社会保障（个人）卡规范
第 5 部分：命令

引言

本部分作为《社会保障（个人）卡规范》的第 5 部分，包括以下主要内容：

——命令概述：对于命令的基本格式做了说明，并对于本册中出现的命令和返回的状态码做了总结。

——基本命令：是 ISO/IEC 7816 定义的基本指令，文中对于指令的格式、定义、响应和状态码都做了说明。

——专有命令：是针对社会保障应用定义的一系列的指令，文中对于指令的格式、定义、响应和状态码都做了说明。

1 适用范围

本规范适用于人力资源和社会保障领域面向各类参保人员发行的社会保障卡。其使用对象主要是与社会保障卡应用相关的卡片设计、制造、管理、发行和受理以及应用系统的研制、开发、集成和维护等组织机构。

2 参考标准

ISO/IEC 7816-4：1995	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/IEC 7816-5：1994	识别卡　带触点的集成电路卡　第 5 部分：应用标识符的编号系统和注册程序
ISO/IEC 9797．1：1997	信息技术　安全技术　电文鉴别代码（MACS）　第 1 部分：用块密码的机制
ISO/IEC 9797．2：2002	信息技术　安全技术　电文鉴别代码（MACS）　第 2 部分：专用散列函数的机械结构
ISO/IEC 10116：2006	信息技术　安全技术　n 位块加密算法的运算方法

3 定义

3.1 终端（Terminal）

为处理社会保障卡业务而在服务网点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其他部件和接口，例如与主机通信的接口。

3.2 命令（Command）

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.3 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。

3.4 交易（Transaction）

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.5　功能（Function）

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.6　集成电路（Integrated Circuit， IC）

设计用于完成处理和/或存储功能的电子器件。

3.7　集成电路卡（IC 卡）（Integrated Circuit（s） Card）

内部封装一个或多个集成电路的 ID-1 型卡。

3.8　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。

3.9　报文鉴别代码（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性。

3.10　半字节（Nibble）

一个字节的高四位或低四位。

3.11　明文（Plain Text）

没有加密的信息。

3.12　密文（Cipher Text）

通过密码系统产生的不可理解的文字或信号。

3.13　密钥（Key）

控制加密转换操作的符号序列。

3.14　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。

3.15　帐户划入（Wipe In Account）

将持卡人基本医疗保险个人帐户上尚未写入卡内的资金额度写到卡内基本医疗保险个人帐户中。

3.16　医疗消费（Medical Treatment Consume）

指持卡人就医、取药等与医疗有关的消费，从资金来源上划分，包括帐户支付、现金支付、统筹基金支付。卡内记录帐户支付、个人自付和统筹基金支付三种形式。

3.17　帐户支付（Account Payment）

指持卡人从卡内基本医疗保险个人帐户中支付医疗费用。

3.18　个人自付（Individual Payment）

指持卡人在医疗消费中，属于基本医疗保险统筹基金支付范围内的个人自付部分，包括现金支付和利用基本医疗保险个人帐户支付的金额。

3.19　统筹基金支付（Social-pooling Fund Payment）

指持卡人在医疗消费中，基本医疗保险统筹基金支付的金额。

3.20　支付年度（Year of Payment）

指卡内基本医疗保险统筹基金支付累计金额所对应的结算年度。

3.21　年度起始日期（Starting Day）

指卡内基本医疗保险统筹基金支付所对应的结算年度起始日期。

4 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

ADF	应用数据文件（Application Definition File）
AEF	应用基本文件（Application Elementary File）
AID	应用标识符（Application Identifier）
an	字母数字型（Alphanumeric）
ans	字母数字及特殊字符型（Alphanumeric Special）
APDU	应用协议数据单元（Application Protocol Data Unit）
ASN	抽象语法表示（Abstract Syntax Notation）
b	二进制（Binary）
BER	基本编码规则（Basic Encoding Rules）
C-APDU	命令 APDU（Command APDU）
CCYYMMDD	年、月、日（Year，Month，Day）
CLA	命令报文的类别字节（Class Byte of the Command Message）
cn	压缩数字（Compressed Numeric）
C-TPDU	命令 TPDU（Command TPDU）
DDF	目录定义文件（Directory Definition File）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
hex	十六进制数（Hexadecimal）
HHMM	时、分（Hours， Minutes）
HHMMSS	时、分、秒（Hours， Minutes， Seconds）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
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	终端发出的命令数据的实际长度（Exact Length of Data Sent by the TAL in a Case 3 or 4 Command）
Le	响应数据的最大期望长度（Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command）
Licc	IC 卡回送的可用数据的实际长度（Exact Length of Data Available in the ICC to be Returned in Response to the Case 2 or 4 Command Received by the ICC）
LEN	长度（Length）
Lr	响应数据域的长度（Length of Response Data Field）

M	必备型（Mandatory）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Master File）
n	数字型（Numeric）
O	可选型（Optional）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
P3	参数 3（Parameter 3）
PIN	个人密码（Personal Identification Number）
PIX	专用应用标识符扩展码（Proprietary Application Identifier Extension）
R-APDU	响应 APDU（Response APDU）
RFU	保留为将来使用（Reserved for Future Use）
RID	已注册的应用提供者标识（Registered Application Provider Identifier）
R-TPDU	响应 TPDU（Response TPDU）
SFI	短文件标识符（Short File Identifier）
SSA	社会保障应用（Social Security Application）
SSSE	社会保障系统环境（Social Security System Environment）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TLV	标签、长度、值（Tag Length Value）
TPDU	传输协议数据单元（Transport Protocol Data Unit）
A=B	A 等于 B
CIA	卡内医疗保险个人帐户（Individual Account for Medical Treatment on Card ）
SPFP	统筹基金支付累计（Social-pooling Fund Payment）
SPIP	个人自付累计（Accumulative Total of Individual Payment）
SSSE	社会保障系统环境（Social Security System Environment）
TAC	交易验证码（Transaction Authorization Cryptogram）
‘0’-‘9’ ‘A’-‘F’	十六进制数字
xx	任意值

