文（FCI）

标签	值			存在方式
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M

表37定义了成功选择ADF后回送的FCI：

表37 SELECT ADF 的响应报文（FCI）

标签	值			存在性方式
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘50’	应用标签	O
		‘87’	应用优先指示符	O
		‘9F08’	应用版本号	M
		‘9F12’	应用优先名称	O
		‘BF0C’	发卡行自定义数据（FCI）	O

6.2.13.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表38。

表38 SELECT 错误状态

SW1	SW2	含 义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	P1、P2 与 Lc 不一致
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁定

注： SW1 SW2=“6A82”用于表示当卡支持部分文件名选择时，没有与此部分文件名相匹配的文件。

6.2.14 UPDATE BINARY 命令

6.2.14.1 定义和范围

UPDATE BINARY命令报文使用C-APDU中给定的数据修改EF文件中已有的数据。

6.2.14.2 命令报文

UPDATE BINARY命令报文编码见表39。

表39 UPDATE BINARY 命令报文

代码	值
CLA	‘00’或‘04’
INS	‘D6’
P1	见表 40
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	修改用的数据+报文鉴别码（MAC）数据元（4 字节）

Le	不存在

CLA='00' 不需要安全报文。

CLA='04' 需要安全报文。

表40定义了命令报文中的引用控制参数。

表40 UPDATE BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X 1								读取模式： -用 SFI 方式
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI（取值范围 21-30）

6.2.14.3 命令报文数据域

命令报文数据域：包括更新原有数据的新数据。

报文鉴别码（MAC）数据元：4字节。

6.2.14.4 响应报文数据域

响应报文数据域不存在。

6.2.14.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表41。

表41 UPDATE BINARY 警告状态

SW1	SW2	含 义
'63'	'CX'	使用内部重试程序更新成功，其中 X 表示剩余重试次数。

IC卡可能回送的错误状态字见表42。

表42 UPDATE BINARY 错误状态

SW1	SW2	含 义
'65'	'81'	内存失败（修改失败）
'67'	'00'	长度错误（Lc 域为空）
'69'	'81'	命令与文件结构不相容
'69'	'82'	不满足安全状态
'69'	'84'	引用数据无效
'69'	'86'	不满足命令执行的条件（不是当前的 EF）
'6A'	'81'	不支持此功能
'6A'	'82'	未找到文件
'6A'	'86'	P1 和 P2 参数错误
'6B'	'00'	参数错误（偏移地址超出了 EF）
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误
'93'	'03'	应用永久锁定

6.2.15 UPDATE RECORD 命令

6.2.15.1 定义和范围

UPDATE RECORD命令报文用C-APDU中给定的数据更改指定的记录。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

6.2.15.2 命令报文

UPDATE RECORD命令报文编码见表43。

表43 UPDATE RECORD 命令报文

代码	值
CLA	‘00’或‘04’
INS	‘DC’
P1	P1=‘00’表示当前记录 P1≠‘00’指定的记录号
P2	见表 44
Lc	后续数据域的长度
Data	更新原有记录的新记录+报文鉴别码（MAC）数据元（4 字节）
Le	不存在

CLA=‘00’不需要安全报文。

CLA=‘04’需要安全报文。

表44定义了命令报文中的引用控制参数。

表44 UPDATE RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

6.2.15.3 命令报文数据域

命令报文数据域由更新原有记录的新记录和报文鉴别码（MAC）数据元（4字节）组成。

6.2.15.4 响应报文数据域

响应报文数据域不存在。

6.2.15.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字见表45。

表45 UPDATE RECORD 警告状态

SW1	SW2	含 义
‘63’	‘CX’	使用内部重试程序更新成功，其中 X 表示剩余重试次数。

IC卡可能回送的错误状态字见表46。

表46 UPDATE RECORD 错误状态

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容

‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

6.2.16 VERIFY 命令

6.2.16.1 定义和范围

VERIFY命令用于校验命令数据域中的个人识别码的正确性。

如PIN文件位于某一应用下，当此应用被锁定时，禁止校验PIN；如PIN文件位于MF下，当应用被锁定后可以执行校验PIN命令。

6.2.16.2 命令报文

VERIFY命令报文编码见表47。

表47 VERIFY 命令报文

代码	值
CLA	‘00’
INS	‘20’
P1	‘00’
P2	‘00’
Lc	可变
Data	外部输入的个人识别码
Le	不存在

P2=’00’表示无特殊限定符被使用。在IC卡上，VERIFY命令在处理过程中应明确知道如何去寻找个人识别码。

6.2.16.3 命令报文数据域

命令报文数据域由持卡者输入的个人识别码组成。

6.2.16.4 响应报文数据域

响应报文数据域不存在。

6.2.16.5 响应报文状态字

此命令执行成功的状态字是“9000”。

当前的应用选择中，命令数据域中外部输入的个人识别码与卡中存放的个人识别码校验失败时，IC卡将回送SW2=’Cx’，其中’x’表示个人识别码允许重试的次数；当卡回送’C0’时，表示不能重试个人识别码。此时再使用VERIFY命令时，将回送失败状态字SW1 SW2=“6983”。

