

居民健康卡用户卡命令集

V1.0

2011 年 11 月

目录

1 适用范围	1
2 规范性引用文件	2
3 定义和缩略语	3
3.1 定义	3
3.2 缩略语	4
4 复位应答	7
5 命令	8
5.1 命令 APDU 格式	9
5.2 响应 APDU 格式	9
5.3 基本命令	10
5.4 应用命令	26

1 适用范围

本规范规定了居民健康卡用户卡应支持的功能、复位应答的格式以及卡片的命令与响应列表。

本规范适用于所有制作、发行、使用居民健康卡的医疗卫生机构、第三方联合发卡机构、持卡人和生产企业。

2 规范性引用文件

下列文件中的条款通过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 16649.4—2010 识别卡 带触点的集成电路卡 第 4 部分

GB/T 16649.5—2002 识别卡 带触点的集成电路卡 第 5 部分

ISO/IEC 14443 识别卡 非接触式集成电路卡 接近式卡

JR/T 0025—2010 中国金融集成电路（IC）卡规范

卫生部《居民健康卡技术规范》（卫办发〔2011〕60 号）

3 定义和缩略语

3.1 定义

3.1.1 居民健康卡（Residents Health Card）

居民健康卡是中华人民共和国居民拥有的，在医疗卫生服务活动中用于身份识别，满足健康信息存储，实现跨地区和跨机构就医、数据交换和费用结算的基础载体，是计算机可识别的 CPU 卡。

3.1.2 CPU 卡（Central Processing Unit Card）

带有中央处理器（CPU）、存储单元以及卡片操作系统的集成电路卡。

3.1.3 芯片（Chip）

本规范中特指居民健康卡中用于完成数据处理和存储功能的集成电路器件。

3.1.4 芯片操作系统（COS, Card Operating System）

CPU 卡芯片中存储和可运行的，以保护应用数据和程序的机密性和完整性，控制 CPU 卡芯片与外界信息交换为目的的嵌入式软件。

3.1.5 加密算法（Cryptographic Algorithm）

为了隐藏或显现数据信息内容的变换算法。

3.1.6 对称加密算法（Symmetric Cryptographic Algorithm）

加密密钥可以从解密密钥中推算出来，反过来也成立，在大多数算法中加密/解密密钥是相同的。

3.1.7 非对称加密算法（Asymmetric Cryptographic Algorithm）

加密算法的加密密钥和解密密钥是不一样的，不能由一个密钥推导出另一个密钥。

3.1.8 密钥（Key）

加密转换中控制操作的符号序列。

3.1.9 对称密钥（Symmetric Key）

在对称加密算法中使用的密钥。

3.1.10 非对称密钥（Asymmetric Key）

在非对称加密算法中使用的密钥，包括公钥和私钥。

3.1.11 公钥（Public Key）

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥用于验证。

3.1.12 私钥（Private Key）

在一个实体使用的非对称密钥对中仅被该实体使用的密钥。在数字签名方案中，私钥用于签名。

3.1.13 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。

3.1.14 生物标识（Biomarker）

人的某种特异性的生物学特征，具有遗传性和终身携带性，如血型。

3.1.15 医学警示（Medical Alert）

患者在就医、急诊或抢救时需要特别提醒医生注意的信息，包括疾病史、体内装置、药物过敏史、对某些物质的不耐受史等。

3.2 缩略语

以下缩略语和符号表示适用于本规范。

表 3-1 缩略语和符号列表

缩略语	中文名	英文名
'0'-'9' 'A'-'F'	十六进制数字	
AID	应用标识符	Application Identifier
An	字母数字型	Alphanumeric
Ans	特殊字母数字型	Alphanumeric Special
B	二进制	Binary
CBC	密码块链接	Cipher Block Chaining
CLA	命令报文的类别字节	Class Byte of Command Message
Cn	压缩数字	Compressed Numeric
COS	芯片操作系统	Card Operating System
CPU	中央处理器	Central Processing Unit
CVN	卡安全码	Card Verification Number
DDF	目录定义文件	Directory Definition File
DF	专用文件	Dedicated File
EF	基本文件	Elementary File
FCI	文件控制信息	File Control Information
FID	文件标识符	File Identifier
IC	集成电路	Integrated Circuit
IEC	国际电工委员会	International Electrotechnical Commission
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
M	必选型	Mandatory
MAC	报文鉴别代码	Message Authentication Code