5 命令概述

5.1 命令 APDU 格式

命令 APDU 由 4 字节长的必备头后跟一个可变长的条件体组成，见表 1：

表 1 命令 APDU 的结构

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

命令 APDU 中发送的数据字节数用 Lc（命令数据域的长度）表示。

响应 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）。

命令 APDU 报文的内容见表 2。

表 2　命令 APDU 的内容

代码	描　　述	长度
CLA	命令类别	1
INS	指令代码	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

5.2　响应 APDU 格式

响应 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，见表 3：

表 3　响应 APDU 的结构

Data	SW1	SW2
<———条件体——>	<———尾——>	

响应报文的详细内容见表 4：

表 4　响应 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

5.3　命令说明

本规范描述命令包括基本命令和专有命令两类。

基本命令包括：

APPLICATION BLOCK（应用锁定）

CARD BLOCK（卡片锁定）

CHANGE PIN（修改个人密码）

EXTERNAL AUTHENTICATION（外部鉴别）

GET RESPONSE（获取响应）

GET CHALLENGE（获取随机数）

INTERNAL AUTHENTICATION（内部鉴别）

PIN CHANGE/UNBLOCK（个人密码修改/解锁）

READ BINARY（读取二进制数据）

READ RECORD（读取记录内容）

SELECT（选择文件）

UPDATE BINARY（更新二进制数据）

UPDATE RECORD（更新记录内容）

VERIFY（校验个人密码）

专有命令包括：

CREDIT FOR LOAD（帐户划入）

DEBIT FOR PURCHASE（医疗消费）

GET BALANCE（读取卡内基本医疗保险个人帐户余额/年度个人自付累计金额/年度统筹基金支付累计金额）

GET TRANSACTION PROOF（取交易认证码）

INITIALIZE FOR LOAD（帐户划入初始化）

INITIALIZE FOR PURCHASE（医疗消费初始化）

UPDATE STARTING DAY（修改年度起始日期）

GET STARTING DAY （读取年度起始日期）

5.4 状态返回码

本规范中定义的指令的返回状态码，见表 5 所示。

表 5 指令返回码总表

SW1	SW2	含 义
‘61’	‘xx’	正常处理，‘xx’表示可以通过后续的“GET RESPONSE”命令得到的额外数据长度
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’）
‘65’	‘81’	内存错误
‘67’	‘00’	LC 错
‘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（无当前基本文件）
‘69’	‘88’	安全报文数据项不正确
‘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’	‘86’	P1、P2 错
‘6A’	‘88’	未找到引用数据
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6D’	‘00’	命令不存在

续表

SW1	SW2	含　义
‘6E’	‘00’	CLA 错
‘6F’	‘00’	数据无效
‘93’	‘02’	MAC 无效
‘93’	‘03’	应用被永久锁定
‘94’	‘01’	金额不足
‘94’	‘02’	交易计数器达到最大值
‘94’	‘03’	密钥索引不支持
‘94’	‘06’	所需 MAC 不可用

6　基本命令

6.1　APPLICATION BLOCK 命令

6.1.1　定义和范围

“APPLICATION BLOCK”命令使当前选择的应用失效。

当“APPLICATION BLOCK”命令成功地完成后，用“SELECT”命令选择已失效的应用，将回送状态码 ‘9303’（应用被永久锁定）。

对其他命令的影响根据不同应用而定。

6.1.2　命令报文

“APPLICATION BLOCK”命令报文编码见表 6。

表 6　APPLICATION BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘1E’
P1	‘00’
P2	‘01’
Lc	‘04’
Data	报文鉴别代码（MAC）数据元，根据本规范第 4 分册中的规定进行编码
Le	不存在

此命令执行成功后将永久锁定应用。

6.1.3　命令报文数据域

命令报文数据域包括根据《社会保障（个人）卡规范》第 4 部分：安全机制中的规定进行编码的报文鉴别码（MAC）数据元。

6.1.4　响应报文数据域

响应报文数据域不存在。

6.1.5　响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 7 所示：

表 7　APPLICATION BLOCK 错误状态

SW1	SW2	含　义
‘65’	‘81’	内存失败
‘67’	‘00’	LC 错
‘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
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1、P2 错
‘6A’	‘81’	功能不支持
‘6A’	‘88’	未找到引用数据
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.2　CARD BLOCK 命令

6.2.1　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码‘6A81’（功能不被支持），且不执行任何其他操作。

6.2.2　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’
P2	‘00’
Lc	‘04’
Data	报文鉴别代码（MAC）数据元，根据本规范第 4 分册中的规定进行编码
Le	不存在

6.2.3　命令报文数据域

命令报文数据域包括根据《社会保障（个人）卡规范》第 4 部分：安全机制中的规定进行编码的报文鉴别代码（MAC）数据元。

6.2.4　响应报文数据域

响应报文数据域不存在。

6.2.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 9 所示：

表 9　CARD BLOCK 错误状态

SW1	SW2	含　　义
‘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’	‘85’	使用条件不满足
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘81’	功能不支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6A’	‘88’	未找到引用数据
‘6E’	‘00’	CLA 错

