ICS 11.120
C 07

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXXXX.2—XXXX

居民健康卡技术规范
第2部分：用户卡应用规范

Residents' health card technical specifications

Part 2：Application specification of the user card

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家卫生和计划生育委员会
发 布

前　　言

WS XXXXX《居民健康卡技术规范》现分为以下部分：

——第1部分：用户卡技术规范

——第2部分：用户卡应用规范

——第3部分：用户卡命令集

——第4部分：终端技术规范

——第5部分：用户卡及终端产品检测规范

……

本部分为 WS XXXXX 的第2部分。

本部分由国家卫生和计划生育委员会卫生信息标准专业委员会提出。

本部分主要起草单位：

本部分主要起草人：

居民健康卡技术规范

第 2 部分：用户卡应用规范

1 适用范围

本部分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。

本部分适用于所有制作、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、维护等单位和部门。

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 16649.4—2010　　识别卡带触点的集成电路卡第 4 部分

WS XXXXX.1-2013　　居民健康卡技术规范 第 1 部分 用户卡技术规范

WS XXXXX.3-2013　　居民健康卡技术规范 第 3 部分 用户卡命令集

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

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。

3.1.7

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。

3.1.8

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.1.9

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/解密密钥是相同的。

3.1.10

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。

3.1.11

密钥 key

加密转换中控制操作的符号序列。

3.1.12

对称密钥 symmetric key

在对称加密算法中使用的密钥。

3.1.13

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。

3.1.14

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。

3.1.15

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。

3.1.16

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。

3.1.17

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。

3.1.18

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部分。

缩略语和符号见表3-1。

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

本部分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部分的应用文件结构，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。