IC卡可能回送的警告状态字见表48。

表48 VERIFY 警告状态

SW1	SW2	含　义
‘63’	‘Cx ‘	校验失败，’ x’ 表示允许重试的次数

IC卡可能回送的错误状态字见表49。

表49 VERIFY 错误状态

SW1	SW2	含　义

‘64’	‘00’	标志状态位没变
‘69’	‘83’	认证方法（个人识别码）锁定
‘69’	‘84’	引用数据无效
‘6A’	‘86’	P1 和 P2 错误
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

7 应用选择

应用选择见JR/T 0025.3第12章。

8 安全机制

8.1 基本安全要求

8.1.1 共存应用

为了独立地管理一张卡上不同应用间的安全问题，每一个应用应该放在一个单独的ADF中。亦即在应用之间应该设计一道“防火墙”以防止跨过应用进行非法访问。另外，每一个应用也不应该与个人化要求和卡中共存的其他应用规则发生冲突。

8.1.2 密钥的独立性

用于一种特定功能（如扣款）的加密/解密密钥不能被任何其他功能所使用，包括保存在IC卡中的密钥和用来产生、派生、传输这些密钥的密钥。

如果应用要求使用SAM，其对终端、发卡方和私有SAM的安全要求见JR//T 0025.2。

8.2 密钥和个人识别码的存放

IC卡应该能够保证用于RSA算法的非对称私有密钥或用于DES算法的对称加密密钥在没有授权的情况下，不会被泄露出来。

如果使用个人识别码，则应保证其在IC卡中的安全存放，且在任何情况下都不会被泄露。

8.3 安全报文传送

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用MAC来实现。数据的可靠性通过对数据域的加密来得到保证。

8.3.1 安全报文传送格式

本部分中定义的安全报文传送格式应符合ISO 7816-4的规定。当CLA字节的第二个半字节等于十六进制数字’4’时，表明对发送方命令数据要采用安全报文传送。卡中的FCI表明某个命令的数据域的数据是否需要加密传输，是否应该以加密的方式处理。安全报文传送格式见表50。

表50 安全报文传送格式

b4	b3	b2	b1	说 明
0	0	x	x	不需要安全报文
0	1	x	x	需要安全报文

8.3.2 报文完整性和验证

MAC是使用命令的所有元素（包括命令头）产生的。一条命令的完整性，包括命令数据域（如果存在的话）中的数据元，通过安全报文传送得以保证。

8.3.2.1 MAC 的位置

MAC是命令数据域中最后一个数据元。

8.3.2.2 MAC 的长度

本部分中MAC的长度规定为4个字节。

8.3.2.3 MAC 密钥的产生

在安全信息处理过程中用到的MAC过程密钥是按照8.3.4中描述的过程密钥的产生过程产生的。MAC DEA密钥的原始密钥用于产生MAC过程密钥。

8.3.2.4 MAC 的计算

按照如下的方式使用单重或三重DEA加密方式产生MAC：

第一步：取8个字节的16进制数字'0'作为初始变量。

第二步：按照顺序将以下数据串联在一起形成数据块：

——CLA、INS、P1、P2 和 Lc[1]；

——所有在 JR/T 0025.2 中定义的数据；

——在命令的数据域中（如果存在）包含明文或加密的数据。（例：如果要更改个人识别码，加密后的个人识别码数据块放在命令数据域中传输）。

第三步：将该数据块分成8字节为单位的数据块，标号为D1、D2、D3和D4等。最后的数据块有可能是1-8个字节。

第四步：如果最后的数据块长度是8字节的话，则在其后加上16进制数字'80 00 00 00 00 00 00 00'，转到第五步。

如果最后的数据块长度不足8字节，则在其后加上16进制数字'80'，如果达到8字节长度，则转入第五步；否则在其后加入16进制数字'0'直到长度达到8字节。

第五步：对这些数据块使用MAC过程密钥进行加密，过程密钥按照8.3.2.3描述的方式产生。如果安全报文传送支持单长度的MAC DEA密钥，则依照图3的方式使用MAC过程密钥来产生MAC（根据在第二步中产生的数据块长度的不同，有可能在计算中会多于或少于四步）。