MF	主控文件	Master File
O	可选型	Optional
PIX	专用应用标识符扩展码	Proprietary Application Identifier Extension
SAM	安全存取模块	Secure Access Module
PVC	聚氯乙烯	Polyvinyl Chloride
RID	已注册的应用提供者标识	Registered Application Provider Identifier
RS232	串行通信接口	
USB	通用串行总线	Universal Serial BUS
Xx	任意值	

4 复位应答

复位应答中历史字节的前 8 个字节固定为芯片提供机构注册标识（2 字节，由国家 IC 卡注册中心分配的注册标识号）||卡片制造机构注册标识（2 字节，由国家 IC 卡注册中心分配的注册标识号）||卡片序列号（4 字节）。

5 命令

在卡片读写过程中，卡片总是处于以下状态之一，在一种状态下，只有某些命令能够被执行。卡片具有的状态如下：

- (1) 空闲状态：此时卡片没有获得读写权限；
- (2) 安全状态：此时卡片获得了一定的读写授权，可以进行读写操作。

卡片上不同应用之间通过“防火墙”以防止跨过应用进行非法访问，在选择其它应用后，所获得的安全状态消失。卡片通过 **EXTERNAL AUTHENTICATION** 命令获得一定的读写授权，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，卡片将如表 5-1 所示进入另一个状态（或同一个）。

表 5-1 说明了命令执行成功后的状态变化。第一行表示命令发出时卡片的当前状态，第一列表示发出的命令，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。

表 5-1 命令执行成功后的状态变化

命令	空闲	安全
SELECT（选择当前应用）	空闲	安全
SELECT（选择其它应用）	空闲	空闲
EXTERNAL AUTHENTICATION	安全	安全
SELECT（选择文件或记录）	空闲	安全
READ BINARY（一般二进制文件）	空闲	安全
READ RECORD（一般记录文件）	空闲	安全
READ BINARY（限制二进制文件）	N/A	安全
READ RECORD（限制记录文件）	N/A	安全
ERASE RECORD	N/A	安全
WRITE RECORD	N/A	安全

5.1 命令 APDU 格式

命令 APDU 的格式如表 5-2 所示

表 5-2 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 5-3:

表 5-3 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	命令发送的数据字节串(=Lc)	变长
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 5-4:

表 5-4 响应 APDU 的结构

Data	SW1	SW2
←——条件体——→	←——尾——→	

响应 APDU 的内容见表 5-5:

表 5-5 响应 APDU 的内容

代码	描 述	长度
Data	响应中接收的数据字节串(=Le)	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

5.3 基本命令

5.3.1 APPLICATION BLOCK 命令

5.3.1.1 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 命令选择已临时锁定的应用时，将回送状态码 ‘6283’（选择文件无效），同时返回 FCI。

对其他命令的影响根据不同应用而定。

5.3.1.2 命令报文

APPLICATION BLOCK 命令报文编码见表 5-6

表 5-6 APPLICATION BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘1E’
P1	‘00’，其他值保留为将来使用
P2	‘00’，临时锁定应用，锁定后可用 APPLICATION_UNBLOCK 解锁
	‘01’，永久锁定应用
Lc	‘04’
Data	报文鉴别代码(MAC)数据元；根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码。
Le	不存在

5.3.1.3 命令报文数据域

命令报文数据域包括根据《居民健康卡技术规范》第 9.4.2 章中的规定进行

编码的报文鉴别码(MAC)数据元。

5.3.1.4 响应报文数据域

响应报文数据域不存在。

5.3.1.5 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如表 5-7 所示：

表 5-7 APPLICATION 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’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据

5.3.2 APPLICATION UNBLOCK 命令

5.3.2.1 定义和范围

APPLICATION UNBLOCK 命令可以对临时锁定的应用解锁，当 APPLICATION UNBLOCK 命令成功地完成后，用 SELECT 命令可以正确选择此应用，应用功能同时被恢复。

5.3.2.2 命令报文

APPLICATION UNBLOCK 命令报文编码见表 5-8：

表 5-8 APPLICATION UNBLOCK 命令报文

代码	数值
CLA	‘84’
INS	‘18’
P1	‘00’

P2	‘00’
Lc	‘04’
DATA	报文鉴别代码(MAC)数据元；根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码。
Le	不存在

5.3.2.3 命令报文数据域

命令报文数据域包括根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码的报文鉴别码(MAC)数据元。

5.3.2.4 响应报文数据域

响应报文数据域不存在。

5.3.2.5 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如表 5-9 所示：

表 5-9 APPLICATION UNBLOCK 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’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据

