
居民健康卡应用规范

V1.1

2012 年 4 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	5
4 文件、数据元、数据对象列表	7
4.1 文件结构	7
4.2 应用数据文件(ADF)	25
4.3 应用基本文件(AEF)	26
4.4 文件结构映射	26
4.5 文件引用	26
5 卡操作	27
5.1 总体操作	27
5.2 内部认证	28
5.3 外部认证	30
5.4 应用锁定	32
5.5 应用解锁	33
5.6 卡锁定	34
5.7 应用维护	34
6 卡业务应用	35
6.1 卡识别应用 (对应 MF\DDF1 数据区)	35
6.2 身份识别应用 (对应 DDF1\DF01 数据区)	39
6.3 基础健康信息应用 (对应 DDF1\DF02 数据区)	43
6.4 管理业务应用(对应 DDF1\DF03 数据区)	47
7 数据签名和验证	55
7.1 数据签名	55
7.2 数据签名验证	57

1 适用范围

本规范规定了居民健康卡的文件结构、数据元以及数据对象列表，描述了居民健康卡各项操作的流程，明确了在不同应用场景下进行数据交换、信息传输以及数据签名和验证的过程。

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、生产企业和持卡人，以及居民健康卡应用系统的研制、维护等单位 and 部门。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2260—2007	中华人民共和国行政区划代码
GB/T 2261.1—2003	人的性别代码
GB/T 2261.2—2003	婚姻状况代码
GB/T 2312—1980	信息交换用汉字编码字符集—基本集
GB 3304—1991	中国各民族名称的罗马字母拼写法和代码
GB/T 4658—2006	学历代码
GB/T 6565—2009	职业分类与代码
GB 11643—1999	公民身份号码
GB 11714—1997	全国组织机构代码编制规则
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
WS 363—2011	卫生信息数据元目录
WS 364—2011	卫生信息数据元值域代码
WS 365—2011	城乡居民健康档案基本数据集
GA 324.1—2001	户口类别代码
JR/T 0025—2010	中国金融集成电路（IC）卡规范
ICD-9-CM	国际疾病分类第九版临床修订
ICD-10	国际疾病与相关健康问题分类代码第十版
ISO/ IEC 14443	识别卡非接触式集成电路卡接近式卡
ISO/IEC 7811/2—2001	识别卡记录技术第 2 部分
卫生部《居民健康卡技术规范》（卫办发〔2011〕60 号）	
卫生部《居民健康卡用户卡命令集》	
卫生部《居民健康卡安全存取模块（SAM）卡技术规范》	
卫生部《居民健康卡安全存取模块（SAM）卡命令集》	

3 定义和缩略语

3.1 定义

3.1.1 应用（Application）

IC 卡和终端之间的应用协议和相关的数据集。

3.1.2 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。

3.1.3 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。

3.1.4 响应（Response）

IC 卡处理完收到的命令报文后，返回给终端的报文。

3.1.5 终端（Terminal）

为完成居民健康卡交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。

3.1.6 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。

3.1.7 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。

3.1.8 卡片操作系统（COS, Card Operating System）

CPU 卡芯片中存储和运行的，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。

3.1.9 加密算法（Cryptographic Algorithm）

为了隐藏或显现数据信息内容的变换算法。

3.1.10 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。

3.1.11 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。

3.1.12 密钥（Key）

加密转换中控制操作的符号序列。

3.1.13 对称密钥（Symmetric Key）

在对称加密算法中使用的密钥。

3.1.14 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。

3.1.15 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。

3.1.16 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。

3.1.17 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。

3.1.18 生物标识（Biomarker）

人的某种生物学特征，具有遗传性和终身携带性，如血型。

3.1.19 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
BER	基本编码规则	Basic Encoding Rules
cn	压缩数字	Compressed Numeric
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

ISO	国际标准化组织	International Organization for Standardization
MAC	报文鉴别代码	Message Authentication Code
MF	主控文件	Master File
SAM	安全存取模块	Secure Access Module
TLV	标签、长度、值	Tag Length Value

4 文件、数据元、数据对象列表

4.1 文件结构

本规范中的文件组织结构来自且符合 GB/T 16649.4 的基本组织结构。

本部分描述了符合本规范的应用文件结构，定义了居民健康卡在医疗领域的各项专有应用，DDF1 是居民健康卡应用环境，DDF2 是其他预留应用环境。

从终端的角度来看，IC 卡上的文件是一种树形结构。树的每一个分支是一个应用数据文件(ADF)或一个目录定义文件(DDF)。一个 ADF 是一个或者多个应用基本文件(AEF)的入口点。一个 ADF 及其相关的数据文件处于树的同一分支上。一个 DDF 是其他 ADF 或者 DDF 的入口点。

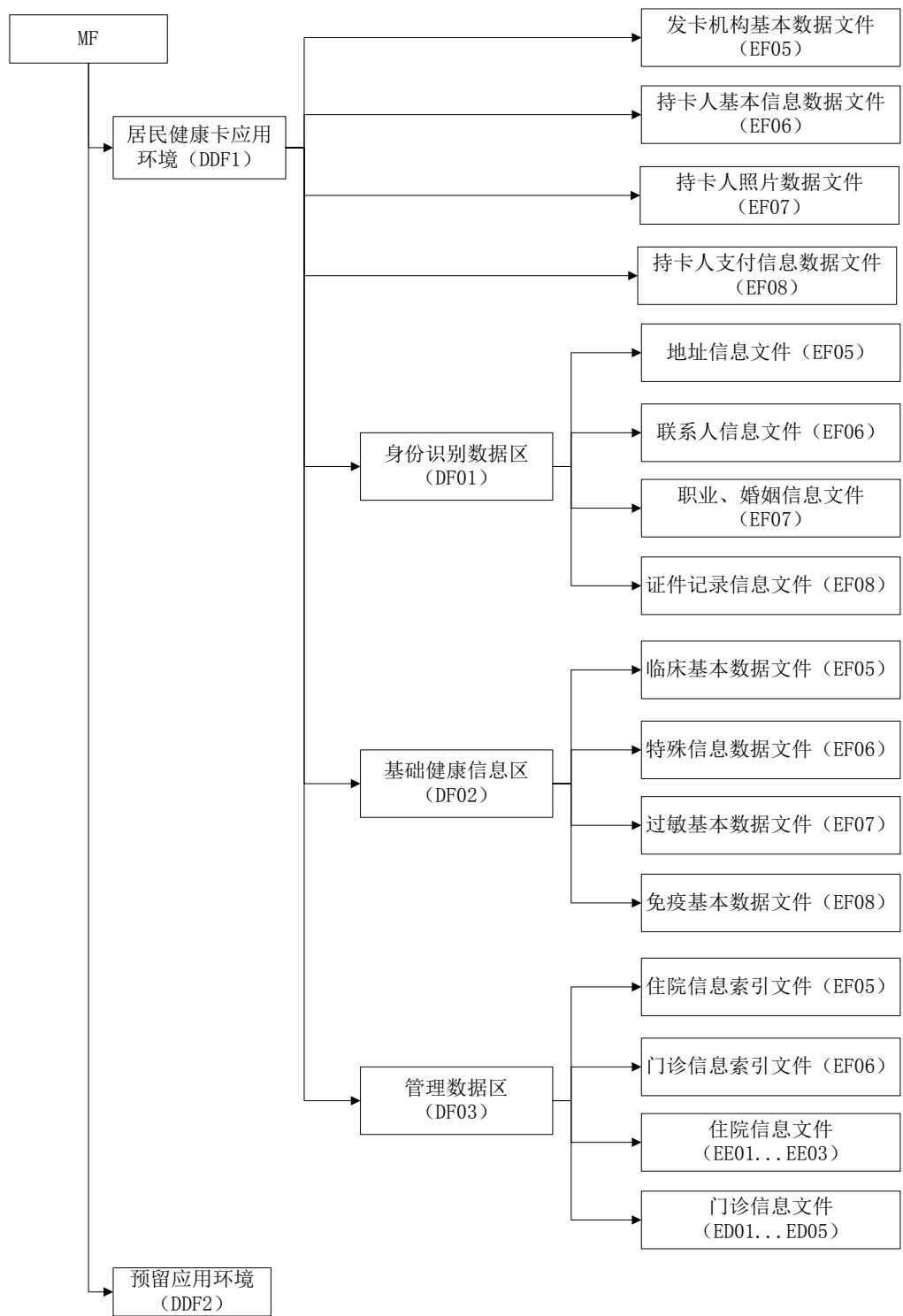


图 4-1 居民健康卡文件结构示意图

发卡机构基本数据文件： FID = ‘EF05’，变长记录文件。

持卡人基本信息数据文件： FID = ‘EF06’，变长记录文件。

持卡人照片数据文件：	FID = ‘EF07’，二进制文件。
持卡人支付信息数据文件：	FID = ‘EF08’，变长记录文件。
身份识别数据区 ADF：	FID = ‘DF01’，AID = ‘915600013200’。
地址信息文件：	FID = ‘EF05’，变长记录文件。
联系人信息文件：	FID = ‘EF06’，变长记录文件。
职业、婚姻信息文件：	FID = ‘EF07’，变长记录文件。
证件记录信息文件：	FID = ‘EF08’，变长记录文件。
基础健康信息区 ADF：	FID = ‘DF02’，AID = ‘915600013201’。
临床基本数据文件：	FID = ‘EF05’，变长记录文件。
特殊信息数据文件：	FID = ‘EF06’，变长记录文件。
过敏基本数据文件：	FID = ‘EF07’，循环记录文件。
免疫基本数据文件：	FID = ‘EF08’，循环记录文件。
管理数据区 ADF：	FID = ‘DF03’，AID = ‘915600013202’。
住院信息索引文件：	FID = ‘EF05’，定长记录文件。
门诊信息索引文件：	FID = ‘EF06’，定长记录文件。
住院信息文件：	FID = ‘EE01’— ‘EE03’，二进制文件。
门诊信息文件：	FID = ‘ED01’— ‘ED05’，二进制文件。

注：1.二进制文件：文件数据是通过连续空间中的字节地址进行存取。

2.记录文件：数据以记录为单位进行存取，同一文件内所有记录的长度可以不相等。同一文件内最多可以容纳 254 条记录。

表 4-1 发卡机构基本数据文件

文件标识（FID）			‘EF05’
文件类型			变长记录
文件存取控制		读=自由	禁止改写
标签	数据元	类型	长度
01	卡的类别	Ans	01
02	规范版本	Ans	04
03	发卡机构名称	Ans	30
04	发卡机构代码	Cn	11

05	发卡机构证书	B	180
06	发卡时间	Cn	04
08	卡号	Ans	18
09	安全码	Ans	03
10	发卡序列号	Ans	10
57	应用城市代码	Cn	03

表 4-2 持卡人基本信息数据文件

文件标识 (FID)			'EF06'
文件类型			变长记录
文件存取控制		读 =RK1 _{DDF1}	禁止改写
标签	数据元	类型	长度
11	姓名	ans	30
12	性别	b	01
13	民族代码	cn	01
14	出生日期	cn	04
15	居民身份证号码	ans	18

表 4-3 持卡人照片数据文件

文件标识 (FID)			'EF07'
文件类型			二进制文件
文件存取控制		读=RK1 _{DDF1}	改写=UK1 _{DDF1}
标签	数据元	类型	长度
	照片	b	3074

注：照片文件存放方式为两字节照片数据长度+照片数据，例如照片数据为 2066 (0x0812) 字节，则文件第一个字节为 0x08，第二个字节为 0x12，从第三个字节开始为照片数据。

表 4-4 持卡人支付信息数据文件

文件标识 (FID)		'EF08'	
文件类型		变长记录	
文件存取控制		读 =RK1 _{DDF1}	改写=UK1 _{DDF1}
标签	数据元	类型	长度
07	卡有效期	Cn	04
16	本人电话 1	ans	20
17	本人电话 2	ans	20
18	医疗费用支付方式	cn	01
19	医疗费用支付方式	cn	01
20	医疗费用支付方式	cn	01

表 4-5 地址信息文件

文件标识 (FID)		'EF05'	
文件类型		变长记录	
文件大小			
文件存取控制		读 =RK1 _{DF01}	改写=UK1 _{DF01}
标签	数据元	类型	长度
21	地址类别 1	cn	01
22	地址 1	ans	100
23	地址类别 2	cn	01
24	地址 2	ans	100

表 4-6 联系人信息文件

文件标识 (FID)		'EF06'	
文件类型		变长记录	
文件存取控制		读 =RK1 _{DF01}	改写=UK1 _{DF01}
标签	数据元	类型	长度
25	联系人姓名 1	ans	30
26	联系人关系 1	cn	01

27	联系人电话 1	ans	20
28	联系人姓名 2	ans	30
29	联系人关系 2	cn	01
30	联系人电话 2	ans	20
31	联系人姓名 3	ans	30
32	联系人关系 3	cn	01
33	联系人电话 3	ans	20

表 4-7 职业、婚姻信息文件

文件标识（FID）		‘EF07’	
文件类型		变长记录	
文件存取控制		读 =RK1 _{DF01}	改写=UK1 _{DF01}
标签	数据元	类型	长度
34	文化程度代码	cn	01
35	婚姻状况代码	cn	01
36	职业代码	ans	03