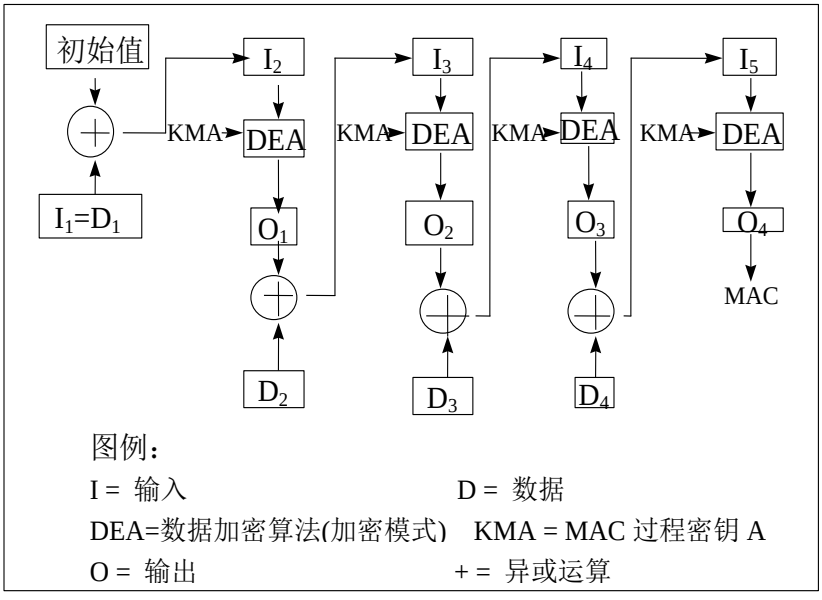


图3 单长度 DEA 密钥的 MAC 算法

如果安全报文传送的处理支持双长度MAC DEA密钥，则使用MAC过程密钥A和B（MAC的产生见图4），（根据第二步产生的数据块的长度，计算过程有可能多于或少于四步）。

[1] Lc 表示命令数据域后面 4 个字节 MAC 数据的长度，例如：APPLICATION BLOCK 命令需要产生一个 MAC，计算 MAC 的 Lc 的输入值是 4-FE，而不是 0，CLA 包括安全报文的表明('X4')。

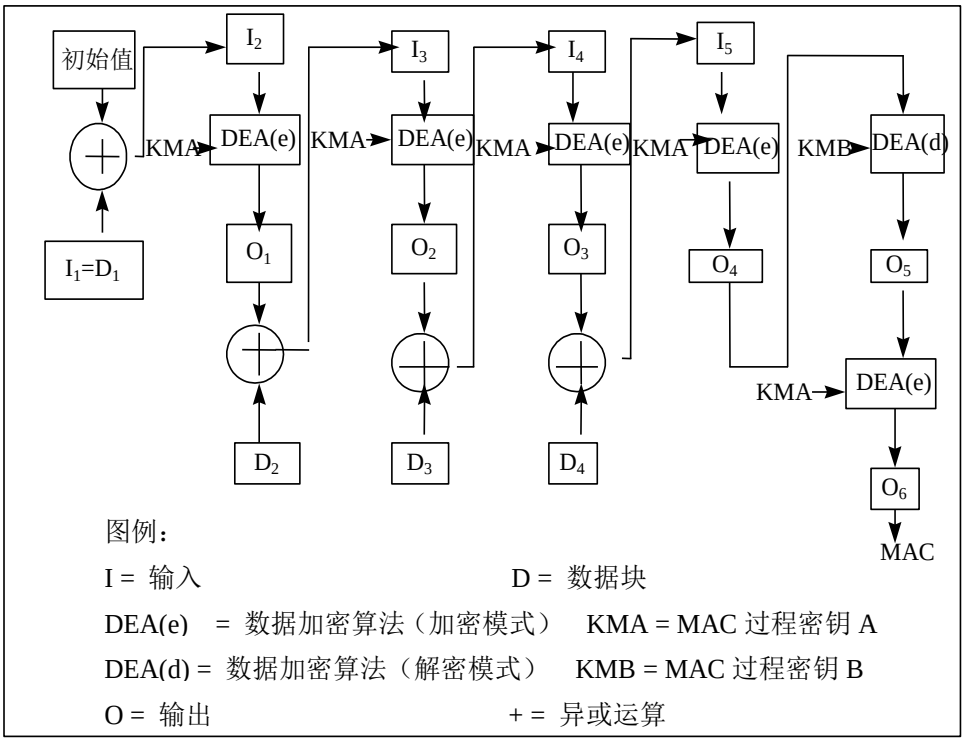


图4 双长度 DEA Key 的 MAC 算法

第六步：最终得到是从计算结果左侧取得的4字节长度的MAC。

8.3.3 数据可靠性

为保证命令中明文数据的保密性，可以将数据加密。所使用的数据加密技术，应被命令发送方和当前卡中被选择的应用所了解。

8.3.3.1 数据加密密钥的计算

在安全报文处理过程中用到的数据，加密过程密钥按照8.3.4中描述的方式产生。数据加密过程密钥的产生过程是从卡中的数据加密DEA密钥开始的。

8.3.3.2 被加密数据的结构

当命令中要求的明文数据需要加密时，它先要被格式化为以下形式的数据块：

——明文数据的长度，不包括填充字符（L_D）；

——明文数据；

——填充字符（根据 8.3.3.3 的要求）。

然后整个数据块使用8.3.3.3中描述的数据加密技术进行加密。

8.3.3.3 数据加密计算

数据加密技术如下所述：

第一步：用L_D表示明文数据的长度，在明文数据前加上L_D产生新的数据块。

第二步：将第一步中生成的数据块分解成8字节数据块，标号为D1、D2、D3和D4等等。最后一个数据块长度有可能不足8位。

第三步：如果最后（或唯一）的数据块长度等于8字节，转入第四步；如果不足8字节，在右边添加16进制数字'80'。如果长度已达8字节，转入第四步；否则，在其右边添加1字节16进制数字'0'直到长度达到8字节。