6.3　CHANGE PIN 命令

6.3.1　定义和范围

“CHANGE PIN”允许持卡人将当前个人密码修改为新的密码。

当“CHANGE PIN”命令成功完成后，卡片要进行以下操作：

密码尝试计数器复位至密码尝试次数的上限；

将原个人密码置为新的个人密码。

此命令中的个人密码（PIN）值以明文方式传送。命令数据中个人密码（PIN）是以 cn 格式存放的，它不需要整字节的填充，只有最低有效字节的低半字节可能需要填充，且填以‘F’。有效的 PIN 至少是 4 个阿拉伯数字。

6.3.2　命令报文

“CHANGE PIN”命令报文见表 10：

表 10　CHANGE PIN 命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘01’
P2	‘00’
Lc	‘03’~‘11’
Data	当前 PIN ‖ ‘FF’ ‖ 新的 PIN
Le	不用

6.3.3　命令报文数据域

如果当前未使用 PIN 或更改后不再使用 PIN，则命令数据域中的‘当前 PIN’或‘新的 PIN’可以不存在。

6.3.4　响应报文数据域

响应报文数据域不存在。

6.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码见表 11 所示。

表 11 CHANGE PIN 警告状态

SW1	SW2	含 义
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’）

IC 卡可能回送的错误状态码见表 12 所示：

表 12 CHANGE PIN 错误状态

SW1	SW2	含 义
‘65’	‘81’	内存错误
‘67’	‘00’	Lc 不正确
‘69’	‘83’	验证方法锁定
‘6A’	‘80’	数据域参数不正确
‘6A’	‘81’	功能不支持
‘6A’	‘86’	参数 P1、P2 不正确
‘93’	‘03’	应用被永久锁定
‘6E’	‘00’	CLA 错

6.4 EXTERNAL AUTHENTICATION 命令

6.4.1 定义和范围

“EXTERNAL AUTHENTICATION”命令要求 IC 卡中的应用验证接口设备中保密模块的有效性，以使接口设备获得某种授权。

IC 卡的响应包括命令处理状态的回送。

6.4.2 命令报文

“EXTERNAL AUTHENTICATION”命令报文编码见表 13：

表 13 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	密钥标识符（见表 14）
Lc	‘10’～‘11’
Data	鉴别用数据
Le	不存在

表 14 定义了命令报文中的密钥标识符。

表 14　密钥标识符的结构

b7	b6	b5	b4	b3	b2	b1	b0	含　　义
0	0	0	0	0	0	0	0	保留密钥。
0								全局参考数据
1								专用参考数据
				x	x	x	x	密钥号

6.4.3　命令报文数据域

命令报文数据域中包含 16-17 个字节的数据：

——第 1 至第 8 个字节为鉴别数据；

——第 9 至第 16 个字节是鉴别所需的原始信息；

——第 17 个字节是可选的，表示密钥版本。

其中，鉴别数据根据《社会保障（个人）卡规范》第 4 部分：安全机制中的规定进行编码。

6.4.4　响应报文数据域

响应报文数据域不存在。

6.4.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码见表 15 所示。

表 15　EXTERNAL AUTHENTICATION 警告状态

SW1	SW2	含　　义
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’）

IC 卡可能回送的错误状态码见表 16 所示：

表 16　EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	含　　义
‘65’	‘81’	内存错误
‘67’	‘00’	Lc 不正确
‘69’	‘83’	鉴别方法锁定
‘69’	‘84’	引用数据无效
‘6A’	‘81’	功能不支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6A’	‘88’	密钥未找到
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.5　GET CHALLENGE 命令

6.5.1　定义和范围

“GET CHALLENGE”命令请求一个用于安全相关过程（例如：安全报文、安全鉴别）的随机数。此随机数只能在当前应用下使用一次。

6.5.2 命令报文

“GET CHALLENGE”命令报文编码见表 17：

表 17 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’或‘10’

6.5.3 命令报文数据域

命令报文数据域不存在。

6.5.4 响应报文数据域

响应报文数据域包括随机数，长度为 4 或 8 或 16 字节。

6.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 18 所示：

表 18 GET CHALLENGE 错误状态

SW1	SW2	含 义
‘67’	‘00’	Le 长度错
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.6 GET RESPONSE 命令

6.6.1 定义和范围

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。

6.6.2 命令报文

“GET RESPONSE”命令报文编码见表 19：

表 19 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

6.6.3 命令报文数据域

命令报文数据域不存在。

6.6.4 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 0，在附加数据有效时，卡片必须回送状态码‘6Cxx’， 否则回送状态码‘6F00’。

6.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码见表 20 所示：

表 20 GET RESPONSE 警告状态

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

IC 卡可能回送的错误状态码见表 21 所示：

表 21 GET RESPONSE 错误状态

SW1	SW2	含 义
‘67’	‘00’	长度错误（Le 不正确）
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6C’	‘xx’	长度错误（Le 不正确，‘xx’表示实际长度）
‘6E’	‘00’	CLA 错
‘6F’	‘00’	数据无效
‘93’	‘03’	应用被永久锁定

6.7 INTERNAL AUTHENTICATION 命令

6.7.1 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鉴别的功能。

当有关的密钥位于 MF 层时，该命令可以用来鉴别整个卡片；当有关的密钥位于 DF 时，该命令可以用来鉴别特定的应用。

6.7.2 命令报文

“INTERNAL AUTHENTICATION”命令报文编码见表 22：

表 22 INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	‘00’
Lc	‘10’~‘11’
Data	鉴别用数据
Le	‘00’

6.7.3 命令报文数据域

命令报文数据域的内容是卡片或应用专用的鉴别数据，包含 16-17 个字节的数据：

——第 1 至第 8 个字节是过程密钥计算使用的数据；

——第 9 至第 16 个字节是鉴别所需的原始信息；

——第 17 个字节是可选的，表示密钥版本。

6.7.4 响应报文数据域

响应报文数据域内容是相关的鉴别数据，其值根据《社会保障（个人）卡规范》第 4 部分：安全机制中的规定进行编码。。

6.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 23 所示：

表 23 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
‘67’	‘00’	Lc 不正确
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6A’	‘88’	密钥未找到
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.8 PIN CHANGE/UNBLOCK 命令