表 4-8 证件记录信息文件

文件标识（FID）		‘EF08’	
文件类型		变长记录	
文件存取控制		读=RK1 _{DF01}	改写=UK1 _{DF01}
标签	数据元	类型	长度
37	证件类别	cn	01
38	证件号码	ans	18
39	健康档案编号	ans	17
40	新农合证（卡）号	ans	18

表 4-9 临床基本数据文件

文件标识（FID）		‘EF05’	
文件类型		变长记录	
文件存取控制		读=RK1 _{DF02}	改写=UK1 _{DF02}
标签	数据元	类型	长度

41	ABO 血型代码	b	01
42	RH 血型代码	cn	01
43	哮喘标志	b	01
44	心脏病标志	b	01
45	心脑血管病标志	b	01
46	癫痫病标志	b	01
47	凝血紊乱标志	b	01
48	糖尿病标志	b	01
49	青光眼标志	b	01
50	透析标志	b	01
51	器官移植标志	b	01
52	器官缺失标志	b	01
53	可装卸的义肢标志	b	01
54	心脏起搏器标志	b	01
55	其他医学警示名称	ans	40

表 4-10 特殊信息数据文件

文件标识 (FID)		'EF06'	
文件类型		变长记录	
文件存取控制		读=RK1 _{DF02}	改写=UK2 _{DF02}
标签	数据元	类型	长度
56	精神病标志	b	01

表 4-11 过敏基本数据文件

文件标识 (FID)		'EF07'	
文件类型		循环记录 (3 条)	
文件存取控制		读=RK1 _{DF02}	改写=UK3 _{DF02}
	数据元	类型	长度
	过敏物质名称	ans	20
	过敏反应	ans	100

表 4-12 免疫基本数据文件

文件标识（FID）			‘EF08’
文件类型			循环记录（10 条）
文件存取控制		读=RK1 _{DF02}	改写=UK3 _{DF02}
	数据元	类型	长度
	免疫接种名称	ans	20
	免疫接种时间	cn	04

表 4-13 住院信息索引文件

文件标识（FID）			‘EF05’
文件类型			定长记录（3 条）
文件存取控制		读=RK1 _{DF03}	改写=UK1 _{DF03} 擦除=UK2 _{DF03}
	数据元	类型	长度
	住院记录有效标志	b	01

表 4-14 门诊信息索引文件

文件标识（FID）			‘EF06’
文件类型			定长记录（5 条）
文件存取控制		读=RK1 _{DF03}	改写=UK1 _{DF03} 擦除=UK2 _{DF03}
	数据元	类型	长度
	门诊记录有效标志	b	01

表 4-15 住院信息文件

文件标识（FID）			‘EE01’— ‘EE03’
文件类型			二进制
文件存取控制		读=RK1 _{DF03}	改写=UK1 _{DF03}
	数据元	类型	长度
	住院机构名称	ans	70
	住院机构组织机构代码	ans	10
	入院日期	cn	04

	住院患者住院次数	cn	02
	病案号	ans	18
	住院患者入院科室名称	ans	50
	住院患者入院病情	cn	01
	住院患者医院感染名称	ans	50
	住院患者损伤和中毒外部原因	ans	07
	住院患者血清学检查项目代码 1	cn	01
	住院患者血清学检查结果代码 1	cn	01
	疾病诊断名称 1	ans	50
	疾病诊断代码 1	ans	07
	确诊日期 1	cn	04
	住院患者诊断符合情况-详细描述 1	ans	20
	住院患者诊断符合情况-代码 1	cn	01
	住院患者疾病诊断类型-详细描述 1	ans	20
	住院患者疾病诊断类型-代码 1	cn	01
	住院患者治疗结果代码 1	cn	01
	手术/操作-名称 1	ans	80
	手术/操作-代码 1	ans	5
	手术/操作-日期 1	cn	04
	麻醉-方法 1	ans	50
	麻醉-方法代码 1	cn	01
	手术切口愈合等级代码 1	cn	01
	住院患者血清学检查项目代码 2	cn	01
	住院患者血清学检查结果代码 2	cn	01
	疾病诊断名称 2	ans	50
	疾病诊断代码 2	ans	07
	确诊日期 2	cn	04
	住院患者诊断符合情况-详细描述 2	ans	20

	住院患者诊断符合情况-代码 2	cn	01
	住院患者疾病诊断类型-详细描述 2	ans	20
	住院患者疾病诊断类型-代码 2	cn	01
	住院患者治疗结果代码 2	cn	01
	手术/操作-名称 2	ans	80
	手术/操作-代码 2	ans	5
	手术/操作-日期 2	cn	04
	麻醉-方法 2	ans	50
	麻醉-方法代码 2	cn	01
	手术切口愈合等级代码 2	cn	01
	住院患者血清学检查项目代码 3	cn	01
	住院患者血清学检查结果代码 3	cn	01
	疾病诊断名称 3	ans	50
	疾病诊断代码 3	ans	07
	确诊日期 3	cn	04
	住院患者诊断符合情况-详细描述 3	ans	20
	住院患者诊断符合情况-代码 3	cn	01
	住院患者疾病诊断类型-详细描述 3	ans	20
	住院患者疾病诊断类型-代码 3	cn	01
	住院患者治疗结果代码 3	cn	01
	手术/操作-名称 3	ans	80
	手术/操作-代码 3	ans	5
	手术/操作-日期 3	cn	04
	麻醉-方法 3	ans	50
	麻醉-方法代码 3	cn	01
	手术切口愈合等级代码 3	cn	01
	住院期间输血品种代码 1	cn	01
	住院期间输血量 1	cn	02

	住院患者输血量计量单位 1	ans	10
	住院期间输血品种代码 2	cn	01
	住院期间输血量 2	cn	02
	住院患者输血量计量单位 2	ans	10
	住院期间输血品种代码 3	cn	01
	住院期间输血量 3	cn	02
	住院患者输血量计量单位 3	ans	10
	住院期间输血品种代码 4	cn	01
	住院期间输血量 4	cn	02
	住院患者输血量计量单位 4	ans	10
	住院患者抢救次数	cn	02
	住院患者抢救成功次数	cn	02
	出院日期	cn	04
	住院患者出院科室名称	ans	50
	住院患者住院天数	cn	03
	住院患者尸检标志	b	01
	住院患者随诊标志	b	01
	住院费用-医疗付款方式代码	cn	01
	住院费用-分类 1	ans	20
	住院费用-分类代码 1	ans	01
	住院费用-金额 1	cn	05
	住院费用-分类 2	ans	20
	住院费用-分类代码 2	ans	01
	住院费用-金额 2	cn	05
	住院费用-分类 3	ans	20
	住院费用-分类代码 3	ans	01
	住院费用-金额 3	cn	05
	住院费用-分类 4	ans	20
	住院费用-分类代码 4	ans	01
	住院费用-金额 4	cn	05

	住院费用-分类 5	ans	20
	住院费用-分类代码 5	ans	01
	住院费用-金额 5	cn	05
	住院费用-分类 6	ans	20
	住院费用-分类代码 6	ans	01
	住院费用-金额 6	cn	05
	住院费用-分类 7	ans	20
	住院费用-分类代码 7	ans	01
	住院费用-金额 7	cn	05
	住院费用-分类 8	ans	20
	住院费用-分类代码 8	ans	01
	住院费用-金额 8	cn	05
	住院费用-分类 9	ans	20
	住院费用-分类代码 9	ans	01
	住院费用-金额 9	cn	05
	住院费用-分类 10	ans	20
	住院费用-分类代码 10	ans	01
	住院费用-金额 10	cn	05
	住院费用-分类 11	ans	20
	住院费用-分类代码 11	ans	01
	住院费用-金额 11	cn	05
	住院费用-分类 12	ans	20
	住院费用-分类代码 12	ans	01
	住院费用-金额 12	cn	05
	住院费用-分类 13	ans	20
	住院费用-分类代码 13	ans	01
	住院费用-金额 13	cn	05
	住院费用-分类 14	ans	20
	住院费用-分类代码 14	ans	01
	住院费用-金额 14	cn	05

	住院费用-分类 15	ans	20
	住院费用-分类代码 15	ans	01
	住院费用-金额 15	cn	05
	住院费用-分类 16	ans	20
	住院费用-分类代码 16	ans	01
	住院费用-金额 16	cn	05
	住院费用-分类 17	ans	20
	住院费用-分类代码 17	ans	01
	住院费用-金额 17	cn	05
	住院费用-分类 18	ans	20
	住院费用-分类代码 18	ans	01
	住院费用-金额 18	cn	05
	住院费用-分类 19	ans	20
	住院费用-分类代码 19	ans	01
	住院费用-金额 19	cn	05
	住院费用-分类 20	ans	20
	住院费用-分类代码 20	ans	01
	住院费用-金额 20	cn	05
	住院总费用	cn	05
	床位费	cn	05
	住院护理费	cn	05
	住院西药费	cn	05
	住院中药费	cn	05
	住院化验费	cn	05
	住院诊疗费	cn	05
	住院手术费	cn	05
	住院检查费	cn	05
	其他住院费用	cn	05
	交易信息签名	b	64
	SAM 卡证书	b	190

表 4-16 门诊信息文件

文件标识（FID）		‘ED01’— ‘ED05’	
文件类型		二进制	
文件存取控制		读=RK1 _{DF03}	改写=UK1 _{DF03}
	数据元	类型	长度
	就诊机构名称	ans	70
	就诊机构组织机构代码	ans	10
	就诊日期时间	cn	07
	门诊号	ans	18
	就医科室名称	ans	50
	医疗付款方式	cn	01
	症状名称 1	ans	50
	症状代码 1	ans	05
	诊断日期 1	cn	04
	门诊诊断名称 1	ans	50
	门诊诊断代码 1	ans	07
	发病日期时间 1	cn	07
	症状持续时间 1	cn	02
	症状名称 2	ans	50
	症状代码 2	ans	05
	诊断日期 2	cn	04
	门诊诊断名称 2	ans	50
	门诊诊断代码 2	ans	07
	发病日期时间 2	cn	07
	症状持续时间 2	cn	02
	症状名称 3	ans	50
	症状代码 3	ans	05
	诊断日期 3	cn	04
	门诊诊断名称 3	ans	50
	门诊诊断代码 3	ans	07
	发病日期时间 3	cn	07

	症状持续时间 3	cn	02
	症状名称 4	ans	50
	症状代码 4	ans	05
	诊断日期 4	cn	04
	门诊诊断名称 4	ans	50
	门诊诊断代码 4	ans	07
	发病日期时间 4	cn	07
	症状持续时间 4	cn	02
	症状名称 5	ans	50
	症状代码 5	ans	05
	诊断日期 5	cn	04
	门诊诊断名称 5	ans	50
	门诊诊断代码 5	ans	07
	发病日期时间 5	cn	07
	症状持续时间 5	cn	02
	检查/检验项目名称 1	ans	80
	检查/检验结果代码 1	cn	01
	检查/检验定量结果 1	cn	05
	检查/检验计量单位 1	ans	20
	检查/检验项目代码 1	ans	20
	检查/检验项目名称 2	ans	80
	检查/检验结果代码 2	cn	01
	检查/检验定量结果 2	cn	05
	检查/检验计量单位 2	ans	20
	检查/检验项目代码 2	ans	20
	检查/检验项目名称 3	ans	80
	检查/检验结果代码 3	cn	01
	检查/检验定量结果 3	cn	05
	检查/检验计量单位 3	ans	20
	检查/检验项目代码 3	ans	20

	检查/检验项目名称 4	ans	80
	检查/检验结果代码 4	cn	01
	检查/检验定量结果 4	cn	05
	检查/检验计量单位 4	ans	20
	检查/检验项目代码 4	ans	20
	检查/检验项目名称 5	ans	80
	检查/检验结果代码 5	cn	01
	检查/检验定量结果 5	cn	05
	检查/检验计量单位 5	ans	20
	检查/检验项目代码 5	ans	20
	检查/检验项目名称 6	ans	80
	检查/检验结果代码 6	cn	01
	检查/检验定量结果 6	cn	05
	检查/检验计量单位 6	ans	20
	检查/检验项目代码 6	ans	20
	检查/检验项目名称 7	ans	80
	检查/检验结果代码 7	cn	01
	检查/检验定量结果 7	cn	05
	检查/检验计量单位 7	ans	20
	检查/检验项目代码 7	ans	20
	检查/检验项目名称 8	ans	80
	检查/检验结果代码 8	cn	01
	检查/检验定量结果 8	cn	05
	检查/检验计量单位 8	ans	20
	检查/检验项目代码 8	ans	20
	检查/检验项目名称 9	ans	80
	检查/检验结果代码 9	cn	01
	检查/检验定量结果 9	cn	05
	检查/检验计量单位 9	ans	20
	检查/检验项目代码 9	ans	20