5.3.3 CARD BLOCK 命令

5.3.3.1 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“不支持此功能”(SW1SW2=‘6A81’)，且不执行任何其他操作。

5.3.3.2 命令报文

CARD BLOCK 命令报文编码见表 5-10:

表 5-10 CARD BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘16’
P1	‘00’, 其他值保留为将来使用
P2	‘00’, 其他值保留为将来使用
Lc	‘04’
Data	报文鉴别代码(MAC)数据元; 根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码
Le	不存在

5.3.3.3 命令报文数据域

命令报文数据域包括根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码的报文鉴别代码(MAC)数据元。

5.3.3.4 响应报文数据域

响应报文数据域不存在。

5.3.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码如表 5-11 所示:

表 5-11 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’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	参数 P1 或/和 P2 错误

'6A'	'88'	未找到引用数据
------	------	---------

5.3.4 EXTERNAL AUTHENTICATION 命令

5.3.4.1 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。

5.3.4.2 命令报文

EXTERNAL AUTHENTICATION 命令报文编码见表 5-12:

表 5-12 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	'00'
INS	'82'
P1	'00'
P2	密钥标识符（见表 5-12 表 5-13）
Lc	'11'
Data	鉴别用数据
Le	不存在

表 5-13 定义了命令报文中的密钥标识符:

表 5-13 密钥标识符的结构

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0	0	0	0	默认密钥
0								全局参考数据
1								专用参考数据
				x	x	x	x	密钥号

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。

5.3.4.3 命令报文数据域

命令报文数据域中包含 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 个字节表示密钥版本。

其中，鉴别数据根据《居民健康卡技术规范》第 9.7.3 章中的规定进行编码。

5.3.4.4 响应报文数据域

响应报文数据域不存在。

5.3.4.5 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如表 5-14 所示：

表 5-14 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如表 5-15 所示：

表 5-15 EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	鉴别方法锁定
‘69’	‘84’	引用数据无效
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	密钥未找到

5.3.5 GET CHALLENGE 命令

5.3.5.1 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。

随机数在使用后失效，不能被下一个命令再次使用。

5.3.5.2 命令报文

GET CHALLENGE 命令报文编码见表 5-16：

表 5-16 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	‘08’

5.3.5.3 命令报文数据域

命令报文数据域不存在。

5.3.5.4 响应报文数据域

响应报文数据域包括随机数，长度为 8 字节。

5.3.5.5 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如表 5-17 所示：

表 5-17 GET CHALLENGE 错误状态

SW1	SW2	含 义
‘67’	‘00’	Le 长度错
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	参数 P1 P2 不正确

5.3.6 INTERNAL AUTHENTICATION 命令

5.3.6.1 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。

5.3.6.2 命令报文

INTERNAL AUTHENTICATION 命令报文编码见表 5-18：

表 5-18 INTERNAL AUTHENTICATION 命令报文

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

INTERNAL AUTHENTICATION 命令的参数 P1 和 P2 为‘00’表示无信息，它们的值是事先确定的。

5.3.6.3 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 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，由终端产生；
- 第 9 至第 16 个字节是鉴别所需的原始信息；
- 第 17 个字节表示密钥版本。

5.3.6.4 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《居民健康卡技术规范》第 9.7.3 章中的规定进行计算。

5.3.6.5 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如表 5-19 所示：

表 5-19 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码如表 5-20 所示：

表 5-20 INTERNAL AUTHENTICATION 错误状态

SW1	SW2	含 义
‘67’	‘00’	Lc 不正确

'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'	参数 P1 P2 不正确
'6A'	'88'	密钥未找到

5.3.7 READ BINARY 命令

5.3.7.1 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）。

5.3.7.2 命令报文

READ BINARY 命令报文编码见表 5-21

表 5-21 READ BINARY 命令报文

代码	值
CLA	'00'
INS	'B0'
P1	见表 5-22
P2	见表 5-22
Lc	不存在
Data	不存在
Le	'00'或要读出的数据的长度

表 5-22 定义了命令报文中的引用控制参数：

表 5-22 READ BINARY 命令引用控制参数

P1								P2								含 义
b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	
0	X	X	X	X	X	X	X	Y	Y	Y	Y	Y	Y	Y	Y	P1×'0x100'+P2 为要读的首字节距离文件首字节的偏移量。