居民健康卡文件结构示意图如图4-1所示 。

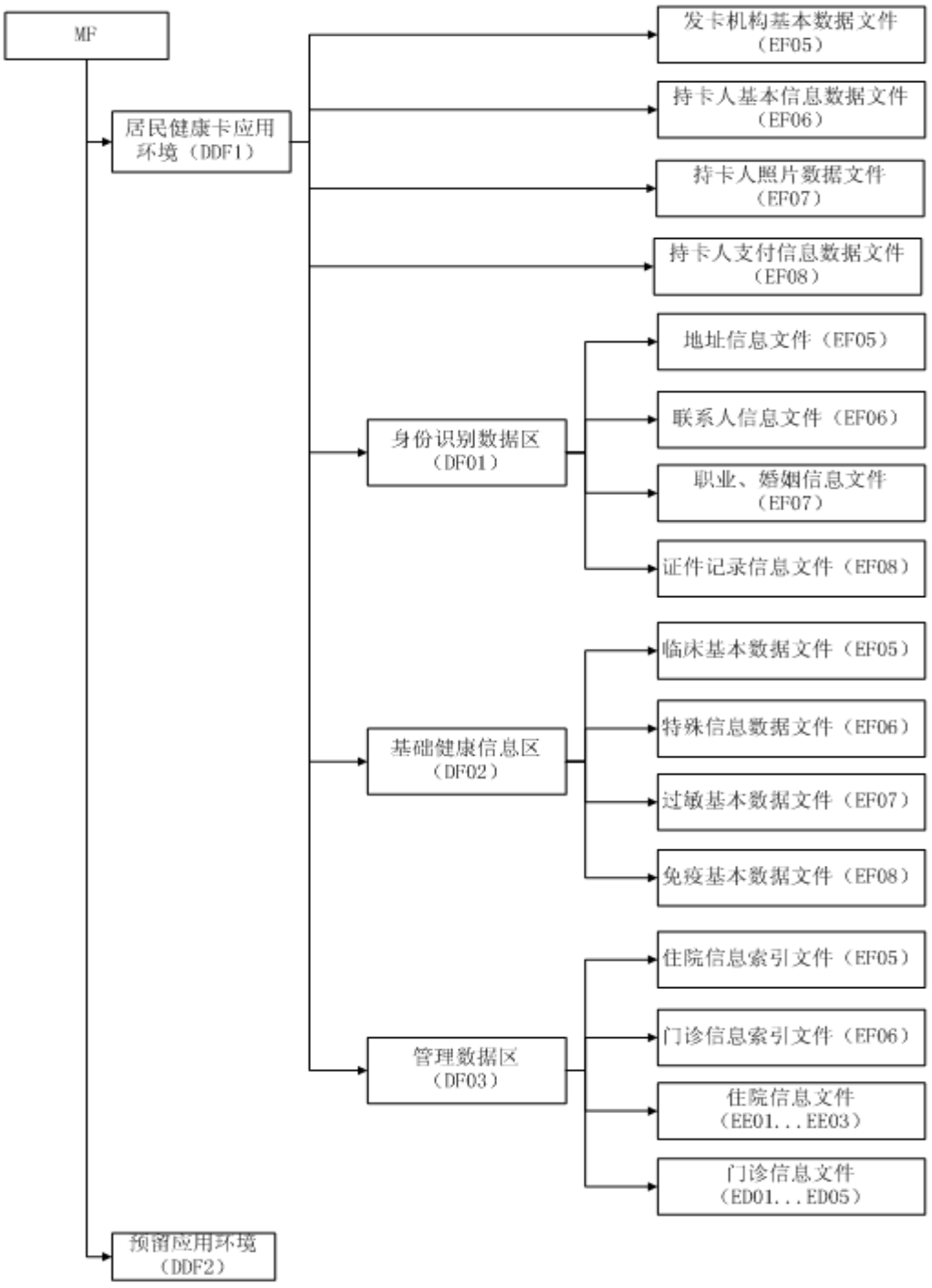

图 4-1 居民健康卡文件结构示意图

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。

发卡机构基本数据文件见表4-1。

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

发卡机构基本数据文件见表4-2。

表 4-2 发卡机构基本数据文件

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

持卡人照片数据文件见表4-3。

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。

持卡人支付信息数据文件见表4-4。

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

地址信息文件见表4-5。

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

联系人信息文件见表4-6。

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

职业、婚姻信息文件见表4-7。

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

证件记录信息文件见表4-8。

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

临床基本数据文件见表4-9。

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

特殊信息数据文件见表4-10。

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

过敏基本数据文件见表4-11。

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

免疫基本数据文件见表4-12。

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

住院信息索引文件见表4-13。

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

门诊信息索引文件见表4-14。

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

住院信息文件见表4-15。

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	ans	20

	述2		
	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

门诊信息文件见表4-16。

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)