	检查/检验项目名称 10	ans	80
	检查/检验结果代码 10	cn	01
	检查/检验定量结果 10	cn	05
	检查/检验计量单位 10	ans	20
	检查/检验项目代码 10	ans	20
	药物名称 1	ans	50
	药物剂型代码 1	cn	01
	用药天数 1	cn	03
	药物使用频率 1	ans	20
	药物使用剂量单位 1	ans	06
	药物使用次剂量 1	cn	03
	药物使用总剂量 1	cn	06
	药物使用途径代码 1	cn	02
	药物名称 2	ans	50
	药物剂型代码 2	cn	01
	用药天数 2	cn	03
	药物使用频率 2	ans	20
	药物使用剂量单位 2	ans	06
	药物使用次剂量 2	cn	03
	药物使用总剂量 2	cn	06
	药物使用途径代码 2	cn	02
	药物名称 3	ans	50
	药物剂型代码 3	cn	01
	用药天数 3	cn	03
	药物使用频率 3	ans	20
	药物使用剂量单位 3	ans	06
	药物使用次剂量 3	cn	03
	药物使用总剂量 3	cn	06
	药物使用途径代码 3	cn	02
	药物名称 4	ans	50

	药物剂型代码 4	cn	01
	用药天数 4	cn	03
	药物使用频率 4	ans	20
	药物使用剂量单位 4	ans	06
	药物使用次剂量 4	cn	03
	药物使用总剂量 4	cn	06
	药物使用途径代码 4	cn	02
	药物名称 5	ans	50
	药物剂型代码 5	cn	01
	用药天数 5	cn	03
	药物使用频率 5	ans	20
	药物使用剂量单位 5	ans	06
	药物使用次剂量 5	cn	03
	药物使用总剂量 5	cn	06
	药物使用途径代码 5	cn	02
	手术/操作名称 1	ans	80
	手术/操作代码 1	ans	5
	手术/操作日期 1	cn	04
	手术/操作名称 2	ans	80
	手术/操作代码 2	ans	5
	手术/操作日期 2	cn	04
	手术/操作名称 3	ans	80
	手术/操作代码 3	ans	5
	手术/操作日期 3	cn	04
	门诊费用分类名称 1	ans	20
	门诊费用分类代码 1	cn	01
	门诊费用金额 1	cn	04
	门诊费用分类名称 2	ans	20
	门诊费用分类代码 2	cn	01
	门诊费用金额 2	cn	04

	门诊费用分类名称 3	ans	20
	门诊费用分类代码 3	cn	01
	门诊费用金额 3	cn	04
	门诊费用分类名称 4	ans	20
	门诊费用分类代码 4	cn	01
	门诊费用金额 4	cn	04
	门诊费用分类名称 5	ans	20
	门诊费用分类代码 5	cn	01
	门诊费用金额 5	cn	04
	门诊费用分类名称 6	ans	20
	门诊费用分类代码 6	cn	01
	门诊费用金额 6	cn	04
	门诊费用分类名称 7	ans	20
	门诊费用分类代码 7	cn	01
	门诊费用金额 7	cn	04
	门诊费用分类名称 8	ans	20
	门诊费用分类代码 8	cn	01
	门诊费用金额 8	cn	04
	门诊费用分类名称 9	ans	20
	门诊费用分类代码 9	cn	01
	门诊费用金额 9	cn	04
	门诊费用分类名称 10	ans	20
	门诊费用分类代码 10	cn	01
	门诊费用金额 10	cn	04
	交易信息签名	b	64
	SAM 卡证书	b	190

4.2 应用数据文件(ADF)

ADF 的树形结构：

(1) 能够将数据文件与应用联系起来；

-
- (2) 确保应用之间的独立性;
 - (3) 可以通过应用选择实现对其逻辑结构的访问。

从终端的角度看, ADF 是一个只包含封装在其文件控制信息(FCI)中的数据对象的文件。

4.3 应用基本文件(AEF)

本规范中, 一个 AEF 包含一个或多个原始 BER-TLV 数据对象, 或一个非结构化的纯数据元。在选择了某一应用后, AEF 通过其文件标识符进行查询。

4.4 文件结构映射

使用下列到 GB/T 16649.4 的映射:

- (1) 一个 GB/T 16649.4 定义的专用文件(DF)映射为一个 ADF 或一个 DDF。
可以通过它来访问基本文件和 DF。在 IC 卡中处于最高层的 DF 称为主文件(MF)。
- (2) GB/T 16649.4 定义的一个基本文件(EF) 对应一个 AEF。EF 永远不会成为另一个文件的入口点。

4.5 文件引用

根据文件的种类, 文件可以通过文件名引用。IC 卡中的任何 ADF 或 DDF 都可以通过它的 DF 名引用。ADF 的 DF 名与它的 AID 对应或以 AID 作为 DF 名的开头。一张 IC 卡中的每个 DF 名字必须在该卡内是唯一的。

5 卡操作

5.1 总体操作

包括对居民健康卡用户卡进行寻卡、上电初始化，鉴别卡真伪、有效期、外部认证读写权限，进入相应的读写操作等业务。

5.1.1 总体操作流程

- (1) 用户卡上电复位，卡片位于 MF 下。
- (2) 发送 SELECT 命令，选择居民健康卡应用环境 DDF1。
- (3) 执行内部认证流程，对卡进行内部认证。
- (4) 发送 SELECT 命令，选择 EF05。
- (5) 发送 READ RECORD 命令，读卡有效期。
- (6) 发送 SELECT 命令到各应用文件。
- (7) 根据各应用文件读写控制权限，选择是否进行外部认证。
- (8) 对相应文件进行读写操作。
- (9) 流程结束。

5.1.2 流程图

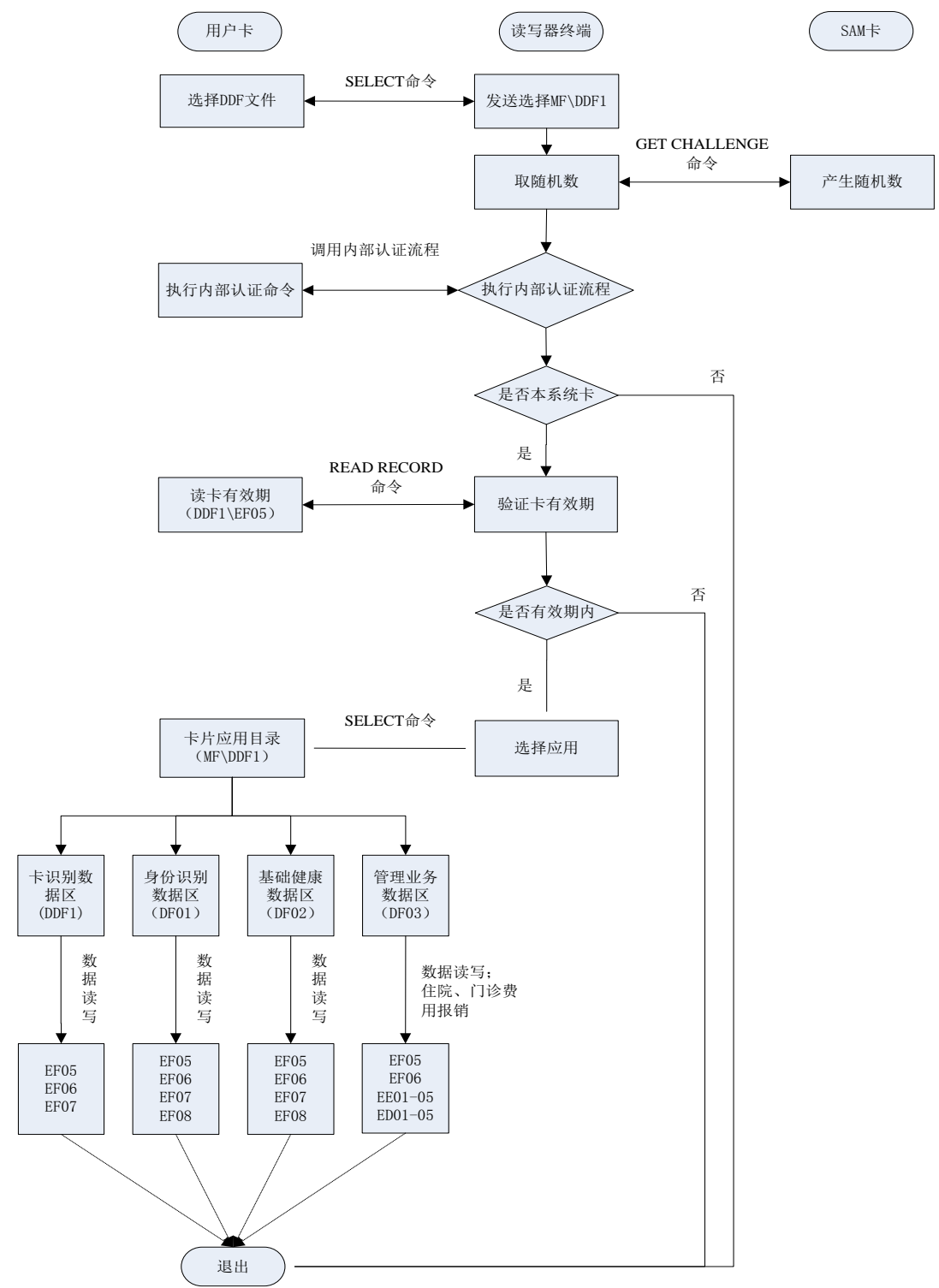


图 5-1 总体应用流程图

5.2 内部认证

内部认证判定用户卡是否本系统卡。

5.2.1 内部认证流程

- (1) 终端从 SAM 卡获取 8 字节随机数。
- (2) 定义 8 字节长度的鉴别所需的原始信息，如 1122334455667788。
- (3) 随机数做为用户卡过程密钥计算使用的数据，同时作为 SAM 卡过程密钥产生因子。
- (4) 终端准备内部认证所需的数据，其中第 1 至第 8 字节为随机数，第 9 至第 16 字节为原始信息，第 17 字节为密钥版本。
- (5) 终端向 SAM 卡发送 DELIVERY SESSION KEY 命令，将指定的密钥进行分散，并产生过程密钥。
- (6) 终端向 SAM 卡发送 CIPHER DATA 命令，加密原始信息。
- (7) 终端将 SAM 卡返回的加密结果左右 8 字节异或，得到鉴别数据 A。
- (8) 终端向用户卡发送 INTERNAL AUTHENTICATION 命令，得到返回值 B。
- (9) 终端比较 A、B 值是否相同，如果相同内部认证成功，否则内部认证失败。
- (10) 流程结束。

5.2.2 流程图

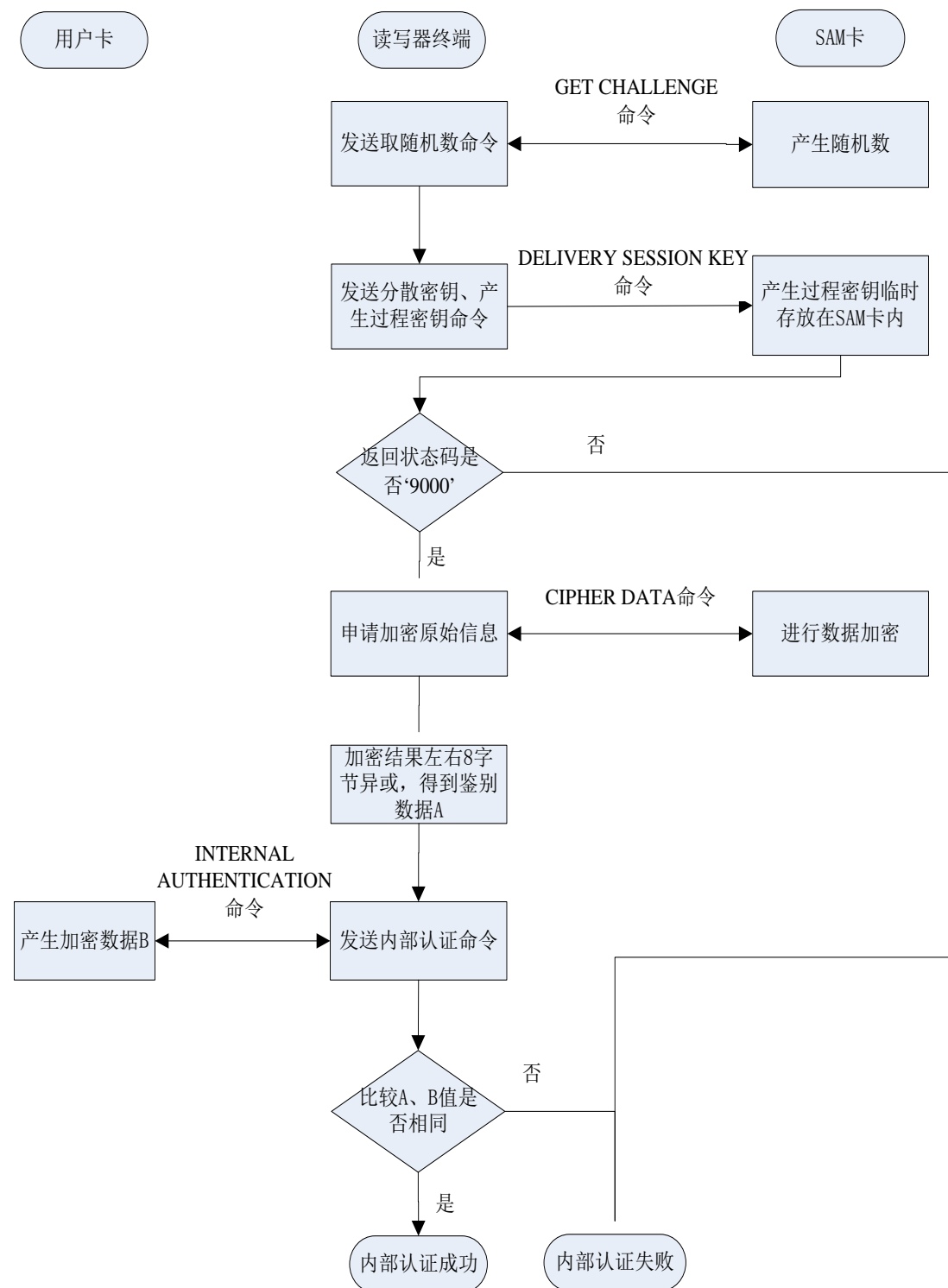


图 5-2 内部认证流程图

5.3 外部认证

用户卡只有通过相应控制密钥的外部认证后，才可以对相应的文件进行读写等操作。

5.3.1 外部认证流程

- (1) 定义 8 字节长度的鉴别所需的原始信息，如 1122334455667788。
- (2) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数。
- (3) 随机数做为 SAM 卡过程密钥产生因子。
- (4) 终端向 SAM 卡发送 DELIVERY SESSION KEY 命令，将指定的密钥进行分散，并产生过程密钥。
- (5) 终端向 SAM 卡发送 CIPHER DATA 命令，加密原始信息。
- (6) 终端将 SAM 卡返回的加密结果左右 8 字节异或，得到鉴别数据。
- (7) 终端准备外部认证所需的数据，其中第 1 至第 8 字节为鉴别数据，第 9 至第 16 字节为原始信息，第 17 字节为密钥版本。
- (8) 终端向用户卡发送 EXTERNAL AUTHENTICATION 命令。
- (9) 用户卡返回状态码如为‘9000’，则外部认证成功，否则外部认证失败。
- (10) 流程结束。