5.3.7.3 命令报文数据域

命令报文数据域不存在。

5.3.7.4 响应报文数据域

当 Le 的值为零时，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。

5.3.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 5-23 所示：

表 5-23 READ BINARY 警告状态

SW1	SW2	含 义
‘62’	‘81’	部分回送的数据可能有错

IC 卡可能回送的错误状态码如表 5-24 所示：

表 5-24 READ BINARY 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’	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
‘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）

5.3.8 READ RECORD 命令

5.3.8.1 定义和范围

READ RECORD 命令读取记录结构的基本文件中指定的记录。

IC 卡的响应由回送记录组成。

5.3.8.2 命令报文

READ RECORD 命令报文编码见表 5-25：

表 5-25 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 5-26）
Lc	不存在
Data	不存在
Le	‘00’ 或记录长度

记录号的取值范围为‘01’-‘FE’。

表 5-26 定义了命令报文中的引用控制参数：

表 5-26 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
					1	0	0	读 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

5.3.8.3 命令报文数据域

命令报文数据域不存在。

5.3.8.4 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。

5.3.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 5-27 所示：

表 5-27 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码如表 5-28 所示：

表 5-28 READ RECORD 错误状态

SW1	SW2	含 义
‘67’	‘00’	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’	‘85’	使用条件不满足
‘69’	‘86’	命令不允许使用（无当前基本文件）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘86’	参数 P1 或 P2 错误

5.3.9 SELECT 命令

5.3.9.1 定义和范围

SELECT 命令通过文件名或 AID、文件标识符来选择 IC 卡中的居民健康卡应用环境、DDF 或 ADF，通过文件标识符来选择 ADF 中的 AEF。

命令执行成功后，居民健康卡应用环境、DDF 或 ADF、AEF 的路径被设定。

除选择 AEF 外，从 IC 卡的响应报文应由回送 FCI 组成。

5.3.9.2 命令报文

SELECT 命令报文编码见表 5-29：

表 5-29 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表 5-30）
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 5-30 定义了命令报文中的引用控制参数：

表 5-30 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、EF（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)。

5.3.9.3 命令报文数据域

命令报文数据域应包括内容见表 5-30。

5.3.9.4 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居民健康卡应用环境、DDF 或 ADF 的 FCI。表 5-31 到表 5-33 规定了此定义所用的标志。《居民健康卡技术规范》不规定 FCI 中回送的附加标志。

表 5-31 定义了成功选择居民健康卡应用环境后回送的 FCI:

表 5-31 SELECT 居民健康卡应用环境的响应报文(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 5-32 定义了成功选择 DDF 后回送的 FCI:

表 5-32 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 5-33 定义了成功选择 ADF 后回送的 FCI:

表 5-33SELECT ADF 的响应报文(FCI)

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

5.3.9.5 响应报文状态码

此命令执行成功的状态码是'9000'。

IC 卡可能回送的警告状态码如表 5-34 所示:

表 5-34 SELECT 警告状态

SW1	SW2	含 义
‘62’	‘81’	返回的数据中的部分可能已被破坏
‘62’	‘83’	选择的文件无效
‘62’	‘84’	FCI 格式与 P2 指定的不符

IC 卡可能回送的错误状态码如表 5-35 所示：

表 5-35 SELECT 错误状态

SW1	SW2	含 义
‘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’	参数 P1 P2 不正确
‘93’	‘03’	应用永久锁定

5.3.10 UPDATE BINARY 命令

5.3.10.1 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。当使用校验方式更新二进制文件时，如果尝试次数超过限制时，临时锁定当前应用。

5.3.10.2 命令报文

UPDATE BINARY 命令报文编码见表 5-36：

表 5-36 UPDATE BINARY 命令报文

代码	值
CLA	‘00’或 ‘04’
INS	‘D6’
P1	见表 5-37
P2	见表 5-37
Lc	后续数据域的长度
Data	写入或修改用的数据
Le	不存在

表 5-37 定义了命令报文中的引用控制参数：

表 5-37 UPDATE BINARY 命令引用控制参数

P1								P2								含 义
b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	b	
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	
0	X	X	X	X	X	X	X	Y	Y	Y	Y	Y	Y	Y	Y	P1×‘0x100’+P2 为要读的首字节距离文件首字节的偏移量。