本部分中，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

总体应用流程图如图5-1所示。

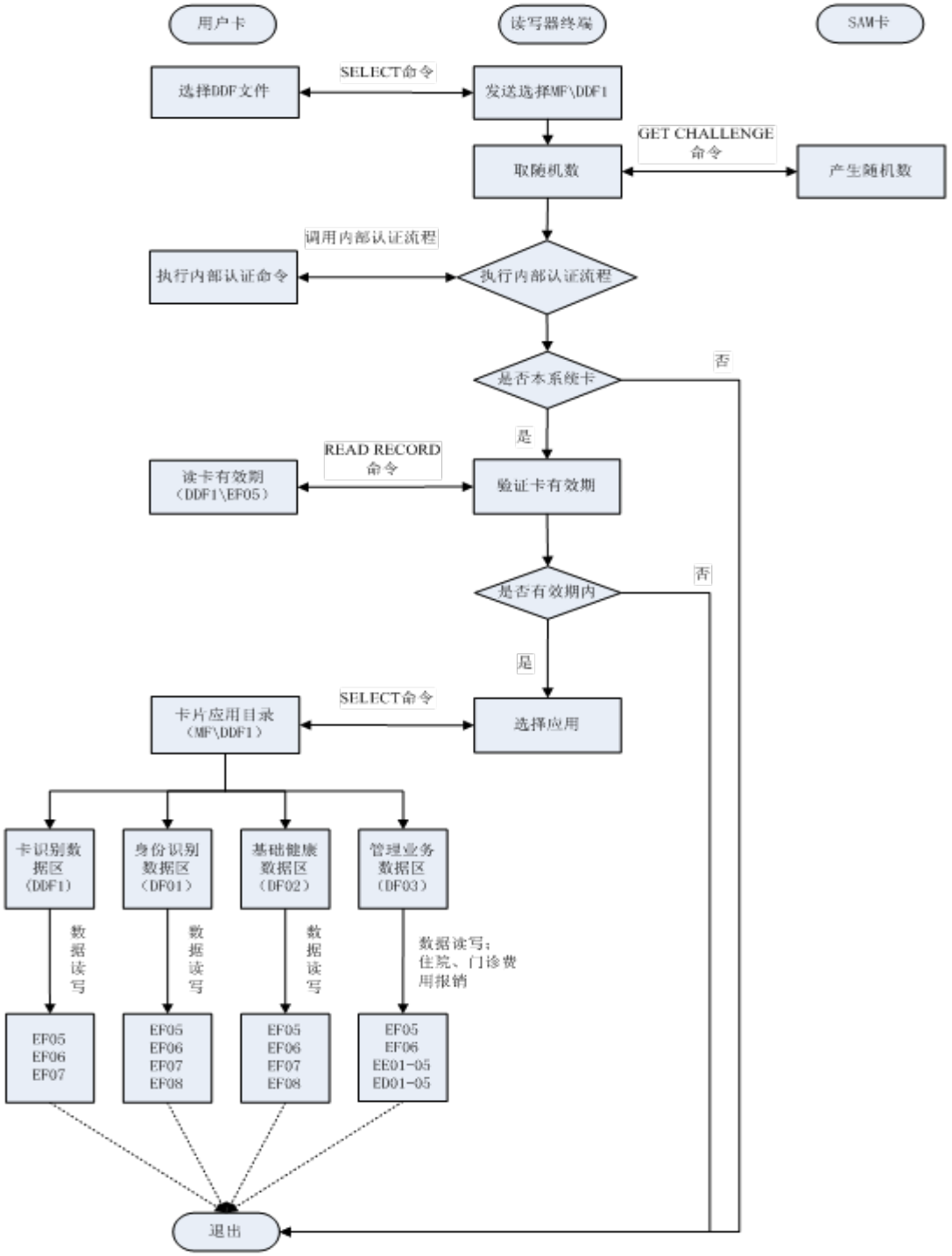

图5-1 总体应用流程图

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 AUTHENTICTION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