5.3.2 流程图

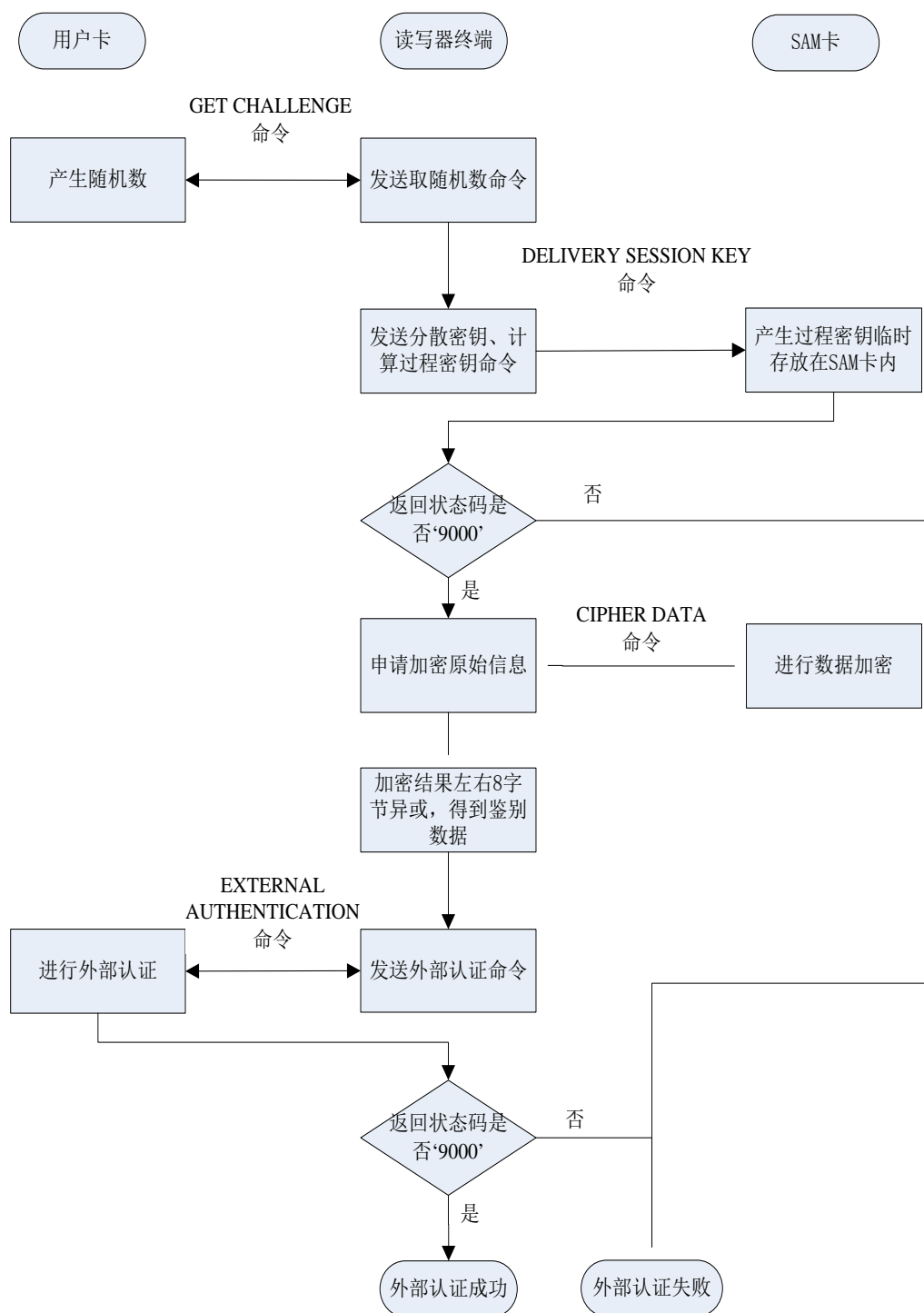


图 5-3 外部认证流程图

5.4 应用锁定

向用户卡发送应用锁定命令可以对卡进行临时锁定或永久锁定。临时锁定方式后可以用应用解锁命令进行解锁，永久锁定方式后不能解锁。另外当使用

校验方式更新记录文件或二进制文件时，如果 MAC 错误尝试次数超过限制，COS 会自动临时锁定当前应用。

5.4.1 应用锁定流程

- (1) 终端向用户卡发送 SELECT 命令，选择待锁定的应用区（DF）。
- (2) 终端执行外部认证流程，对该 DF 下的 LK 密钥进行外部认证。
- (3) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数。
- (4) 随机数做为 SAM 卡过程密钥产生因子。
- (5) 终端向 SAM 卡发送 DELIVERY SESSION KEY 命令，将指定的 STK 密钥进行分散，并产生过程密钥。
- (6) 终端向 SAM 卡发送 CIPHER DATA 命令，对应用锁定（APPLICATION BLOCK）命令头进行 MAC 计算。
- (7) 终端向用户卡发送 APPLICATION BLOCK 命令 +MAC 值，对该 DF 进行应用锁定。

5.5 应用解锁

临时锁定后的用户卡应用区，只有该应用区进行应用解锁后，才可以继续使用。

5.5.1 应用解锁流程

- (1) 终端向用户卡发送 SELECT 命令，选择被临时锁定的应用区（DF）。
- (2) 终端执行外部认证流程，对该 DF 下的 LK 密钥进行外部认证。
- (3) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数。
- (4) 随机数做为 SAM 卡过程密钥产生因子。
- (5) 终端向 SAM 卡发送 DELIVERY SESSION KEY 命令，将指定的 STK 密钥进行分散，并产生过程密钥。
- (6) 终端向 SAM 卡发送 CIPHER DATA 命令，对应用解锁（APPLICATION UNBLOCK）命令头进行 MAC 计算。
- (7) 终端向用户卡发送 APPLICATION UNBLOCK 命令 +MAC 值，对该 DF 进行应用解锁。

5.6 卡锁定

用户卡不允许再使用时，可以执行卡锁定命令，对该用户卡进行永久卡锁定，卡锁定后不能解锁。

5.6.1 卡锁定流程

- (1) 终端向用户卡发送 SELECT 命令，选择待锁定的卡片根目录（MF）。
- (2) 终端执行外部认证流程，对 MF 下的 BK 密钥进行外部认证。
- (3) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数。
- (4) 随机数做为 SAM 卡过程密钥产生因子。
- (5) 终端向 SAM 卡发送 DELIVERY SESSION KEY 命令，将指定的 STK 密钥进行分散，并产生过程密钥。
- (6) 终端向 SAM 卡发送 CIPHER DATA 命令，对卡锁定（CARD BLOCK）命令头进行 MAC 计算。
- (7) 终端向用户卡发送 CARD BLOCK 命令 +MAC 值，对该用户卡进行卡锁定。

5.7 应用维护

应用维护包括卡锁定、应用锁定、应用解锁、数据带 MAC 更新。这些过程必须在拥有相应的操作权限控制密钥的终端上按如下步骤执行：

- (1) 通过外部认证，满足操作的安全状态；
- (2) 终端向卡申请一随机数；
- (3) 发送相应的应用维护命令，卡在收到命令后执行以下操作：
 - a. 使用前一步骤产生的随机数，利用《居民健康卡技术规范》中 9.6 节描述的方式产生过程密钥；
 - b. 使用该过程密钥产生 MAC，并与命令报文中的 MAC 进行比较，如果结果一致，则相应的功能被实现，否则回送错误状态信息。MAC 产生方式见《居民健康卡技术规范》中 9.4 节描述。

6 卡业务应用

在卡业务应用过程中，向 SAM 卡发送应用命令需要满足《居民健康卡安全存取模块（SAM）卡命令集》中第 8 章关于命令使用条件的要求。

6.1 卡识别应用 (对应 MF\DDF1 数据区)

读写卡识别数据区内的数据，卡识别数据区包括发卡基本数据（EF05）和持卡人基本数据（EF06）、照片数据（EF07）和持卡人支付信息数据（EF08）。

6.1.1 读卡识别数据区信息

6.1.1.1 描述

读取用户卡中 MF\DDF1 中的基本文件(即 EF05、EF06、EF07 和 EF08)数据。

6.1.1.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.1.1.3 处理流程

- (1) 终端根据应用执行的情况决定从用户卡读取哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对文件的读控制密钥的情况，决定是否执行外部认证。（读控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送 READ RECORD 命令读取指定记录，读照片信息，则发送 READ BINARY 命令读取数据。
- (5) 用户卡根据读记录所需的读控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则用户卡读取记录数据，读取成功则返回记录数据到终端，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续读取对应 EF 文件中的记录。

6.1.1.4 流程图

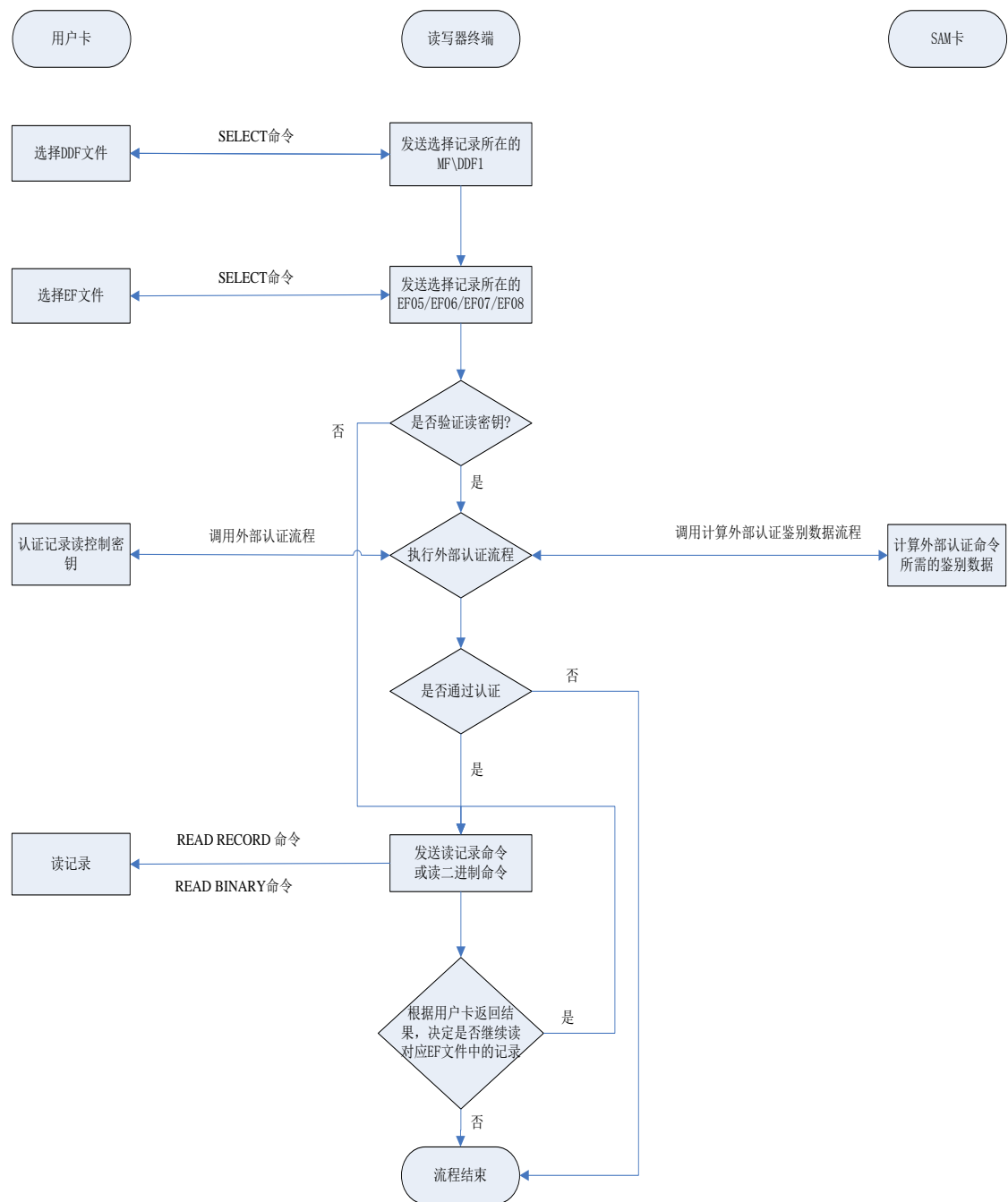


图 6-1 读卡识别数据流程图

6.1.2 写卡识别数据区信息

6.1.2.1 描述

更新用户卡中 MF\DDF1 中的基本文件(即 EF07 和 EF08)数据。

6.1.2.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.1.2.3 处理流程

- (1) 终端根据应用执行的情况决定更新用户卡中哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对应用文件的写控制密钥的情况，决定是否执行外部认证。（写控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送带密文+MAC 安全报文的 UPDATE RECORD 命令更新指定记录，在这一过程中，使用 STK_{DDFI} 计算密文及 MAC；终端发送 UPDATE BINARY 命令更新 EF07 数据。
- (5) 用户卡根据写记录所需的写控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则验证密文和 MAC 是否正确（密文和 MAC 的计算方法和步骤参见《居民健康卡技术规范》9.4 节描述），如果正确，则将解密后的明文数据写入卡内，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续更新对应 EF 文件中的记录。