6.8.1 定义和范围

该命令让发卡方解锁个人密码（即重置个人密码尝试计数器的值为应用设定的最大次数），或者更改个人密码。

命令中个人密码的传递采用加密方式。

6.8.2 命令报文

“PIN CHANGE/UNBLOCK”命令报文编码见表 24：

表 24 PIN CHANGE/UNBLOCK 命令报文

代码	值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	见表 25
Lc	数据域长度
Data	加密的个人密码数据元和报文鉴别代码（MAC）数据元，根据《社会保障（个人）卡规范》第 4 部分：安全机制的规定进行编码
Le	不存在

表 25 定义了命令报文中的控制参数。

表 25　PIN CHANGE/UNBLOCK 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　　义
0	0	0	0	0	0	0	0	解锁个人密码。仅重置尝试计数器，并不更改个人密码。
0	0	0	0	0	0	0	1	更改个人密码。重置尝试计数器并以新 PIN 取代原 PIN。

6.8.3　命令报文数据域

表 26 给出了 Lc 值与数据域内容的关系。

表 26　Lc 值与数据域内容的对应关系

操作	Lc 值	数据域内容
解锁个人密码	‘04’	Lc 应包括 MAC 数据元的长度。
更改个人密码	‘0C’或‘14’	Lc 应同时包括被加密的个人密码数据元和 MAC 数据元的长度。

个人密码数据元和 MAC 数据元根据《社会保障（个人）卡规范》第 4 部分：安全机制的规定进行编码。

当被加密的个人密码数据元长度为零时，卡片应使卡片内部已存在的有效的 PIN 置为空的 PIN。

6.8.4　响应报文数据域

响应报文数据域不存在。

6.8.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 27 所示：

表 27　PIN CHANGE/UNBLOCK 错误状态

SW1	SW2	含　　义
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 不正确
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘85’	不满足使用条件
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘80’	数据域参数不正确
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	参数 P1、 P2 不正确
‘6A’	‘88’	未找到引用数据
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.9 READ BINARY 命令

6.9.1 定义和范围

“READ BINARY”命令用于读取透明文件的内容（或部分内容）。

6.9.2 命令报文

“READ BINARY”命令报文编码见表 28：

表 28 READ BINARY 命令报文

代码	值
CLA	‘00’
INS	‘B0’
P1	见表 29
P2	
Lc	不存在
Data	不存在
Le	‘00’或要读出的数据的长度

表 29 定义了命令报文中的引用控制参数。

表 29 READ BINARY 命令引用控制参数

P1								P2								含 义
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0	x	x	x	x	x	y	y	y	y	y	y	y	y	xxxxx 表示短文件标识符 SFI，yyyyyyyy 为要读的首字节距离文件首字节的偏移量。
0	x	x	x	x	x	x	x	y	y	y	y	y	y	y	y	P1×256+P2 为要读的首字节距离文件首字节的偏移量。

6.9.3 命令报文数据域

命令报文数据域不存在。

6.9.4 响应报文数据域

当 Le 的值为 0 时，读出自要读的首字节起的 256 个字节；如果在读出 256 个字节前已到达文件最后一个字节，则自要读的首字节起的全部字节将被读出。

6.9.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 30 所示：

表 30 READ BINARY 的错误状态码

SW1	SW2	含 义
‘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（无当前基本文件）
‘6A’	‘81’	功能不被支持
‘6A’	‘82’	未找到文件

续表

SW1	SW2	含　义
‘6A’	‘86’	参数 P1、 P2 不正确
‘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）
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.10 READ RECORD 命令

6.10.1 定义和范围

“READ RECORD”命令读取记录结构的基本文件中一些指定的记录或一个记录起始部分的数据。

IC 卡的响应由回送记录组成。

6.10.2 命令报文

“READ RECORD”命令报文编码见表 31：

表 31 READ RECORD 命令报文

代码	值
CLA	‘00’
INS	‘B2’
P1	记录号或记录标识符
P2	引用控制参数（见表 32）
Lc	不存在
Data	不存在
Le	‘00’或要读出的数据的长度

记录号的取值范围为‘01’-‘FE’，‘00’表示当前记录。

表 32 定义了命令报文中的引用控制参数。

表 32 READ RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
0	0	0	0	0	-	-	-	对当前文件进行操作
x	x	x	x	x	-	-	-	短文件标识符 SFI
-	-	-	-	-	1	0	0	读 P1 指定的记录
-	-	-	-	-	1	0	1	从 P1 指定的记录开始读到最后一个记录
-	-	-	-	-	1	1	0	从最后一个记录开始读到 P1 指定的记录
-	-	-	-	-	0	0	0	读具有 P1 指定的记录标识符的第一个实例
-	-	-	-	-	0	0	1	读具有 P1 指定的记录标识符的最后一个实例
-	-	-	-	-	0	1	0	读具有 P1 指定的记录标识符的下一个实例
-	-	-	-	-	0	1	1	读具有 P1 指定的记录标识符的上一个实例

6.10.3 命令报文数据域

命令报文数据域不存在。

6.10.4 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。

READ RECORD 当 Le=00 时，应以 6Cxx 返回可读的实际长度。

6.10.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 33 所示：

表 33 READ RECORD 错误状态

SW1	SW2	含 义
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	命令不允许使用（无当前基本文件）
‘6A’	‘81’	功能不被支持
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘86’	参数 P1、P2 不正确
‘6C’	‘xx’	长度错误（Le 错误；‘xx’为实际长度）
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.11 SELECT 命令