内部认证流程图如图5-2所示。

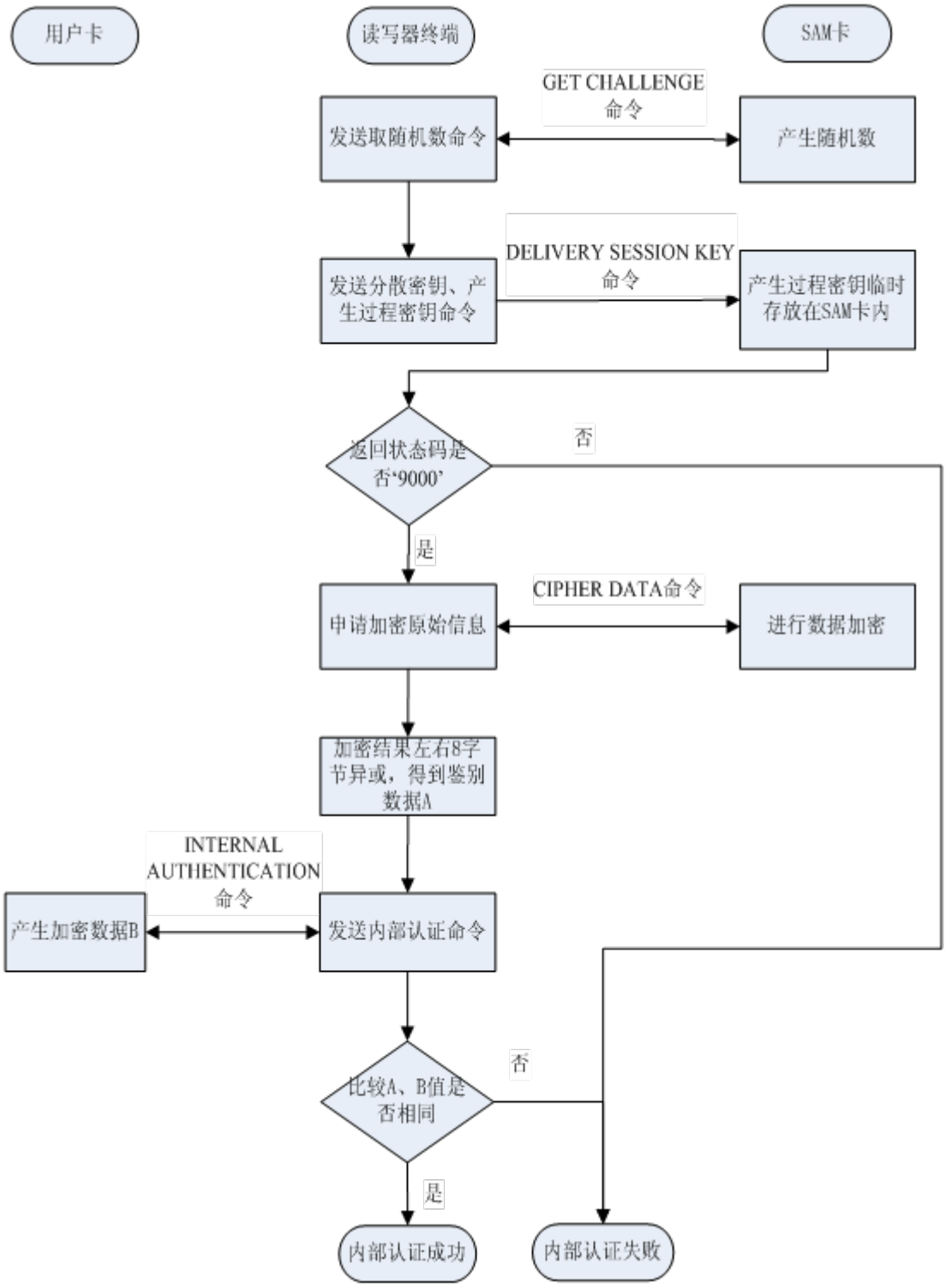

图 5-2 内部认证流程图

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

外部认证流程图如图5-3所示。

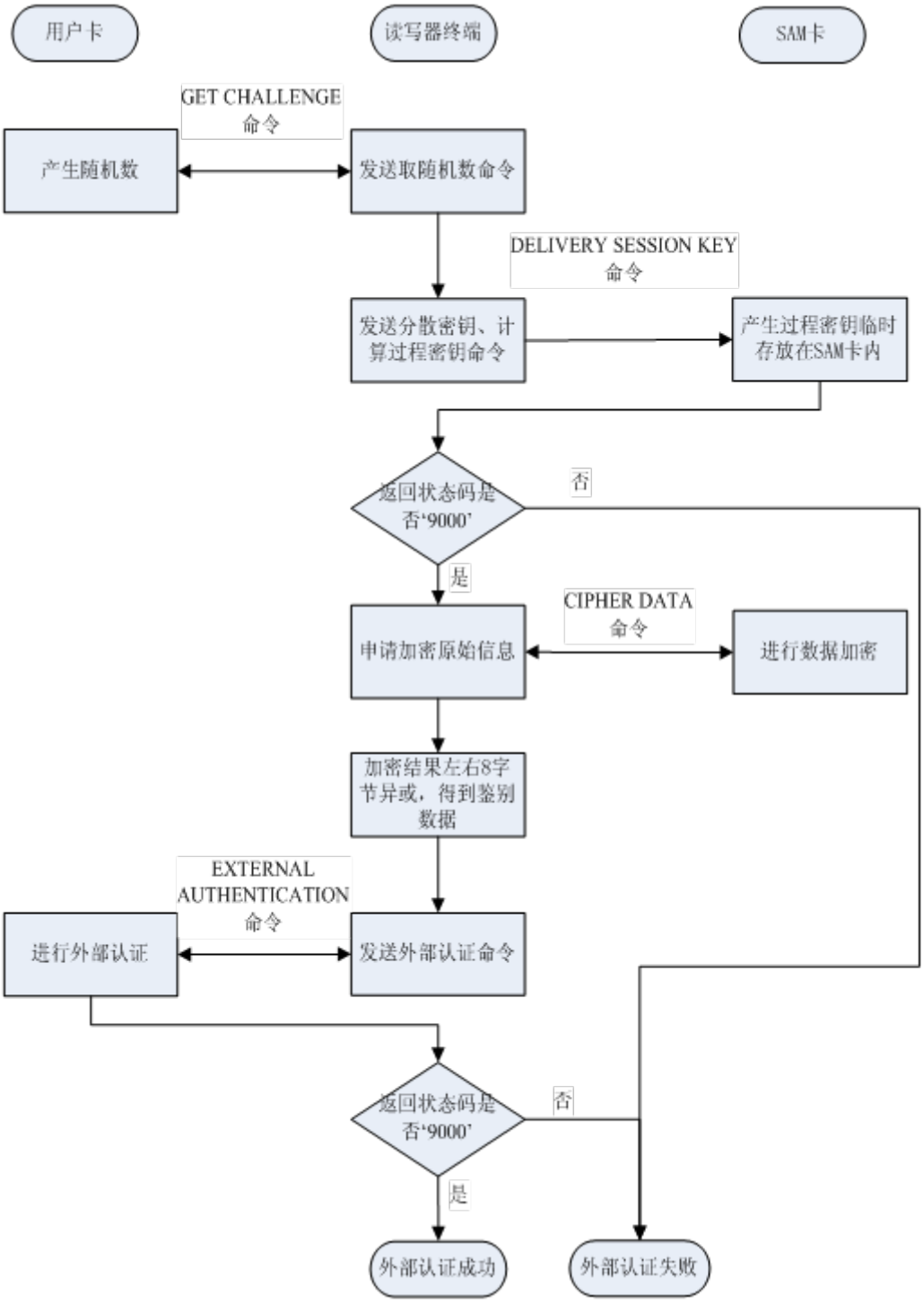

图 5-3 外部认证流程图

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WS XXXXX.1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WS XXXXX.1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 WS XXXXX.3 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WS XXXXX.1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WS XXXXX.1，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