6.1.2.4 流程图

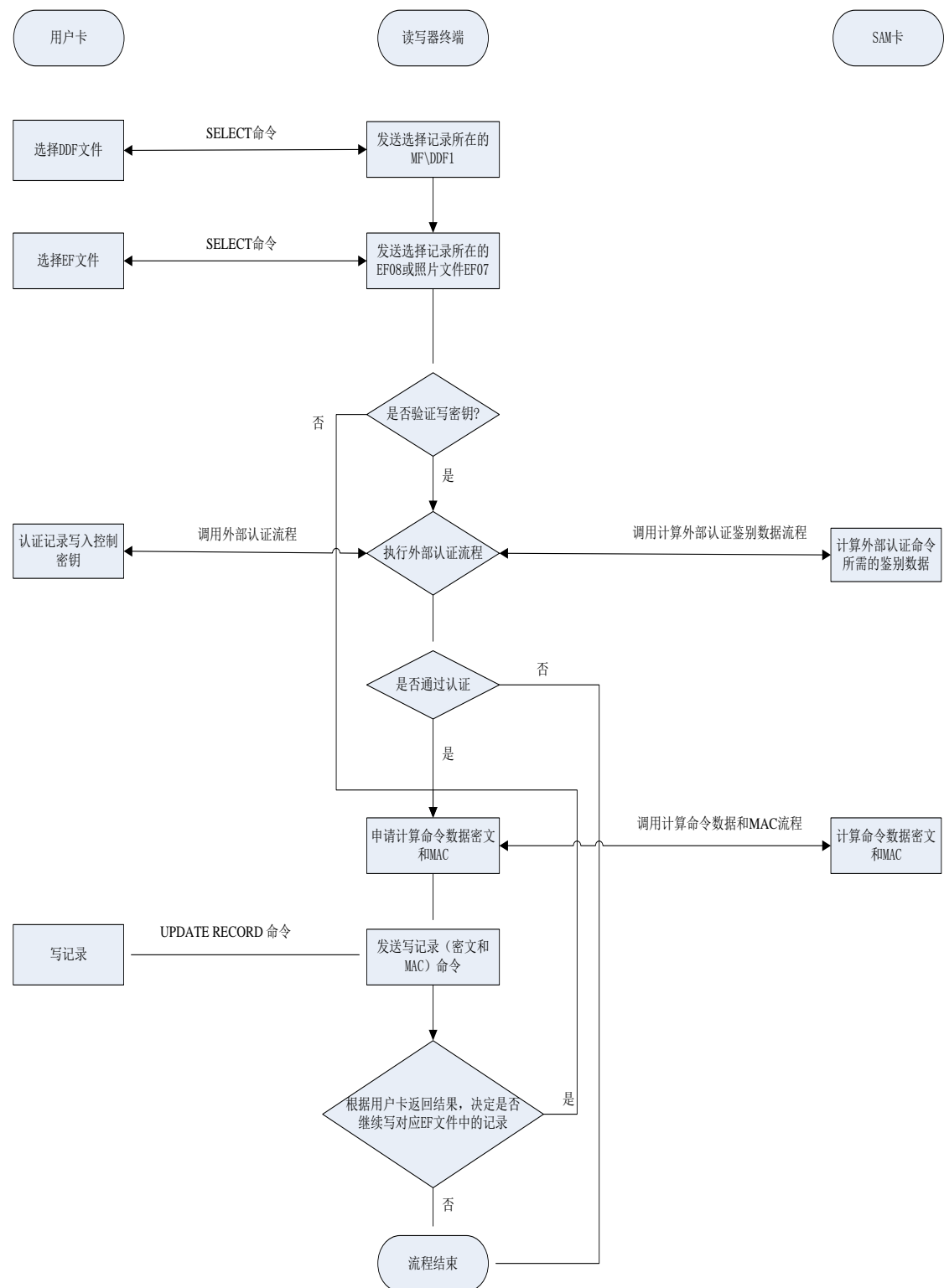


图 6-2 写卡识别数据处理流程图

6.2 身份识别应用（对应 DDF1\DF01 数据区）

读写身份识别数据区内的数据，身份识别数据区包括 EF05、EF06、EF07 和 EF08 文件。

6.2.1 读 DF01 应用数据

6.2.1.1 描述

读取用户卡中的 DF01 应用数据。

6.2.1.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.2.1.3 处理流程

- (1) 终端根据应用执行的情况决定从用户卡读取哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对应用文件的读控制密钥的情况，决定是否执行外部认证。（读控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送 READ RECORD 命令读取指定记录。
- (5) 用户卡根据读记录所需的读控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则用户卡读取记录数据，读取成功则返回记录数据到终端，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续读取对应 EF 文件中的记录。

6.2.1.4 流程图

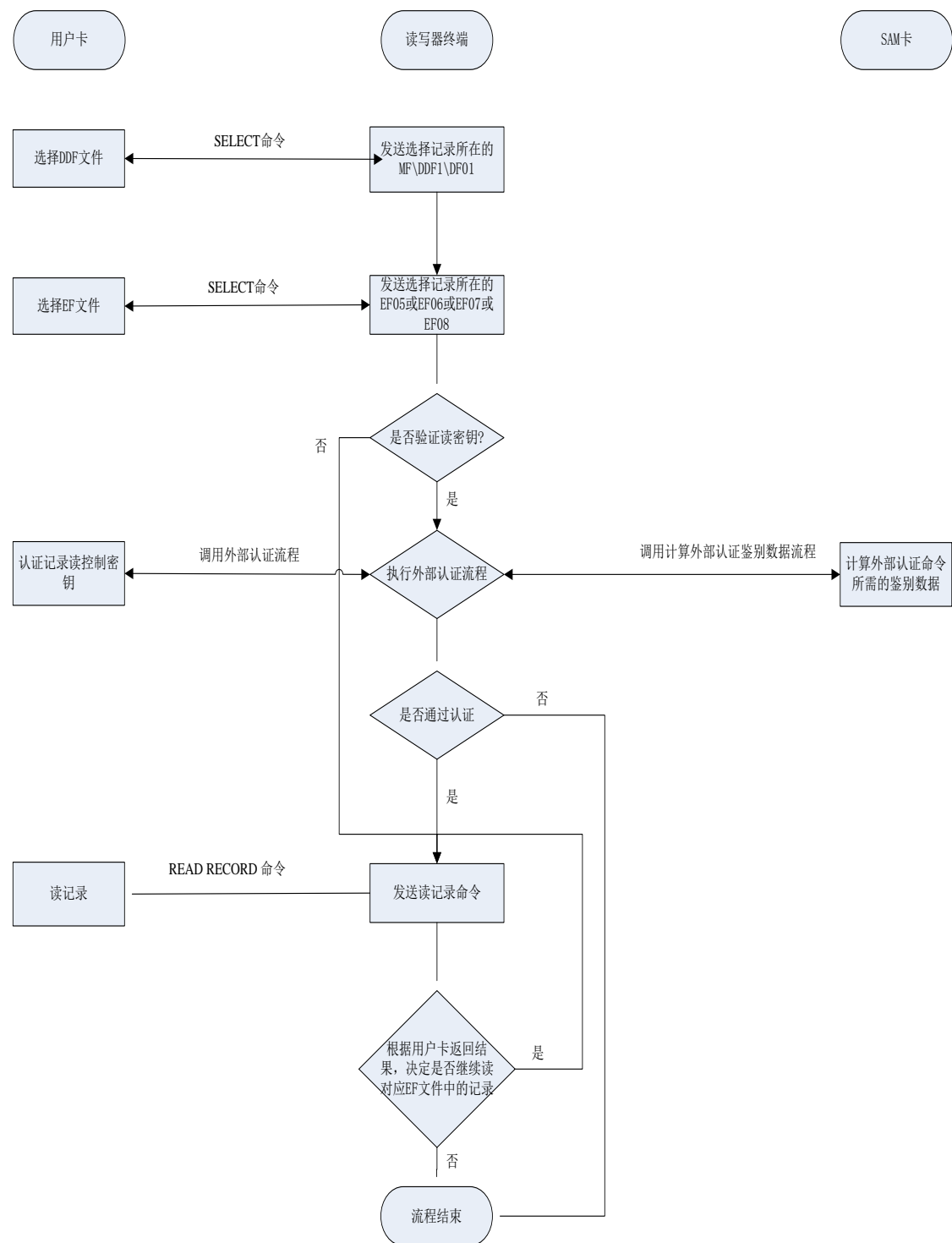


图 6-3 读 DF01 应用数据处理流程图

6.2.2 写 DF01 应用数据

6.2.2.1 描述

更新用户卡中的 DF01 应用数据。

6.2.2.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.2.2.3 处理流程

- (1) 终端根据应用执行的情况决定更新用户卡中哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对应用文件的写控制密钥的情况，决定是否执行外部认证。（写控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送带密文+MAC 安全报文的 UPDATE RECORD 命令更新指定记录。
- (5) 用户卡根据写记录所需的写控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则验证密文和 MAC 是否正确（密文和 MAC 的计算方法和步骤参见《居民健康卡技术规范》9.4 节描述），如果正确，则将解密后的明文数据写入卡内，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续更新对应 EF 文件中的记录。