6.11.1 定义和范围

“SELECT”命令通过文件名或 AID、文件标识符来选择 IC 卡中的 SSSE、DDF 或 ADF，通过文件标识符来选择 ADF 中的 AEF。应用选择在《社会保障（个人）卡规范》第 3 部分：文件系统和应用选择中描述。

本指令定义适用于MF和SSSE，PSE、PPSE下的SELECT命令由JR/T0025规定。

命令执行成功后，SSSE、DDF 或 ADF、AEF 的路径被设定。

除选择 AEF 外， IC 卡的响应报文应由回送的 FCI 组成。

在当前 DF 未被改变时，该 DF 下的所有安全状态应被保持。

6.11.2 命令报文

“SELECT”命令报文编码见表 34：

表 34 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表 35）
P2	‘00’第一个或唯一一个文件实例 ‘02’下一个文件实例
Lc	‘05’-‘10’（使用文件名或 AID 时）或‘02’（使用文件标识符时）或‘00’
Data	文件名、AID、文件标识符或不存在

Le	‘00’

表 35 定义了命令报文中的引用控制参数。

表 35　SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　　义
0	0	0	0	0	0	0	0	用文件标识符选择 MF、DF（数据域=文件标识符或空）
0	0	0	0	0	0	1	0	用文件标识符在当前 DF 下选择 EF（数据域=EF 的文件标识符）
0	0	0	0	0	1	0	0	通过文件名选择 DF（数据域=DF 的文件名）

如果 P1=‘00’并且数据域为空或等于‘3F00’，该命令将选择主控文件（MF）。

6.11.3　命令报文数据域

命令报文数据域可能是文件名、AID、文件标识符或不存在。该命令在 MF 下时，DDF 名称可以为 JR/T0025 规定的 PSE 或 PPSE，或本规范规定的 SSSE。

6.11.4　响应报文数据域

除选择 AEF 外，响应报文中数据域应包括所选择的 SSSE、DDF 或 ADF 的 FCI。表 3 6 到表 3 8 规定了所用的标志。本规范不规定 FCI 中回送的附加标志。选择 PSE 或 PPSE 后的响应 FCI 由 JR/T0025 规定。

表 36 定义了成功选择 SSSE 后回送的 FCI。

表 36　SELECT SSSE 的响应报文（FCI）

标志			值	存在方式
‘6F’			FCI 模板	M
	‘84’		DF 名	M
	‘A5’		FCI 专用模板	M
		‘88’	目录基本文件的 SFI	O
		‘9F0C’	发卡方自定义 FCI 数据	O

表 37 定义了成功选择 DDF 后回送的 FCI。

表 37　SELECT DDF 的响应报文（FCI）

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

表 38 定义了成功选择 ADF 后回送的 FCI。

表 38　SELECT ADF 的响应报文（FCI）

标志		值	存在方式
‘6F’		FCI 模板	M
	‘84’	DF 名	M

6.11.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

IC卡是否支持使用部分DF名进行DF文件选择不作强制规定。但是，如果IC卡支持部分名称选择，那么它应该遵守下列规则：

当一个 DF 成功选中后，终端重复发出选择(SELECT)命令，且 P2 设置为选择下一个文件的选项(参见表 41)及使用相同的部分 DF 名时，卡片应该选中与部分 DF 名称匹配的不同的 DF 文件(如果这样的 DF 存在)。在没有应用层命令干扰的情况下重复发出相同的选择(SELECT)命令，卡片应该可以找到所有满足条件的 DF 文件，且每个文件不会被找到两次。当所有满足条件的 DF 都被选择后，再发出同样的选择(SELECT)命令，应该得到没有文件被选择的结果，卡片应该响应 SW1SW2='6A82'(文件未找到)。

IC 卡可能回送的错误状态码见表 39 所示：

表 39　SELECT 错误状态

SW1	SW2	含　　义
'67'	'00'	P1、P2 与 Lc 不一致
'6A'	'81'	功能不被支持
'6A'	'82'	未找到文件
'6A'	'86'	参数 P1、P2 不正确
'6E'	'00'	CLA 错
'93'	'03'	应用被永久锁定

6.12　UPDATE BINARY 命令

6.12.1　定义和范围

"UPDATE BINARY"命令报文使用命令 APDU 中给定的数据写入或修改透明结构的基本文件的全部或部分数据。

6.12.2　命令报文

"UPDATE BINARY"命令报文编码见表 40：

表 40　UPDATE BINARY 命令报文

代码	值
CLA	'00'或'04'
INS	'D6'
P1	见表 41
P2	
Lc	后续数据域的长度
Data	写入或修改用的数据
Le	不存在

表 41 定义了命令报文中的引用控制参数。

表 41　UPDATE BINARY 命令引用控制参数

P1								P2								含　　义
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	

1	0	0	X	X	X	X	X	Y	Y	Y	Y	Y	Y	Y	Y	xxxxx 表示短文件标识符 SFI，yyyyyyyy 为要写入或修改的首字节距离文件首字节的偏移量。
0	X	X	X	X	X	X	X	Y	Y	Y	Y	Y	Y	Y	Y	P1×256+P2 为要写入或修改的首字节距离文件首字节的偏移量。

6.12.3 命令报文数据域

命令报文数据域包括用来写入或更新原有数据的新数据。

6.12.4 响应报文数据域

响应报文数据域不存在。

6.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 42 所示：

表 42 UPDATE BINARY 错误状态

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	Lc 长度错误
‘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（无当前基本文件）
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	参数 P1、 P2 不正确
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.13 UPDATE RECORD 命令