读卡识别数据流程图如图6-1所示。

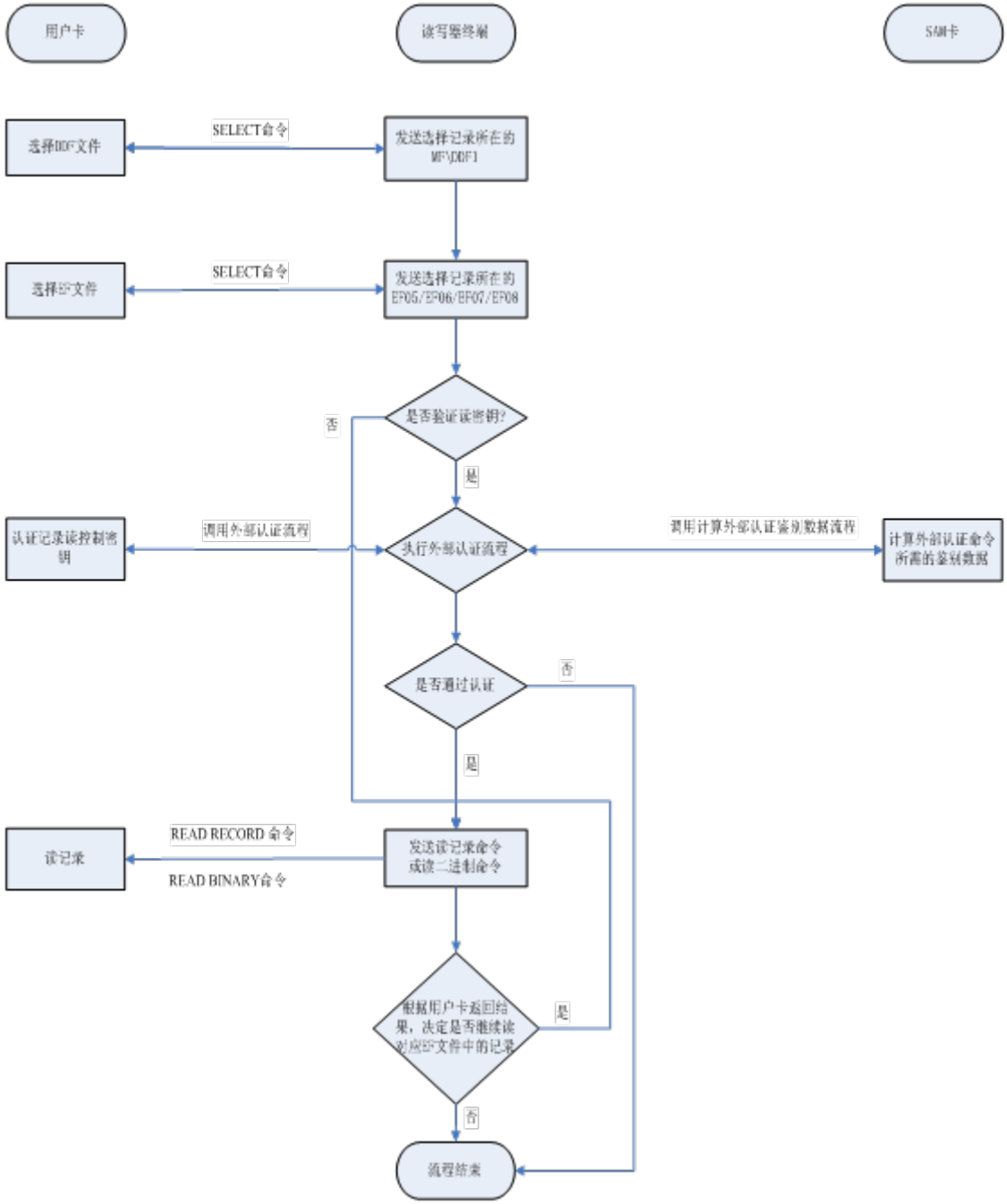

图 6-1 读卡识别数据流程图

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WS XXXXX.3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WS XXXXX.1中定义的对应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WS XXXXX.1，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_{DDF1}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WS XXXXX.1 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