6.2.2.4 流程图

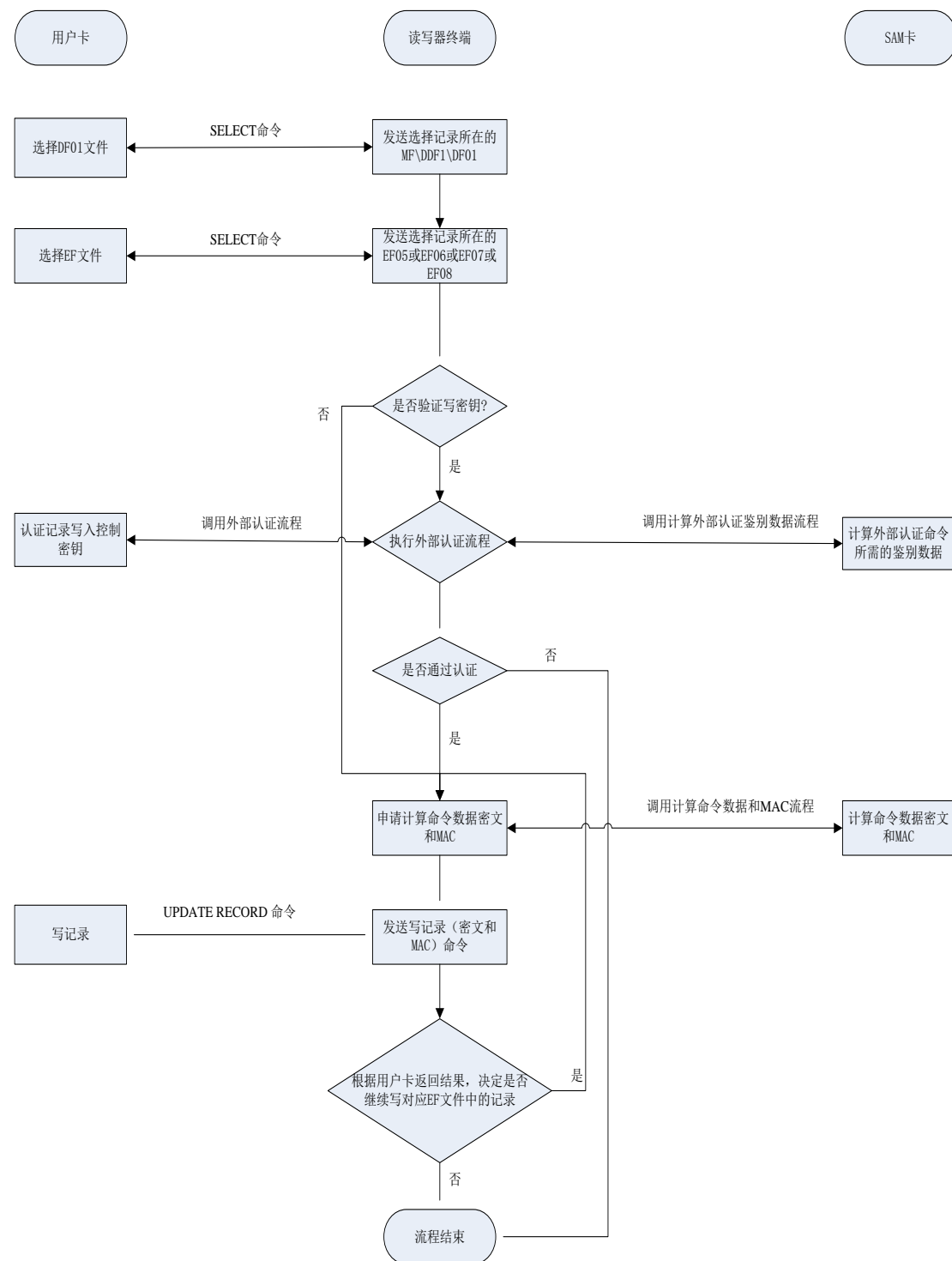


图 6-4 写 DF01 应用数据处理流程图

6.3 基础健康信息应用（对应 DDF1\DF02 数据区）

读写基础健康信息区内的数据，基础健康信息区包括 EF05、EF06、EF07 和 EF08 文件。

6.3.1 读 DF02 应用数据

6.3.1.1 描述

读取用户卡中的 DF02 应用数据。

6.3.1.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.3.1.3 处理流程

- (1) 终端根据应用执行的情况决定从用户卡读取哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对应文件的读控制密钥的情况，决定是否执行外部认证。（读控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送 READ RECORD 命令读取指定记录。
- (5) 用户卡根据读记录所需的读控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则用户卡读取记录数据，读取成功则返回记录数据到终端，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续读取对应 EF 文件中的记录。

6.3.1.4 流程图

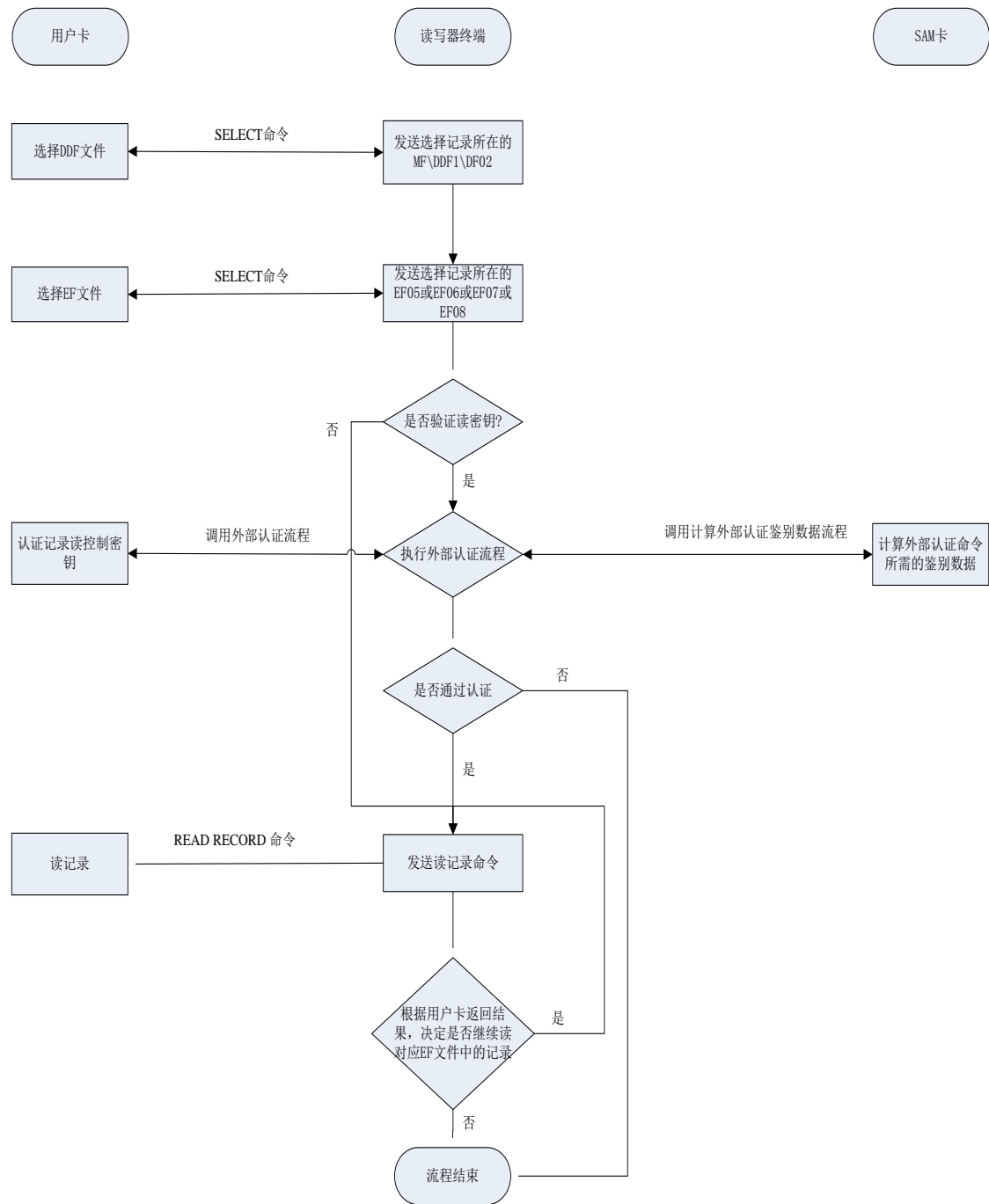


图 6-5 读 DF02 应用数据处理流程图

6.3.2 写 DF02 应用数据

6.3.2.1 描述

更新用户卡中的 DF02 应用数据。

6.3.2.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.3.2.3 处理流程

- (1) 终端根据应用执行的情况决定更新用户卡中哪些记录。
- (2) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件。
- (3) 终端根据应用执行情况和《居民健康卡技术规范》中定义的对应用文件的写控制密钥的情况，决定是否执行外部认证。（写控制密钥的情况参见《居民健康卡技术规范》，外部认证命令处理过程参见本文档的对应章节）。
- (4) 终端发送带密文+MAC 安全报文的 UPDATE RECORD 命令更新指定记录。
- (5) 用户卡根据写记录所需的写控制权限，判断命令执行的条件是否满足，如果不满足则返回错误码到终端；如果满足则验证密文和 MAC 是否正确（密文和 MAC 的计算方法和步骤参见《居民健康卡技术规范》9.4 节描述），如果正确，则将解密后的明文数据写入卡内，否则返回错误码到终端。
- (6) 终端根据用户卡返回结果，决定是否继续更新对应 EF 文件中的记录。

6.3.2.4 流程图

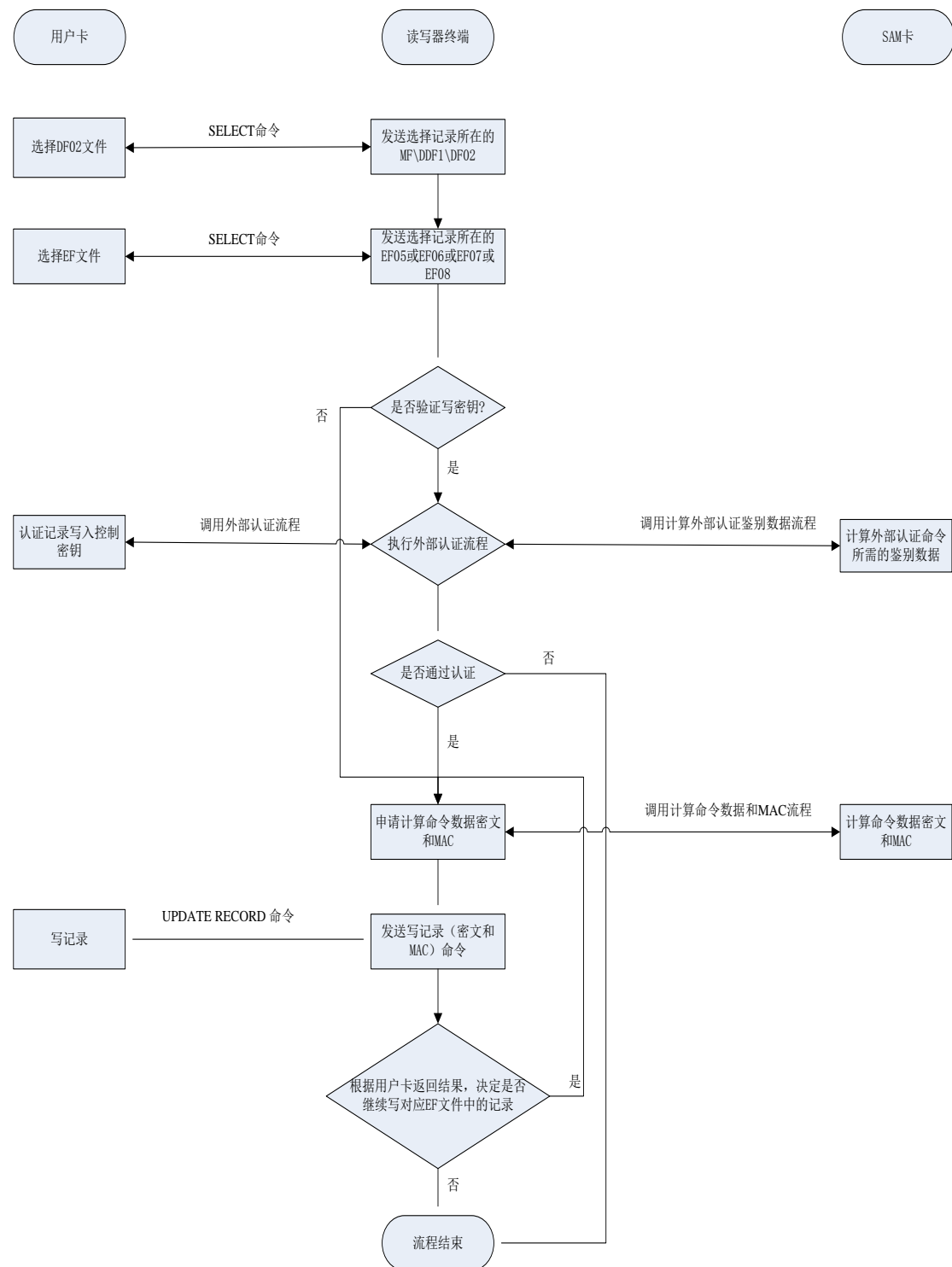


图 6-6 写 DF02 应用数据处理流程图

6.4 管理业务应用(对应 DDF1\DF03 数据区)

包括对住院信息和门诊信息的记录、提取和报销。MAC 的计算方法和步骤参见《居民健康卡技术规范》9.4 节描述。对住院信息和门诊信息进行签名时的 SAM 卡证书数据，从 SAM 卡的 SAM 卡证书文件中读取，SAM 卡证书文件参见《居民健康卡安全存取模块（SAM）卡技术规范》相应描述。

6.4.1 记录住院信息

6.4.1.1 描述

读写用户卡中住院信息索引文件(DF03\EF05)及住院信息(DF03\EE01-03)。

6.4.1.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.4.1.3 记录住院信息流程

- (1) 终端获得住院信息索引文件读权限。
- (2) 终端向用户卡发送 SELECT 命令，选择住院信息索引文件，从第一条记录开始搜索到第一个值为空（‘FF’）的记录，根据这条记录的记录号 RN 确定住院信息文件的文件标识符 FID（‘EE’+RN）。
- (3) 如果没有空记录，则无法记录住院信息，流程结束。
- (4) 终端获得住院信息文件写权限。
- (5) 终端向用户卡发送 SELECT 命令，选择住院信息文件。
- (6) 终端执行数据签名流程，将待签名的住院信息数据发送到 SAM 卡进行签名，得到 64 字节签名值。
- (7) 终端向用户卡发送 UPDATE BINARY 命令，写入本次住院信息、签名值和 SAM 卡证书数据。
- (8) 终端向用户卡发送 SELECT 命令，选择住院信息索引文件。
- (9) 终端向用户卡发送带 MAC 安全报文的 WRITE RECORD 命令，写入院索引信息文件第 RN 条记录。
- (10) 流程结束。