第四步：每一个数据块使用8.3.3.1中描述的数据加密方式加密。

如果采用单长度数据加密DEA密钥，数据块的加密见图5（使用数据加密过程密钥A进行加密）。

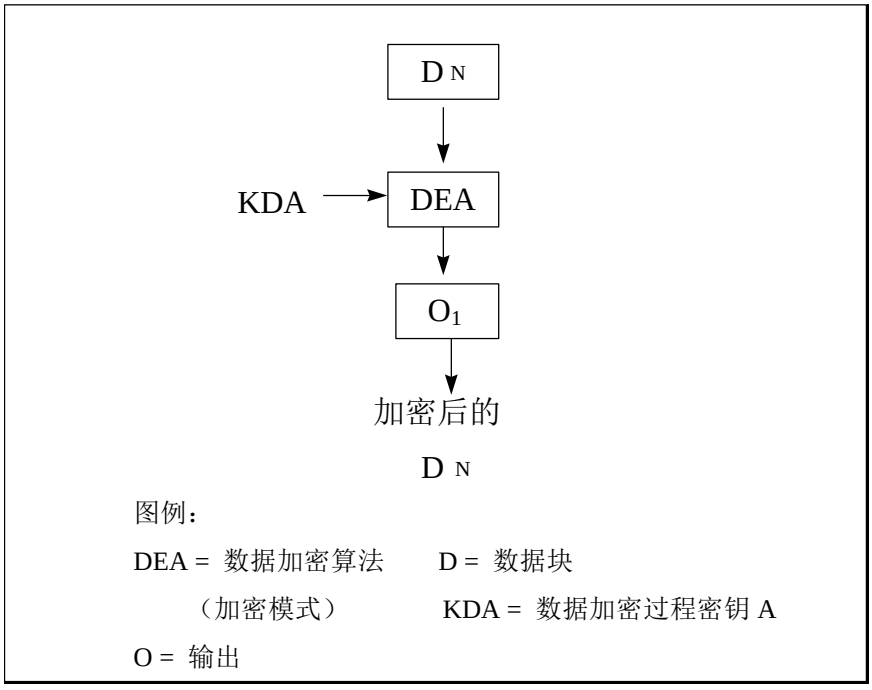


图5 单长度 DEA 密钥的数据加密

如果采用双长度数据加密DEA密钥，则数据块的加密见图6（使用数据加密过程密钥A和B来进行加密）。

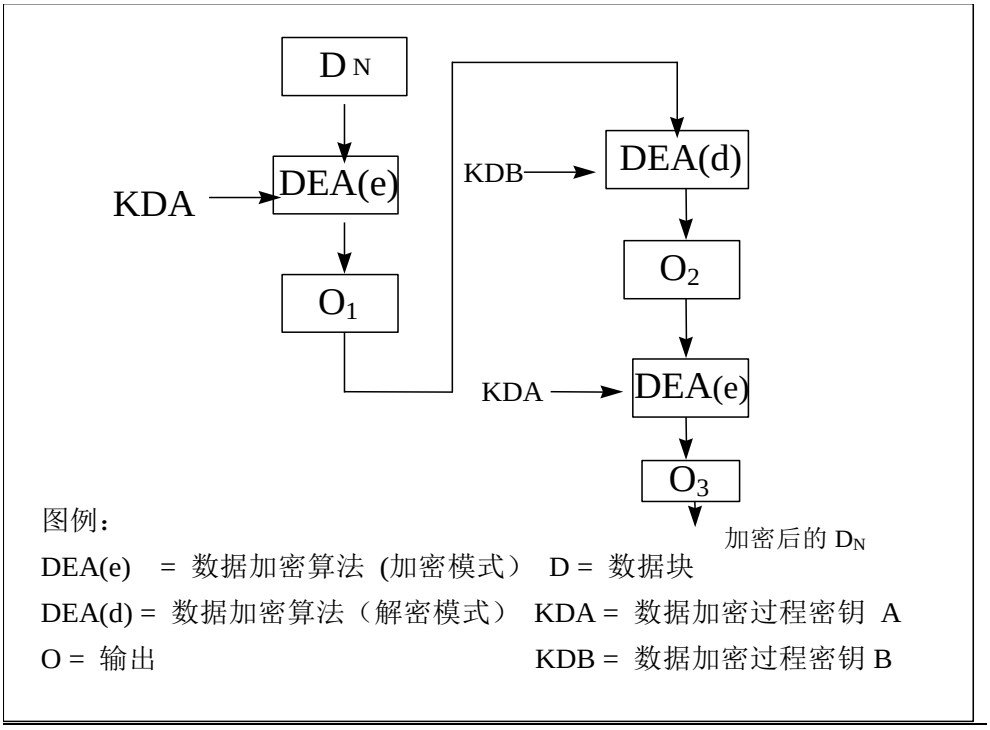


图6 使用双长度 DEA 密钥的数据加密

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的D1、加密后的D2等）。并将结果数据块插入到命令数据域中。