6.13.1 定义和范围

“UPDATE RECORD”命令报文用命令 APDU 中给定的数据添加记录或更改指定记录。

对线性结构文件来说，当指定的记录号不存在时，可按记录号顺序添加记录。按记录标识符访问的记录不存在时，也应视为添加新的记录。

对循环结构文件来说，当使用“P1 指定标识的上一个实例”命令选项时应视为添加新的记录。

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。

6.13.2 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	记录号或记录标识符（‘00’，表示当前记录）
P2	见表 44
Lc	Data 域数据长度
Data	添加的或更新原有记录的新记录
Le	不存在

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
0	0	0	0	0	-	-	-	当前的 EF 文件
x	x	x	x	x	-	-	-	用 SFI 方式
-	-	-	-	-	1	x	x	利用 P1 中的记录号
-	-	-	-	-	1	0	0	P1 记录号
-	-	-	-	-	0	x	x	利用 P1 中的记录标识符
-	-	-	-	-	0	0	0	P1 指定标识的第一个实例
-	-	-	-	-	0	0	1	P1 指定标识的最后一个实例
-	-	-	-	-	0	1	0	P1 指定标识的下一个实例
-	-	-	-	-	0	1	1	P1 指定标识的上一个实例
其余值								RFU

6.13.3　命令报文数据域

命令报文数据域由添加的或更新原有记录的新记录组成。

6.13.4　响应报文数据域

响应报文数据域不存在。

6.13.5　响应报文状态码

命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 45 所示：

表 45　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’	‘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）
‘69’	‘88’	安全报文数据项不正确

‘6A’	‘81’	功能不被支持
‘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’	‘85’	Lc 与 TLV 结构不符
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

6.14 VERIFY 命令

6.14.1 定义和范围

“VERIFY”命令用于校验命令数据域中的个人密码的正确性。

6.14.2 命令报文

“VERIFY”命令报文编码见表 46：

表 46 VERIFY 命令报文

代码	值
CLA	‘00’
INS	‘20’
P1	‘00’
P2	‘00’
Lc	‘00’或‘02’~‘08’
Data	外部输入的个人密码或空
Le	不存在

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密码。

6.14.3 命令报文数据域

命令报文数据域不为空时由持卡者输入的个人密码组成。

6.14.4 响应报文数据域

响应报文数据域不存在。

6.14.5 响应报文状态码

当命令报文数据域不为空时，此命令执行成功的状态码是‘9000’。命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败时（包括卡中存放的个人密码为空的情况），IC 卡将回送 SW1SW2=‘63Cx’，‘x’表示个人密码允许重试的次数；当卡回送‘63C0’时，表示不能重试个人密码。此时再使用 VERIFY 命令时，将回送失败状态码 SW1 SW2=‘6983’。

当命令报文数据域为空时，如果卡中存放的个人密码不为空，则 IC 卡将回送 SW1 SW2=‘63Cx’，‘x’表示个人密码允许重试的次数，个人密码的重试次数不变；否则，IC 卡将回送状态码‘9000’。

IC 卡可能回送的警告状态码见表 47 所示。

表 47 VERIFY PIN 警告状态

SW1	SW2	含　　义
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数

IC 卡可能回送的错误状态码见表 48 所示：

表 48　VERIFY 错误状态

SW1	SW2	含　　义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	个人密码锁定
‘69’	‘84’	引用数据无效
‘6A’	‘81’	功能不被支持

续表

SW1	SW2	含　　义
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据
‘6E’	‘00’	CLA 错
‘93’	‘03’	应用被永久锁定

7　专有命令

本规范定义的专有命令，用于医疗保险应用，在应用执行过程中，针对医疗保险应用来说卡片处于以下状态之一：

空闲状态；

帐户划入状态；

医疗消费状态。

在一种状态下，只有某些指令能够执行。应用选择完成后，卡片首先进入空闲状态。当卡片从终端接收到一条命令时，它必须首先检查当前状态是否允许执行该命令。在命令执行成功后，卡片进入另一个状态（或同一个）。如果命令执行不成功，则卡片进入空闲状态。

下表说明了命令执行成功后的状态变化。第 1 行表示命令发出时卡片的当前状态，第 1 列表示发出的命令，整张表给出的是在当前状态下某个命令执行成功后的状态。阴影部分表示在卡片处于相应状态时发出此命令是无效的。在这种情况下，卡片不执行该命令，返回‘6901’状态码，同时卡片的状态变为空闲。见表 49 描述。

表 49　命令执行成功后的状态变化

当前状态 / 命令	空闲	帐户划入	医疗消费
INITIALIZE FOR LOAD	帐户划入	帐户划入	帐户划入
INITIALIZE FOR PURCHASE	医疗消费	医疗消费	医疗消费
CREDIT FOR LOAD	不允许	空闲	不允许
DEBIT FOR PURCHASE	不允许	不允许	空闲
GET BALANCE	空闲	帐户划入	医疗消费
GET TRANSACTION PROOF	空闲	帐户划入	医疗消费

7.1 CREDIT FOR LOAD 命令

7.1.1 定义和范围

“CREDIT FOR LOAD”命令用于帐户划入。在执行“CREDIT FOR LOAD”命令之前，必须成功执行“INITIALIZE FOR LOAD”命令。

7.1.2 命令报文

“CREDIT FOR LOAD”命令报文编码见表 50。

表 50 CREDIT FOR LOAD 命令报文

代码	值
CLA	‘B0’
INS	‘2A’
P1	‘00’
P2	‘00’
Lc	‘0B’
Data	见表 51
Le	‘04’

7.1.3 命令报文数据域

表 51 定义了“CREDIT FOR LOAD” 命令报文数据域。

表 51 CREDIT FOR LOAD 命令报文数据域

说明	长度（字节）
交易时间（主机）	‘07’
MAC2	‘04’