6.4.1.4 流程图

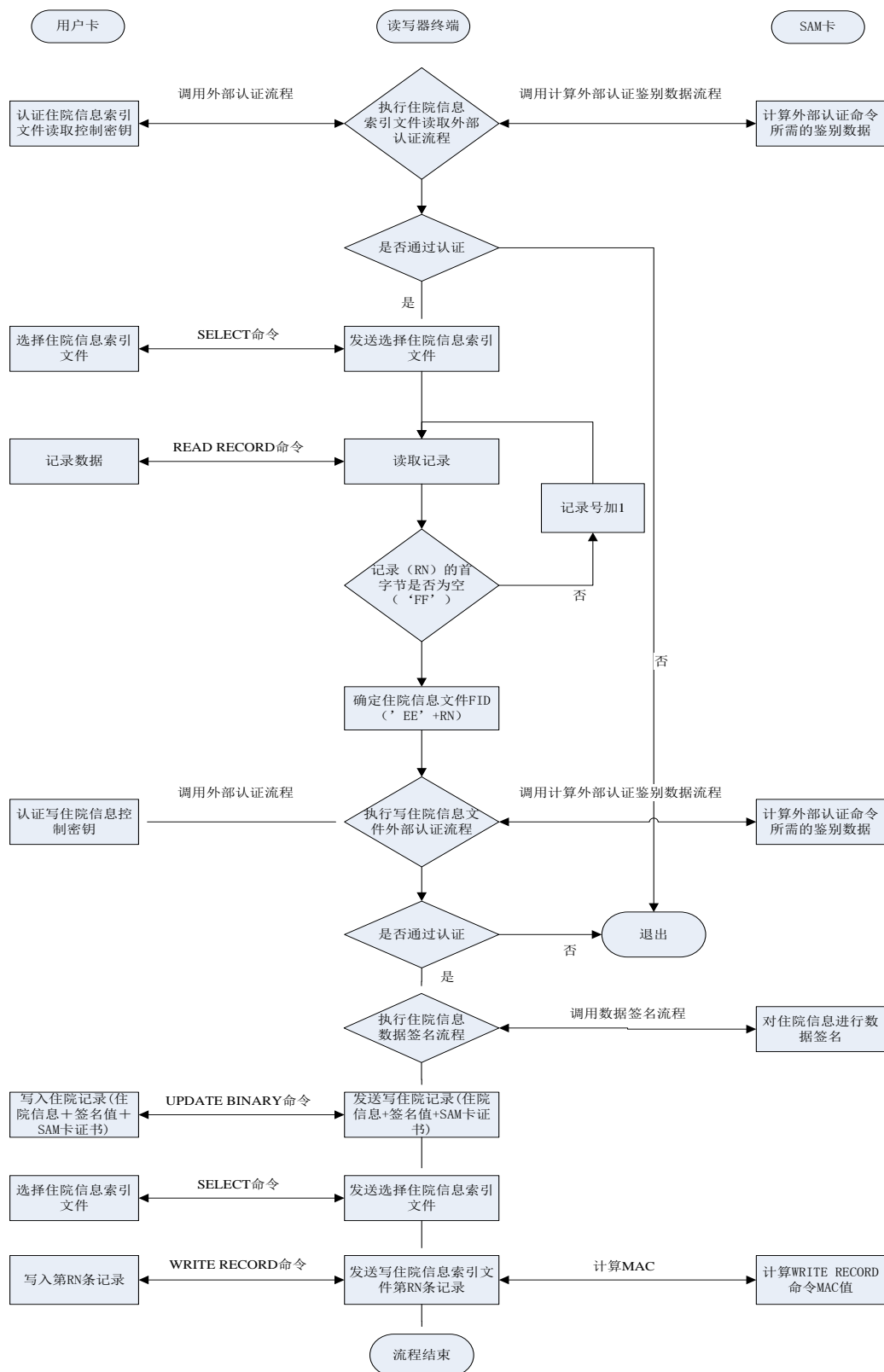


图 6-7 住院信息记录流程图

6.4.2 记录门诊信息

6.4.2.1 描述

读写用户卡中门诊信息索引文件（DF03\EF06）及门诊信息（DF03\ED01-05）。

6.4.2.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.4.2.3 记录门诊信息流程

- (1) 终端获得门诊信息索引文件读权限。
- (2) 终端向用户卡发送 SELECT 命令，选择门诊信息索引文件，从第一条记录开始搜索到第一个值为空（‘FF’）的记录，根据这条记录的记录号 RN 确定门诊信息文件的文件标识符 FID（‘ED’+RN）。
- (3) 如果没有空记录，则无法记录门诊信息，流程结束。
- (4) 终端获得门诊信息文件写权限。
- (5) 终端向用户卡发送 SELECT 命令，选择门诊信息文件。
- (6) 终端执行数据签名流程，将待签名的门诊信息数据发送到 SAM 卡进行签名，得到 64 字节签名值。
- (7) 终端向用户卡发送 UPDATE BINARY 命令，写入本次门诊信息、签名值和 SAM 卡证书数据。
- (8) 终端向用户卡发送 SELECT 命令，选择门诊信息索引文件。
- (9) 终端向用户卡发送带 MAC 安全报文的 WRITE RECORD 命令，写入门诊索引信息文件第 RN 条记录。
- (10) 流程结束。

6.4.2.4 流程图

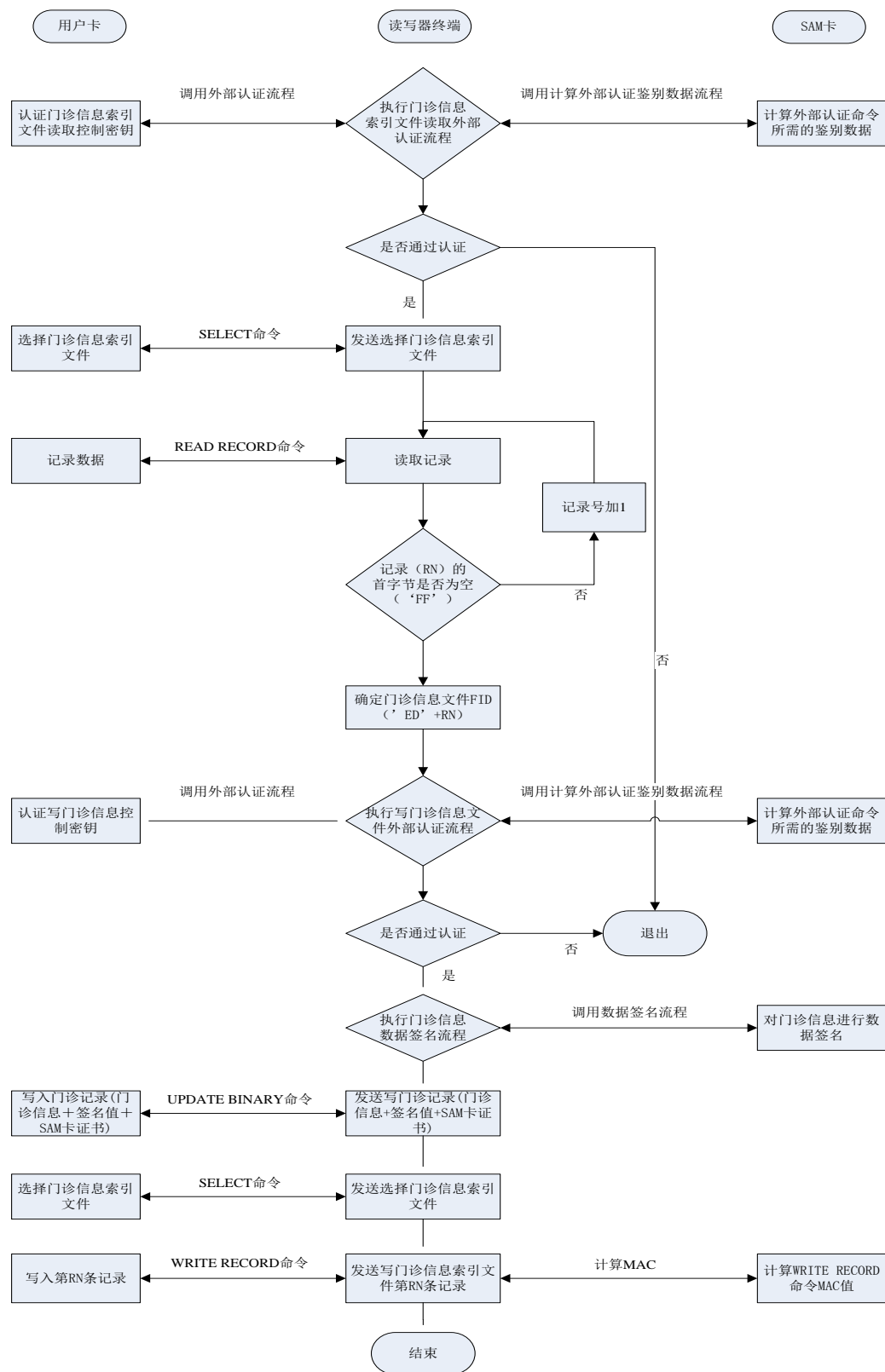


图 6-8 门诊信息记录流程图

6.4.3 住院费用信息提取及费用报销

6.4.3.1 描述

本部分描述了住院费用提取及报销的简易流程。

6.4.3.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.4.3.3 住院费用信息提取及报销流程

- (1) 终端获得住院信息索引文件（DF03\EF05）读权限。
- (2) 终端向用户卡发送 **SELECT** 命令，选择住院信息索引文件，从第一条记录开始搜索不为空（‘00’）的记录，根据这条记录的记录号 **RN** 确定住院信息文件的文件标识符 **FID**（‘EE’+RN）。
- (3) 终端向用户卡发送 **SELECT** 命令，选择住院信息文件。
- (4) 终端向用户卡发送 **READ BINARY** 命令，读取住院记录数据（住院信息、签名值和 **SAM** 卡证书）。
- (5) 终端将住院记录数据发送到后台，由后台验证签名的有效性。
- (6) 终端根据后台返回结果，判断住院记录数据签名验证是否成功。
- (7) 终端获得住院信息索引文件擦除权限。
- (8) 终端向用户卡发送 **SELECT** 命令，选择住院信息索引文件。
- (9) 终端向用户卡发送带 **MAC** 安全报文的 **ERASE RECORD** 命令，擦除住院索引信息文件第 **RN** 条记录有效标志。
- (10) 流程结束。