8.3.3.4 数据解密计算

卡片接收到命令之后，需要将包含在命令中的加密数据进行解密。数据解密的技术如下：

第一步：将命令数据域中的数据块分解成8字节长的数据块，标号为D1、D2、D3和D4等等。每个数据块使用如8.3.3.1所描述的方法产生的数据加密过程密钥进行解密。

如果采用单长度数据加密的DEA密钥，数据块解密见图7（使用数据加密过程密钥A进行解密）。

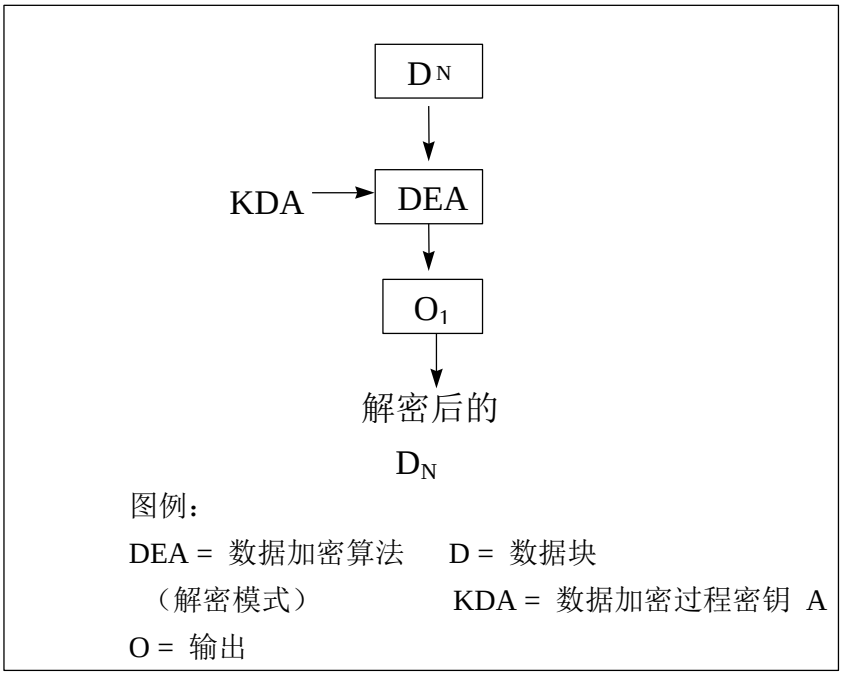


图7 使用单长度 DEA 密钥的数据解密

如果采用双长度数据加密的DEA密钥，则数据块的解密见图8（使用数据加密过程密钥A和B来进行解密）。

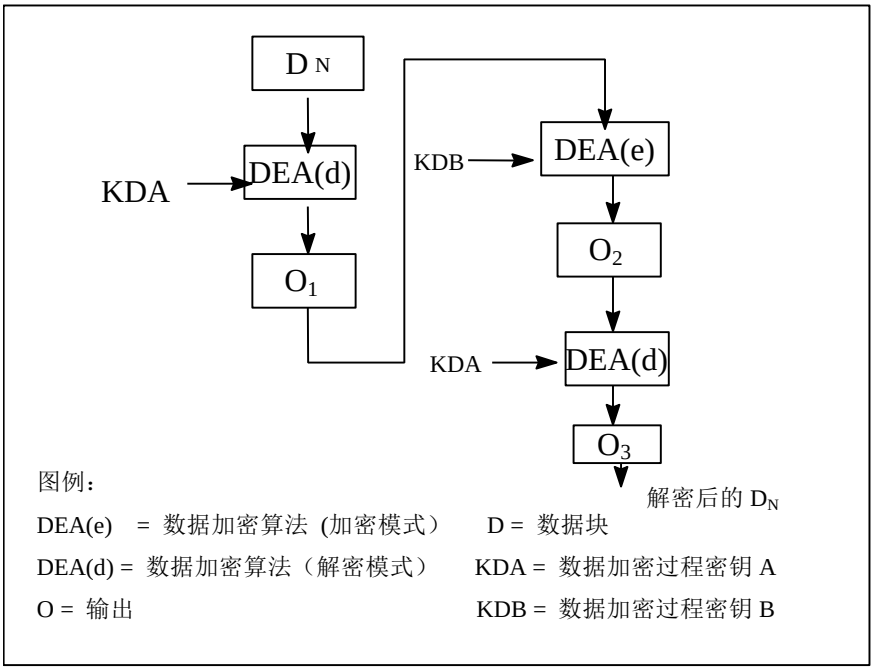


图8 使用双长度 DEA 密钥的数据解密

第二步：计算结束后，所有解密后的数据块依照顺序（解密后的D1、解密后的D2等）链接在一起。数据块由LD、明文数据、填充字符（如果在8.3.3.3描述的加密过程中增加的话）组成。