7.1.4 响应报文数据域

“CREDIT FOR LOAD”响应报文数据域见表 52。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

表 52 CREDIT FOR LOAD 响应报文数据域

说明	长度（字节）
TAC	‘04’

7.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 53 描述了 IC 卡可能回送的错误状态。

表 53 CREDIT FOR LOAD 错误状态

SW1	SW2	含 义
‘65’	‘81’	EEPROM 损坏，导致卡锁定
‘67’	‘00’	Lc 长度错
‘69’	‘01’	命令不接受（无效状态）

‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘02’	MAC 无效
‘93’	‘03’	应用被永久锁定

7.2 DEBIT FOR PURCHASE 命令

7.2.1 定义和范围

“DEBIT FOR PURCHASE”命令用于医疗消费。在执行“DEBIT FOR PURCHASE”命令之前，必须成功执行“INITIALIZE FOR PURCHASE”命令。

7.2.2 命令报文

“DEBIT FOR PURCHASE”命令报文编码见表 54：

表 54 DEBIT FOR PURCHASE 命令报文

代码	值
CLA	‘B0’
INS	‘2C’
P1	‘01’
P2	‘00’
Lc	‘0F’
Data	见表 55
Le	‘08’

7.2.3 命令报文数据域

表 55 定义了“DEBIT FOR PURCHASE”命令报文数据域。

表 55 DEBIT FOR PURCHASE 命令报文数据域

说明	长度（字节）
终端交易序号	‘04’
交易时间	‘07’
MAC1	‘04’

7.2.4 响应报文数据域

此命令执行成功的响应报文数据域见表 56。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

表 56 DEBIT FOR PURCHASE 响应报文数据域

说明	长度（字节）
TAC	‘04’
MAC2	‘04’

7.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 57 描述了 IC 卡可能回送的错误状态。

表 57 DEBIT FOR PURCHASE 错误状态

SW1	SW2	含　　义
‘65’	‘81’	EEPROM 损坏，导致卡锁定
‘67’	‘00’	Lc 长度错
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘02’	MAC 无效
‘93’	‘03’	应用被永久锁定

7.3 GET BALANCE 命令

7.3.1 定义和范围

“GET BALANCE”命令用于读取卡内基本医疗保险个人帐户（CIA）余额/年度个人自付累计金额（SPIP）/年度统筹基金支付累计金额（SPFP）。该命令需验证个人密码（PIN）（如果持卡人设置）。

7.3.2 命令报文

“GET BALANCE”命令报文编码见表 58：

表 58　GET BALANCE 命令报文

代码	值
CLA	‘B0’
INS	‘26’
P1	‘00’
P2	‘01’：用于 CIA； ‘02’：用于 SPIP； ‘03’：用于 SPFP； 其他值保留。
Lc	不存在
Data	不存在
Le	‘04’（P2=‘01’时）； ‘06’（P2=‘02’或‘03’时）。

7.3.3 命令报文数据域

命令报文数据域不存在。

7.3.4 响应报文数据域

此命令执行成功的响应报文数据域见表 59。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

表 59　GET BALANCE 响应报文数据域

说明	长度（字节）
CIA 余额/SPIP 金额/SPFP 金额	‘04’

支付年度（当 P2=‘02’或‘03’时存在）	‘02’

7.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 60 描述了 IC 卡可能回送的错误状态。

表 60 GET BALANCE 错误状态

SW1	SW2	含 义
‘67’	‘00’	Le 长度错
‘69’	‘82’	不满足安全状态
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持

续表

SW1	SW2	含 义
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定

7.4 GET TRANSACTION PROOF 命令

7.4.1 定义和范围

“GET TRANSACTION PROOF” 命令用于取交易认证码（TAC 和 MAC）。它提供了一种在交易处理过程中拔出并再次插卡后 IC 卡的恢复机制。该命令的用法在《社会保障（个人）卡规范》第 7 部分：应用流程中说明。

7.4.2 命令报文

“GET TRANSACTION PROOF” 命令报文编码见表 61。

表 61 GET TRANSACTION PROOF 命令报文

代码	值
CLA	‘B0’
INS	‘2E’
P1	‘00’
P2	要取的 MAC 和 TAC 所对应的交易类型标识
Lc	‘02’
Data	见表 62
Le	‘08’

7.4.3 命令报文数据域

表 62 定义了“GET TRANSACTION PROOF”命令报文数据域。

表 62 GET TRANSACTION PROOF 命令报文数据域

说明	长度（字节）
要取的 MAC 和 TAC 所对应的 CIA 划入或医疗消费交易序号	‘02’

7.4.4 响应报文数据域

如果命令中指定的交易类型标识和 CIA 划入或医疗消费交易序号对应的 MAC 或 TAC

可用，则响应报文数据域见表 63：

表 63　GET TRANSACTION PROOF 响应报文数据域

说明	长度（字节）
MAC	‘04’
TAC	‘04’

7.4.5　响应报文状态码

此命令执行成功的状态码是‘9000’。表 64 描述了 IC 卡可能回送的错误状态。

表 64　GET TRANSACTION PROOF 错误状态

SW1	SW2	含　义
‘67’	‘00’	Le 长度错
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定
‘94’	‘06’	所需 MAC 不可用

7.5　INITIALIZE FOR LOAD 命令

7.5.1　定义和范围

“INITIALIZE FOR LOAD”命令用于帐户划入的初始化。执行该命令后即选择了帐户划入交易，下一条应执行“CREDIT FOR LOAD”命令。“INITIALIZE FOR LOAD”命令仅对下一条命令有效。