5.3.10.3 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。

5.3.10.4 响应报文数据域

响应报文数据域不存在。

5.3.10.5 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如表 5-38 所示：

表 5-38 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’	‘85’	使用条件不满足
‘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’	‘80’	基本文件标识符错误
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6B’	‘00’	参数错误（偏移地址超出了 EF）

5.3.11 UPDATE RECORD 命令

5.3.11.1 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的记录。当使用校验方式更新记录时，如果尝试次数超过限制时，临时锁定当前应用。

UPDATE RECORD 命令不能对健康应用的住院信息索引文件记录和门诊信息索引文件记录进行更新操作。

对线性结构文件来说，只能使用指定记录号（P1 中指定）方式更新记录。

对循环结构文件来说，只能使用“上一个记录”命令选项添加或更新记录，添加或更新后该记录的记录号为 1。

5.3.11.2 命令报文

UPDATE RECORD 命令报文编码见表 5-39：

表 5-39UPDATE RECORD 命令报文

代码	值
CLA	‘00’或 ‘04’
INS	‘DC’
P1	指定的记录号(‘01’~‘FE’)
P2	见表 5-40
Lc	后续数据域的长度
Data	添加的或更新原有记录的新记录
Le	不存在

表 5-40 定义了命令报文中的引用控制参数：

表 5-40 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				当前文件
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

5.3.11.3 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。

5.3.11.4 响应报文数据域

响应报文数据域不存在。

5.3.11.5 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如表 5-41 所示：

表 5-41 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’	‘85’	使用条件不满足
‘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’	‘80’	基本文件标识符错误
‘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
‘6A’	‘85’	Lc 与 TLV 结构不符
‘6A’	‘86’	参数 P1 或/和 P2 不正确

5.4 应用命令

5.4.1 ERASE RECORD 命令

5.4.1.1 定义和范围

ERASE RECORD 命令专用于擦除居民健康应用的住院信息索引文件记录和门诊信息索引文件记录。使用安全报文方式擦除，如果尝试次数超过限制时，临时锁定当前应用。

擦除索引文件记录前，需要获得文件的擦除权限。

5.4.1.2 命令报文

ERASE RECORD 命令报文编码见表 5-42:

表 5-42 ERASE RECORD 命令报文

代码	值
CLA	‘84’
INS	‘0C’
P1	指定的记录号
P2	见表 5-43
Lc	‘04’
Data	报文鉴别代码(MAC)数据元；根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码。
Le	不存在

表 5-43 定义了命令报文中的引用控制参数:

表 5-43 ERASE RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
					1	0	0	记录号在 P1 中给出
其余值								RFU

5.4.1.3 命令报文数据域

命令报文数据域包括根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码的报文鉴别码(MAC)数据元。

5.4.1.4 响应报文数据域

响应报文数据域不存在。

5.4.1.5 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如表 5-44 所示:

表 5-44ERASE 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'	'85'	使用条件不满足
'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'	不支持此功能
'6A'	'83'	未找到记录
'6A'	'86'	参数 P1 或/和 P2 不正确
'6E'	'00'	CLA 错误

5.4.2 WRITE RECORD 命令

5.4.2.1 定义和范围

WRITE RECORD 命令专用于生效居民健康应用的住院信息索引文件记录和门诊信息索引文件记录，对记录文件写入特定值 '00H'。使用安全报文方式写入，如果尝试次数超过限制时，临时锁定当前应用。

写入索引文件记录前，需要获得文件的写入权限。

5.4.2.2 命令报文

WRITE RECORD 命令报文编码见表 5-45：

表 5-45 WRITE RECORD 命令报文

代码	值
CLA	'84'
INS	'D2'
P1	指定的记录号
P2	见表 5-46
Lc	'04'
Data	报文鉴别代码(MAC)数据元；根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码。
Le	不存在

表 5-46 定义了命令报文中的引用控制参数：

表 5-46 WRITE RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
					1	0	0	记录号在 P1 中给出

其余值	RFU
-----	-----

5.4.2.3 命令报文数据域

命令报文数据域包括根据《居民健康卡技术规范》第 9.4.2 章中的规定进行编码的报文鉴别码(MAC)数据元。

5.4.2.4 响应报文数据域

响应报文数据域不存在。

5.4.2.5 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如表 5-47 所示：

表 5-47WRITE 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’	‘85’	使用条件不满足
‘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’	不支持此功能
‘6A’	‘83’	未找到记录
‘6A’	‘86’	参数 P1 或/和 P2 不正确
‘6E’	‘00’	CLA 错误