第三步：因为LD表示明文数据的长度，因此，它被用来恢复明文数据。

8.3.4 过程密钥的产生

MAC和数据加密过程密钥的产生如下所述。（在本条中统称为“过程密钥A”和“过程密钥B”）

8.3.4.1 基于单长度 DEA 密钥的过程密钥

第一步：卡片/发卡方决定是使用MAC DEA密钥A还是数据加密DEA密钥A来进行所选择的算法处理。（以后统称为“KeyA”）

第二步：用KeyA与预先决定的变量（如当前的交易序号）作异或运算产生过程密钥A。在作异或运算前，数据（如交易序号）如果少于8个字节，则在其右边用十六进制数字’0’填满。

8.3.4.2 基于双长度 DEA 密钥的过程密钥

第一步：卡片/发卡方决定是使用MAC DEA密钥A和B还是数据加密DEA密钥A和B来进行所选择的算法处理。（以后统称为“KeyA”和“KeyB”）

第二步：用KeyA与预先决定的变量（如当前的交易序号）作异或运算产生过程密钥A。在作异或运算前，数据（例如：交易序号）如果少于8个字节，则在其右边用十六进制数字’0’填满。

用KeyB与第二步中产生的过程密钥A所用数据的非作异或运算得到过程密钥B。非运算是以位为单位的，把值为’1’的位转换为’0’，将值为’0’的位转换为’1’。在作异或运算前，数据如果少于8个字节，则在其右边用十六进制数字’0’填满。

8.3.5 安全报文传送的命令情况

ISO 7816-4定义了四种命令情况。本条简单的讨论这些情况对C-APDU的作用。

情况一：这种情况时，没有数据送到IC卡（Lc）中，也没有数据从卡中返回（Le）。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC

CLA的第二个半字节是’4’表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

情况二：这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

CLA的第二个半字节是’4’表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

情况三：这种情况时，命令中有数据传送到卡中，但没有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC

CLA的第二个半字节是’4’表明支持第二种情况的安全报文传送技术。Lc为命令数据加上MAC的长度。

情况四：这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

CLA的第二个半字节是’4’表明支持第二种情况的安全报文传送技术。Lc为命令数据加上MAC的长度。

8.4 认可的加密算法

8.4.1 对称算法（DES）

安全报文允许使用64位块加密算法，该算法在ISO 8731-1、ISO 8732、ISO/IEC 10116中定义。以下定义的单DES加密和3-DES加密版本都可以用在8.3中描述的加密运算和MAC机制中。

3-DES加密是指使用双长度（16字节）密钥$K=(K_L||K_R)$将8字节明文数据块加密成密文数据块，如下所示：

$$Y=DES(K_L)[DES^{-1}(K_R)[DES(K_L)[X]]]$$

解密的方式如下：

$$X=DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L)[Y]]]$$

8.4.2 非对称算法（RSA）

JR/T 0025.2未强制要求使用非对称算法，非对称算法对于终端是可选的。

RSA算法被用来进行静态和动态数据验证以及数字签名。公开密钥的指数可以为奇数，也可以为偶数。

算法产生的数字签名的长度等于所用的模数的大小。模数的最大限制见表51。

表51 不同模数在字节上的最大限制

描 述	最大长度
验证授权公开密钥模数	248 字节
发卡方公开密钥模数	247 字节
IC 卡公开密钥模数	128 字节

同时，验证授权公开密钥模数的长度N_{CA}，发卡方公开密钥模数的长度N_I，IC卡公开密钥模数的长度N_{IC}应该满足以下关系：$N_{IC}<N_I<N_{CA}$。

在选择公开密钥模数的长度时，应该考虑到密钥的生命周期以及在此生命周期内被解密的可能性。每个密钥的长度范围（上、下限）在其相应的专用规范中规定。

发卡方公开密钥的指数的长度与IC卡公开密钥的指数长度由发卡方决定。指数可以是预先约定的固定的数字如2、3或$2^{16}+1$，但是它的长度不能超过其对应的密钥模数长度的四分之一。