7.5.2　命令报文

“INITIALIZE FOR LOAD”命令报文编码见表 65。

表 65　INITIALIZE FOR LOAD 命令报文

代码	值
CLA	‘B0’
INS	‘28’
P1	‘00’
P2	‘01’； 其他值保留。
Lc	‘0B’
Data	见表 66
Le	‘10’

7.5.3　命令报文数据域

表 66 定义了“INITIALIZE FOR LOAD” 命令报文数据域。

表 66　INITIALIZE FOR LOAD 命令报文数据域

说明	长度（字节）
密钥索引号	‘01’
交易金额	‘04’
终端机编号	‘06’

7.5.4　响应报文数据域

此命令执行成功的响应报文数据域见表 67。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

表 67　INITIALIZE FOR LOAD 响应报文数据域

说明	长度（字节）
CIA 余额	‘04’
CIA 划入交易序号	‘02’
密钥版本号	‘01’
算法标识	‘01’
伪随机数	‘04’
MAC1	‘04’

7.5.5　响应报文状态码

此命令执行成功的状态码是‘9000’。表 68 描述了 IC 卡可能回送的错误状态。

表 68　INITIALIZE FOR LOAD 错误状态

SW1	SW2	含　义
‘65’	‘81’	EEPROM 损坏，导致卡锁定
‘67’	‘00’	Lc 长度错
‘69’	‘82’	不满足安全状态
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定
‘94’	‘02’	交易计数器达到最大值
‘94’	‘03’	密钥索引不支持

7.6　INITIALIZE FOR PURCHASE 命令

7.6.1　定义和范围

“INITIALIZE FOR PURCHASE”命令用于医疗消费的初始化。执行该命令后即选择了医疗消费交易，下一条应执行“DEBIT FOR PURCHASE”命令。“INITIALIZE FOR PURCHASE”命令仅对下一条命令有效。

7.6.2 命令报文

“INITIALIZE FOR PURCHASE”命令报文编码见表 69。

表 69 INITIALIZE FOR PURCHASE 命令报文

代码	值
CLA	‘B0’
INS	‘28’
P1	‘01’
P2	‘01’； 其他值保留。
Lc	‘13’

续表

代码	值	
Data	见	
	密钥索引号	‘01’
	个人帐户支付金额	‘04’
	个人自付金额	‘04’
	70	
Le	‘16’	

7.6.3 命令报文数据域

表 70 定义了“INITIALIZE FOR PURCHASE”命令报文的数据域。

表 70 INITIALIZE FOR PURCHASE 命令报文数据域

说明	长度（字节）
密钥索引号	‘01’
个人帐户支付金额	‘04’
个人自付金额	‘04’
统筹基金支付金额	‘04’
终端机编号	‘06’

7.6.4 响应报文数据域

此命令执行成功的响应报文数据域见表 71。如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

表 71 INITIALIZE FOR PURCHASE 响应报文数据域

说明	长度（字节）
CIA 余额	‘04’
SPIP 金额	‘04’
SPFP 金额	‘04’
支付年度	‘02’
医疗消费交易序号	‘02’

密钥版本号	‘01’
算法标识	‘01’
伪随机数	‘04’

7.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 72 描述了 IC 卡可能回送的错误状态。

表 72 INITIALIZE FOR PURCHASE 错误状态

SW1	SW2	含 义
‘65’	‘81’	EEPROM 损坏，导致卡锁定
‘67’	‘00’	Lc 长度错
‘69’	‘82’	不满足安全状态
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定
‘94’	‘01’	金额不足
‘94’	‘02’	交易计数器达到最大值
‘94’	‘03’	密钥索引不支持

7.7 UPDATE STARTING DAY 命令

7.7.1 定义和范围

“UPDATE STARTING DAY”命令用于修改医疗保险帐户中的“年度起始日期”数据元。修改权限与在该应用下建立文件的权限相同。

使用该命令必须验证经过 DSK 密钥（DSK 密钥是专用于控制和更新年度起始日期的密钥）认证。

7.7.2 命令报文

“UPDATE STARTING DAY”命令报文编码见表 73：

表 73 UPDATE STARTING DAY 命令报文

代码	值
CLA	‘B0’
INS	‘56’
P1	‘00’
P2	‘00’

Lc	‘02’
Data	年度起始日期
Le	不存在

7.7.3 命令报文数据域

表 74 定义了“UPDATE STARTING DAY”命令报文数据域。

表 74 UPDATE STARTING DAY 命令报文数据域

说明	长度（字节）
年度起始日期（格式：mmdd）	‘02’

7.7.4 响应报文数据域

响应报文数据域不存在。

7.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 75 描述了 IC 卡可能回送的错误状态。

表 75 UPDATE STARTING DAY 错误状态

SW1	SW2	含 义
‘69’	‘82’	不满足安全状态
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定

7.8 GET STARTING DAY 命令

7.8.1 定义和范围

“GET STARTING DAY”命令用于读取医疗保险帐户中的“年度起始日期”数据元。

7.8.2 命令报文

“GET STARTING DAY”命令报文编码见表 76：

表 76 GET STARTING DAY 命令报文

代码	值
CLA	‘B0’
INS	‘56’
P1	‘01’
P2	‘00’
Lc	不存在

Data	不存在
Le	‘02’

7.8.3 命令报文数据域

命令报文数据域不存在。

7.8.4 响应报文数据域

表 77 定义了“GET STARTING DAY”响应报文数据域。

表 77 GET STARTING DAY 响应报文数据域

说明	长度（字节）
年度起始日期（格式：mmdd）	‘02’

7.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。表 78 描述了 IC 卡可能回送的错误状态。

表 78 GET STARTING DAY 错误状态

SW1	SW2	含 义
‘69’	‘82’	不满足安全状态
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘6E’	‘00’	命令类型错
‘93’	‘03’	应用被永久锁定