6.4.3.4 流程图

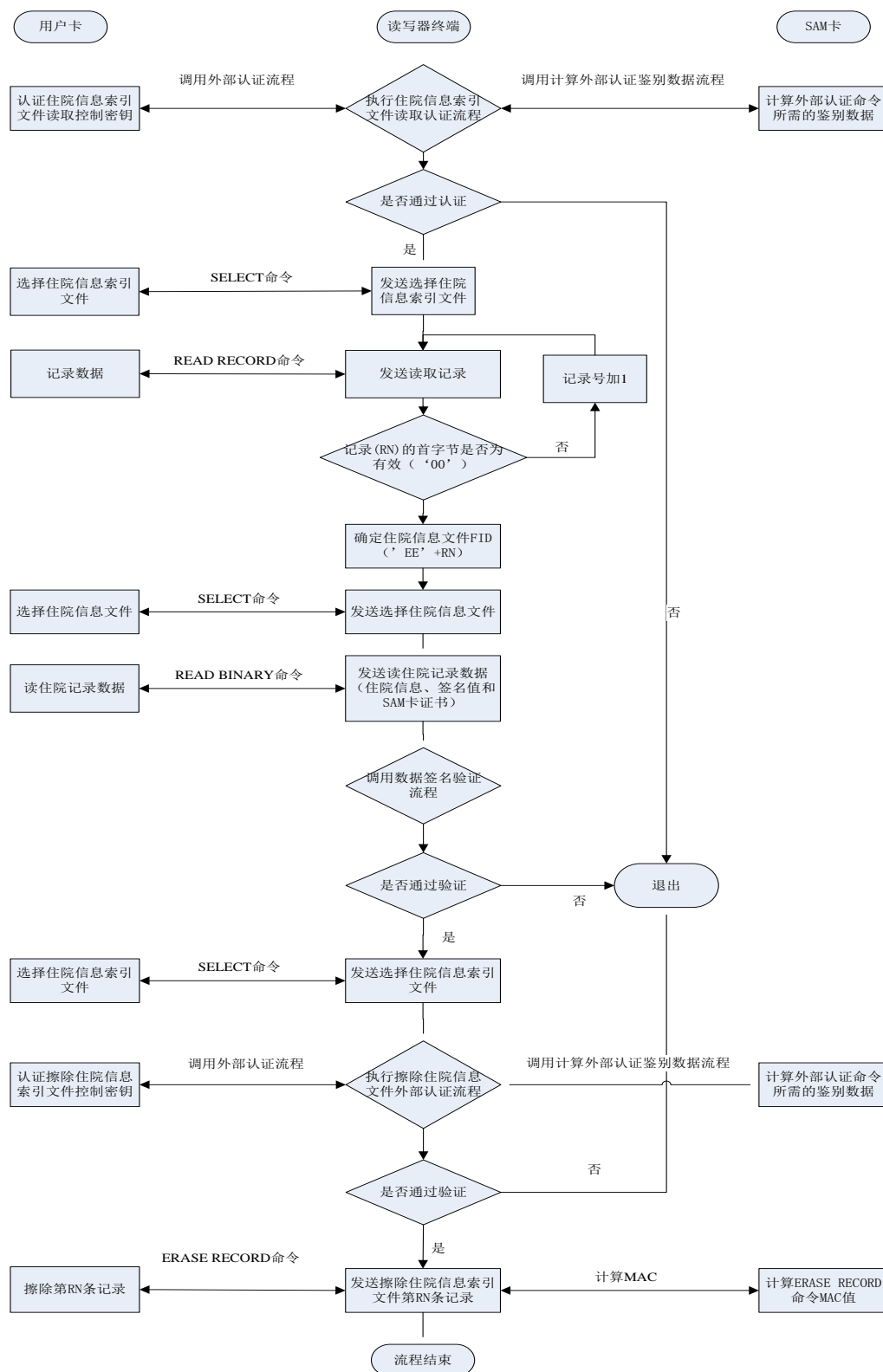


图 6-9 住院费用提取及报销流程图

6.4.4 门诊费用信息提取及报销

6.4.4.1 描述

本部分描述了门诊费提取及报销的简易流程。

6.4.4.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

6.4.4.3 门诊费用提取及报销流程

- (1) 终端获得门诊信息索引文件（DF03\EF06）读权限。
- (2) 终端向用户卡发送 **SELECT** 命令，选择门诊信息索引文件，从第一条记录开始搜索不为空（‘00’）的记录，根据这条记录的记录号 **RN** 确定门诊信息文件的文件标识符 **FID**（‘ED’+RN）。
- (3) 终端向用户卡发送 **SELECT** 命令，选择门诊信息文件。
- (4) 终端向用户卡发送 **READ BINARY** 命令，读取门诊记录数据（门诊信息、签名值和 **SAM** 卡证书）。
- (5) 终端将门诊记录数据发送到后台，由后台验证签名的有效性。
- (6) 终端根据后台返回结果，判断门诊记录数据签名验证是否成功。
- (7) 终端获得门诊信息索引文件擦除权限。
- (8) 终端向用户卡发送 **SELECT** 命令，选择门诊信息索引文件。
- (9) 终端向用户卡发送带 **MAC** 安全报文的 **ERASE RECORD** 命令，擦除门诊索引信息文件第 **RN** 条记录有效标志。
- (10) 流程结束。

6.4.4.4 流程图

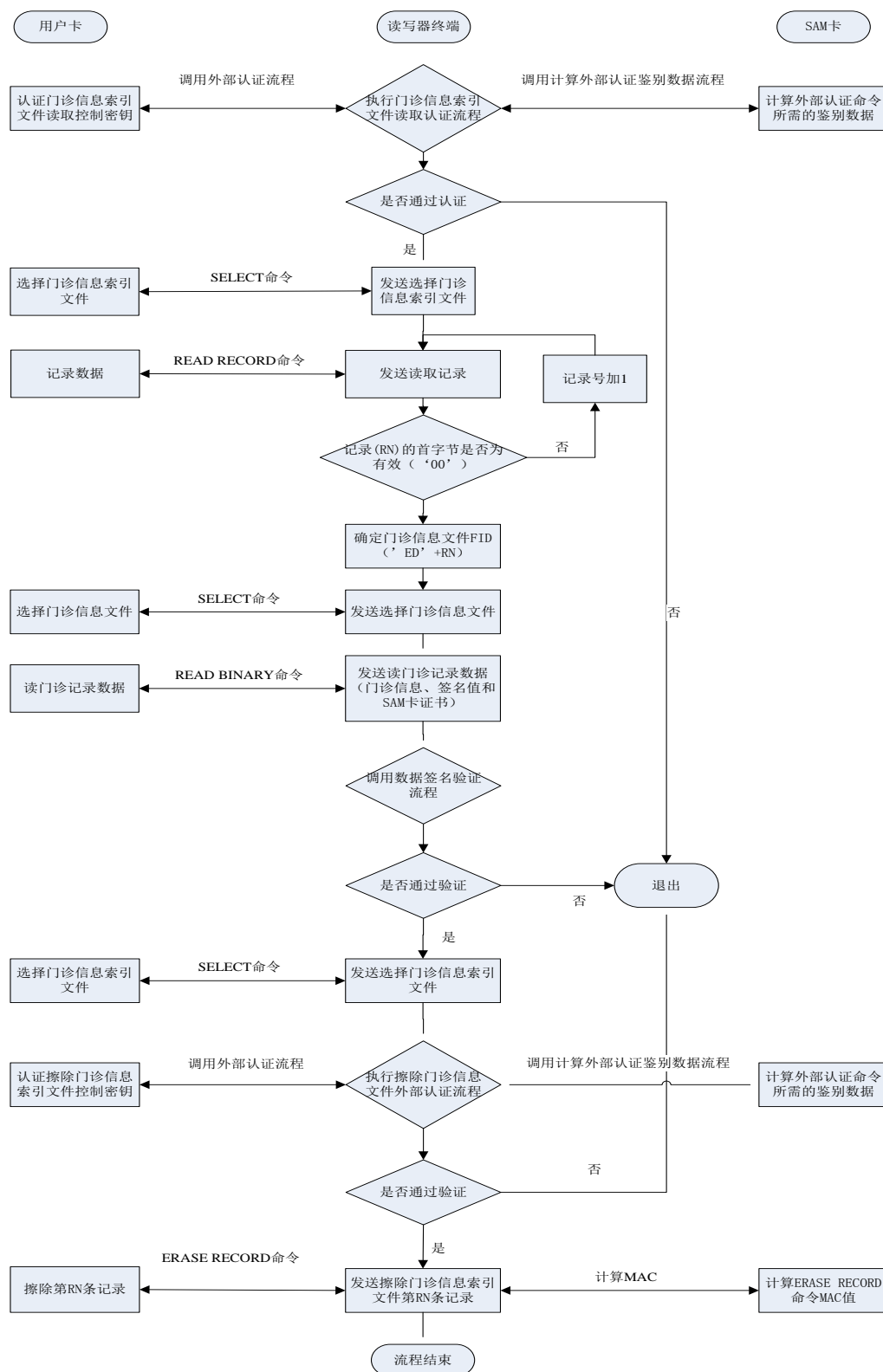


图 6-10 门诊费用提取及报销流程图

7 数据签名和验证

7.1 数据签名

7.1.1 描述

住院信息或门诊信息写入到用户卡时需要进行数据签名，以保证数据的真实性和完整性。待签名数据为住院（或门诊）信息文件中除签名值和 SAM 卡证书之外的所有数据项内容。

7.1.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

7.1.3 数据签名流程

- (1) 终端获得需签名的住院（或门诊）信息数据。
- (2) 终端向 SAM 卡发送 SELECT 命令，选择 SAM 卡 DF01 目录。
- (3) 终端将获得的住院（或门诊）信息记录数据分组，向 SAM 卡循环发送 DATA COMPRESS 命令，使用 SM3 算法计算，得到 32 字节哈希值。
- (4) 终端向 SAM 卡发送 DIGITAL SIGNATURES 命令，用私钥对哈希值做签名，得到 64 字节签名值。
- (5) 流程结束。

7.1.4 流程图

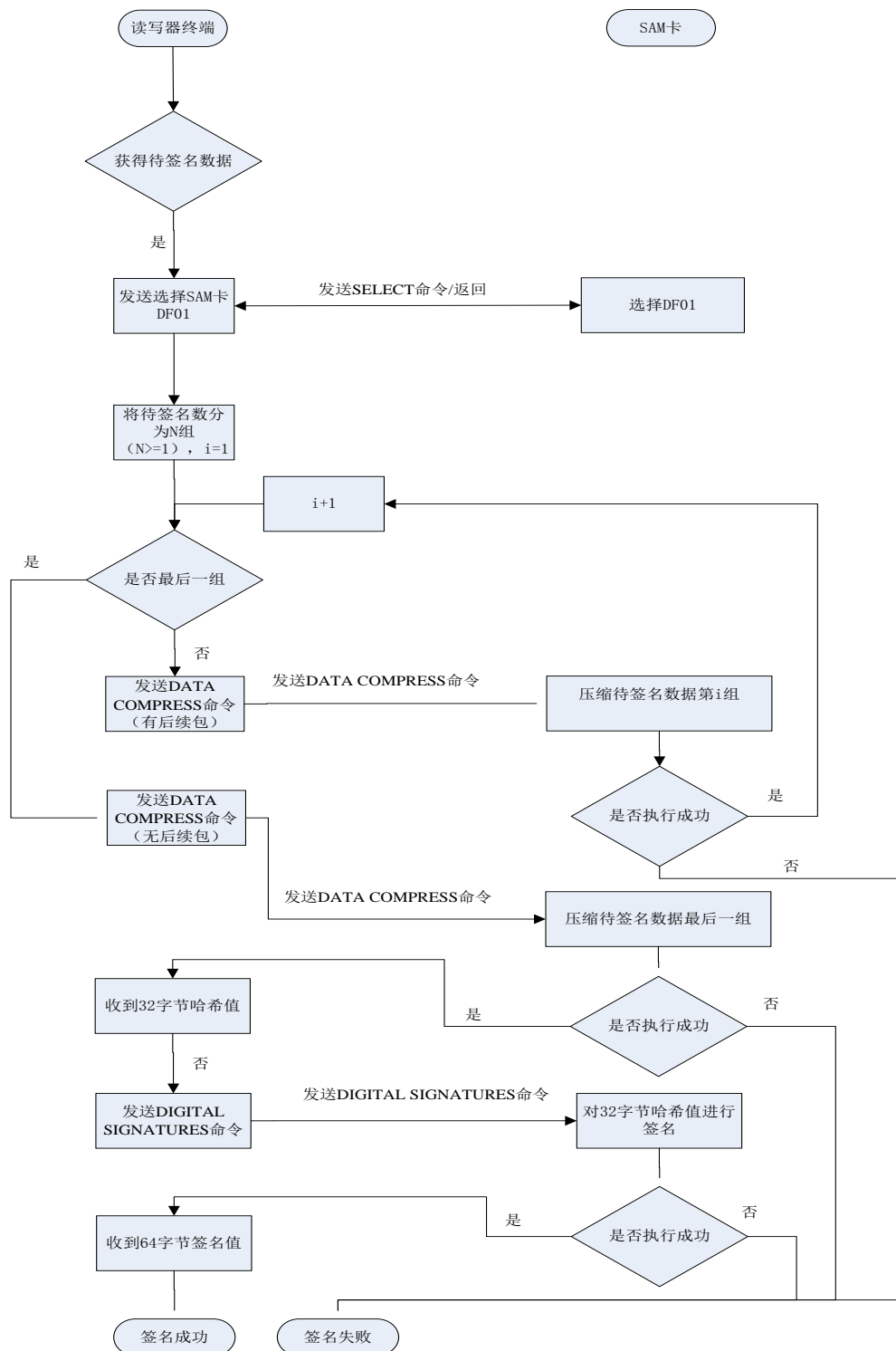


图 7-1 数据签名流程图

7.2 数据签名验证

7.2.1 描述

本部分描述了数据签名验证的流程。通过验证数据签名，保证数据真实，没有被篡改。验证签名数据为住院（或门诊）信息文件的住院（或门诊）信息的记录、交易签名和 SAM 卡证书。

7.2.2 命令

参见《居民健康卡用户卡命令集》和《居民健康卡安全存取模块（SAM）卡命令集》。

7.2.3 数据签名验证流程

证书密钥的使用参见《居民健康卡技术规范》中 9.10.2.2 节。

- (1) 终端读取用户卡住院（或门诊）信息文件的住院（或门诊）信息的记录、交易签名和 SAM 卡证书，并将上述三项数据项发到后台，由后台进行数据签名验证。
- (2) 后台将验证结果发送到终端。
- (3) 终端根据返回结果判断数据签名验证是否成功。
- (4) 流程结束。

7.2.4 流程图

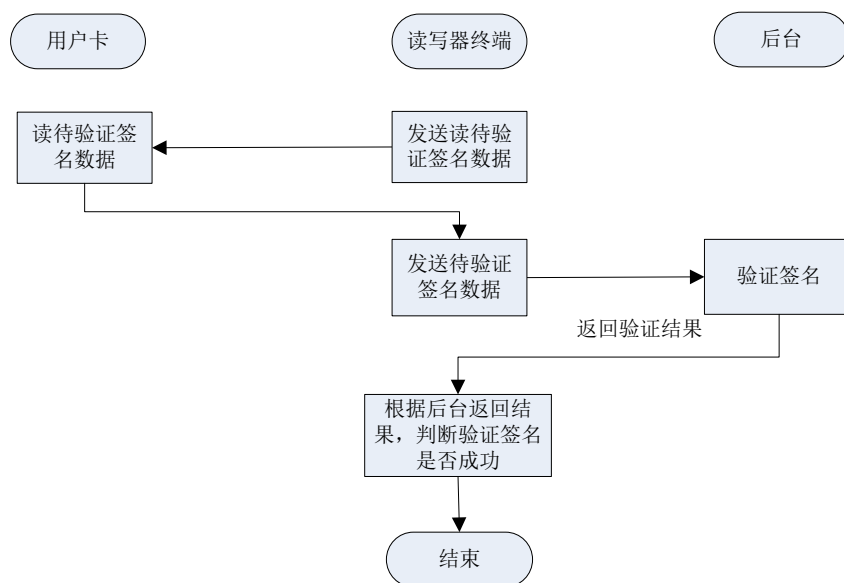


图 7-2 数据签名验证流程图