该数字签名算法中的公开密钥算法的标志码为16进制数字’01’。

RSA算法的密钥、签名和恢复功能在下面说明。公开密钥的奇偶指数将分别考虑。同时，也规定了密钥产生过程的最低要求。

8.4.2.1 奇数公开密钥指数

8.4.2.1.1 密钥

带有奇数公开密钥指数e的RSA数字签名机制的私有密钥S_K包括两个素数p和q，p-1和q-1与e是互素的，它们与私有密钥指数d存在如下关系：

$$ed\equiv 1 \bmod (p-1)(q-1)$$

相对应的公开密钥P_K包括公开密钥模数n=pq和公开密钥指数e。

8.4.2.1.2 签名功能

带有奇数公开密钥指数的RSA的签名功能定义如下：

$$S=Sign(SK)[X]:=X^d \bmod n,\ 0<X<n,$$

X是要签名的数据，S是相对应的数字签名。

8.4.2.1.3 恢复功能

带有奇数公开密钥指数的RSA的恢复功能定义如下：

$$X=Recover(P_K)[S]:=S^e \bmod n.$$

8.4.2.2 密钥的产生

对RSA密钥对的主要要求是保证模数是一个素数，即是一个不能通过有效的有特殊目的的因数分解算法分解的整数。

8.4.3 安全哈希算法（SHA-1）

SHA-1中输入任意长度的信息，产生一个20字节的哈希值。SHA-1算法见GB/T 18238.3。

本哈希算法的标志编码为16进制数'01'。

附 录 A
（资料性附录）
指令－状态字列表

表 A.1 指令状态字列表 1

SW1	SW2	状态字默认含义	CHANGE PIN	CREDIT FOR LOAD	DEBIT FOR PURCHASE /CASH WITHDRAW	DEBIT FOR UNLOAD	GET BALANCE	GET TRANSACTION PROVE	INITIALIZE FOR CASH WITHDRAW	INITIALIZE FOR LOAD	INITIALIZE FOR PURCHASE	INITIALIZE FOR UNLOAD	INITIALIZE FOR UPDATE	RELOAD PIN
61	XX[2]	正常处理												
62	00	无信息提供												
62	81	回送的数据可能有错												
62	82	文件长度<Le												
62	83	选择的文件无效												
62	84	FCI 格式与 P2 指定的不符												
63	00	认证失败												
63	CX[3]	验证失败，还剩下 X 次尝试机会	√											
64	00	状态标志位未变												
65	81	内存错误	√	√	√	√	√	√	√	√	√	√	√	√
67	00	长度错误		√	√	√				√		√	√	√
68	82	不支持安全报文												
69	00	不能处理												
69	01	命令不接受（无效状态）	√	√	√	√	√	√						
69	81	命令与文件结构不相容												
69	82	不满足安全状态												
69	83	验证方法锁定	√											
69	84	引用数据无效												√
69	85	使用条件不满足	√	√	√		√	√	√	√	√	√	√	√

[2] 'XX'表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
[3] 使用内部重试程序更新成功； X='0'表示不提供计数器； X!='0'表示重试次数

69	86	不满足命令执行的条件（非当前 EF）												
69	87	安全报文数据项丢失												
69	88	安全信息数据对象不正确												√
6A	80	数据域参数不正确	√											
6A	81	功能不支持								√				
6A	82	未找到文件												
6A	83	未找到记录												
6A	84	文件中存储空间不够												
6A	86	P1 和 P2 参数不正确	√				√			√		√	√	√
6A	88	引用数据找不到												√
6B	00	参数错误（偏移地址超出了 EF）												
6C	XX	长度错误（Le 错误；’XX’为实际长度）												
6F	00	数据无效												
90	00	成功执行，无错误	√	√	√	√	√	√	√	√	√	√	√	√
93	01	金额不足			√									
93	02	MAC 无效		√	√	√	√							
93	03	应用永久锁住												√
94	01	金额不足							√		√	√		
94	02	交易计数器到达最大值							√	√	√	√	√	
94	03	密钥索引不支持							√	√	√	√	√	
94	06	所需 MAC 不可用						√						
6E	00	不支持的类：CLA 错	√	√	√	√	√	√	√	√	√	√	√	√
6D	00	不支持的指令代码												
66	00	接收通讯超时	√	√	√	√	√	√	√	√	√	√	√	√
66	01	接收字符奇偶错	√	√	√	√	√	√	√	√	√	√	√	√
66	02	校验和不对												
66	03	当前 DF 文件无 FCI												
66	04	当前 DF 下无 SF 或 KF												

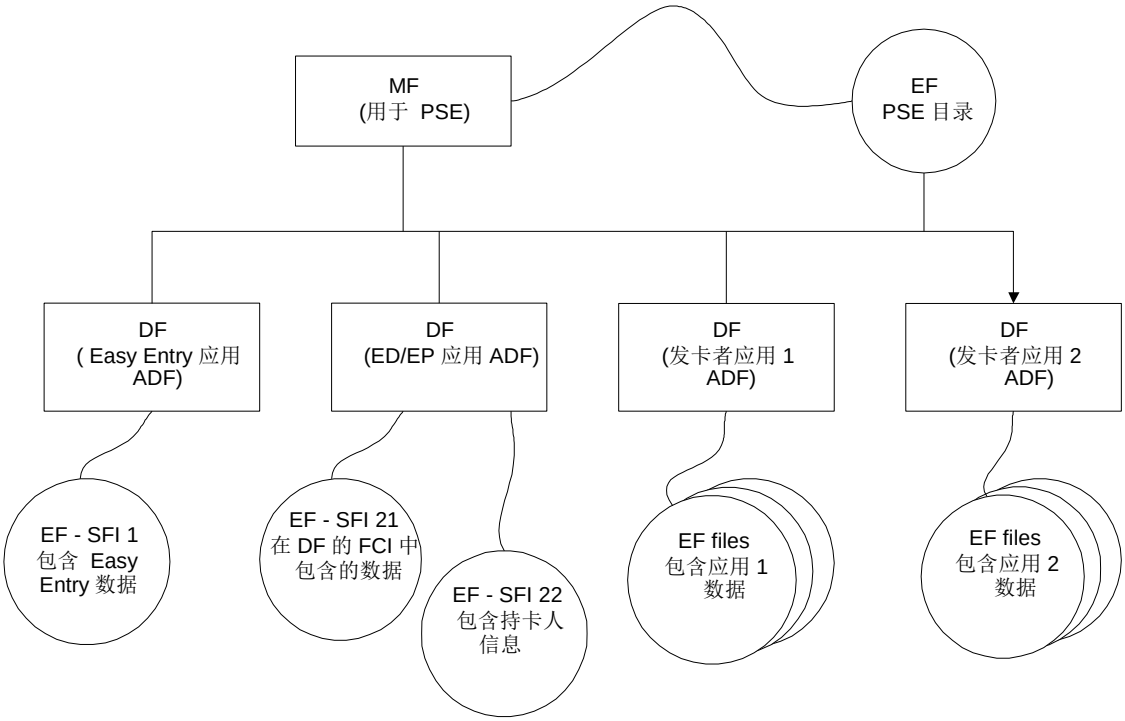
表 A.2 指令状态字列表 2

SW1	SW2	状态字 默认含义	UPDATE OVERDRAW LIMIT	APPLICATION BLOCK	APPLICATION UNBLOCK	CARD BLOCK	EXTERNAL AUTHENTICATION	GET RESPONSE	GET CHALLENGE	INTERNAL AUTHENTICATION	PIN CHANGE/UNBLOCK	READ BINARY	READ RECORD	SELECT	UPDATE BINARY	UPDATE RECORD	VERIFY
61	XX	正常处理						√									
62	00	无信息提供		√							√						
62	81	回送的数据可能有错		√				√		√	√	√	√				
62	82	文件长度<Le										√					
62	83	选择的文件无效		√										√			
62	84	FCI 格式与 P2 指定的不符												√			
63	00	认证失败					√										
63	CX	验证失败，还剩下 X 次尝试机会													√	√	√
64	00	状态标志位未变		√	√	√				√	√		√	√			√
65	81	内存错误	√	√	√	√					√				√	√	
67	00	长度错误	√				√（Lc 错误）	√		√		√（Lc 域为空）	√（Lc 域不存在）	√（P1 P2 与 Lc 不一致）	√（Lc 域为空）	√（Lc 域为空）	
68	82	不支持安全报文								√							
69	00	不能处理	√														
69	01	命令不接受（无效状态）	√														
69	81	命令与文件结构不相容										√	√		√	√	
69	82	不满足安全状态		√	√						√	√			√	√	
69	83	验证方法锁定					√										√
69	84	引用数据无效		√							√						√
69	85	使用条件不满足	√							√							
69	86	不满足命令执行的条件（非当前 EF）										√			√	√	
69	87	安全报文数据项丢失		√	√	√					√						
69	88	安全信息数据对象不正确		√	√	√					√						

6A	80	数据域参数不正确								√							
6A	81	功能不支持							√			√	√	√	√	√	
6A	82	未找到文件										√	√	√	√	√	
6A	83	未找到记录											√			√	
6A	84	文件中存储空间不够														√	
6A	86	P1 和 P2 参数不正确		√			√	√	√	√	√			√			√
6A	88	引用数据找不到		√							√						√
6B	00	参数错误（偏移地址超出了 EF）										√			√		
6C	XX	长度错误(Le 错误;'XX'为实际长度）						√				√					
6F	00	数据无效						√									
90	00	成功执行，无错误	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
93	01	金额不足															
93	02	MAC 无效	√														
93	03	应用永久锁住			√						√						
94	01	金额不足															
94	02	交易计数器到达最大值															
94	03	密钥索引不支持															
94	06	所需 MAC 不可用															
6E	00	不支持的类：CLA 错	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
6D	00	不支持的指令代码															
66	00	接收通讯超时	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
66	01	接收字符奇偶错	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
66	02	校验和不对															
66	03	当前 DF 文件无 FCI															
66	04	当前 DF 下无 SF 或 KF															

附 录 B
（资料性附录）
卡片结构示例

图B.1给出了一个卡片内部结构示例，该卡片支持电子存折、电子钱包、Easy entry以及两个没有定义的发卡方应用。图B.1仅仅是一个例子。可能有其他不限定卡中应用数目的卡片内部结构。



图B.1 卡片内部结构示例

参考文献

[1] EMV 支付系统集成电路卡规范：2004，第 1 册～第 4 册