写卡识别数据处理流程图如图6-2所示。

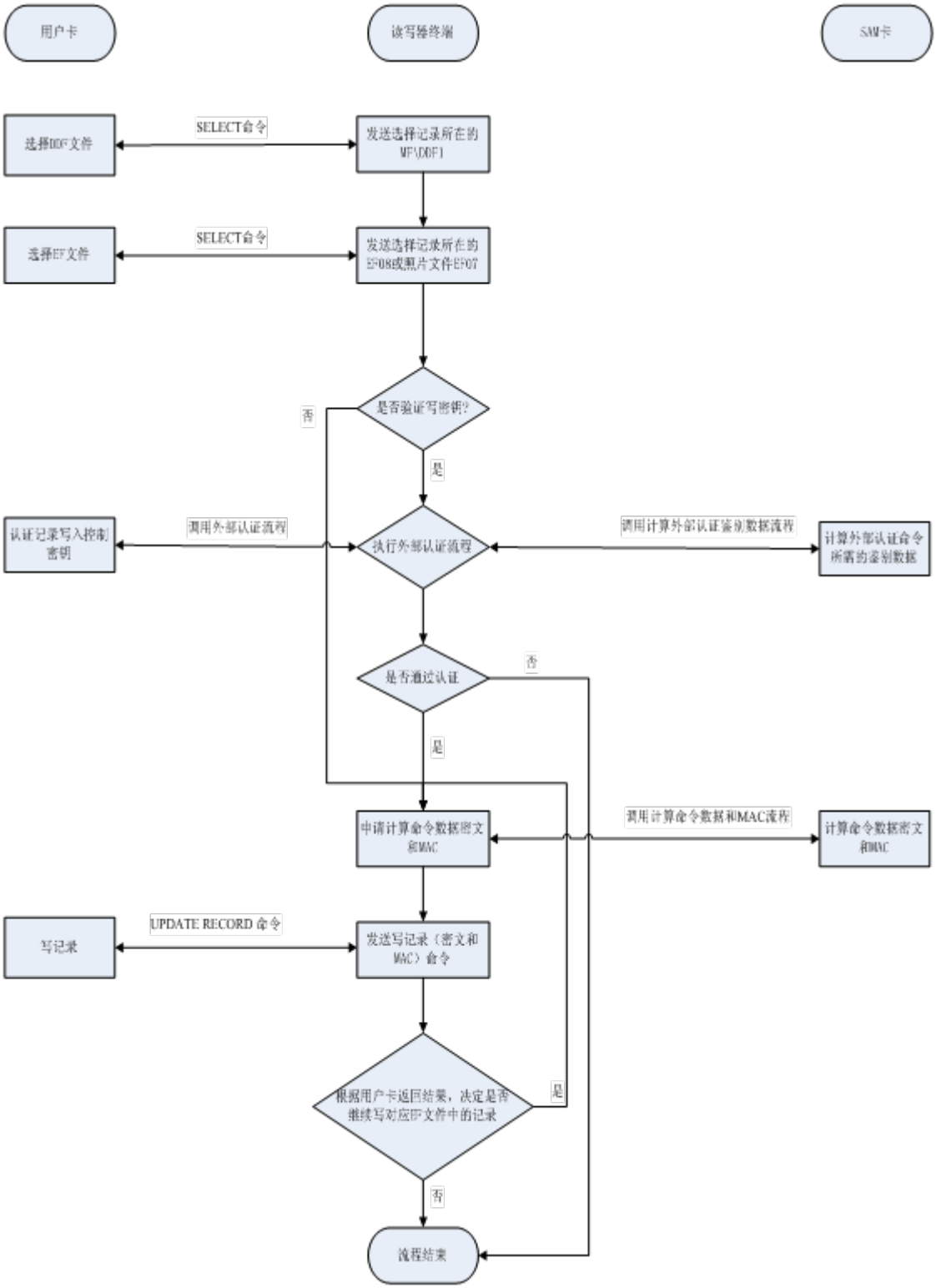

图 6-2 写卡识别数据处理流程图

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WS XXXXX.3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WS XXXXX.1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WS XXXXX.1，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

读DF01应用数据处理流程图如图6-3所示。

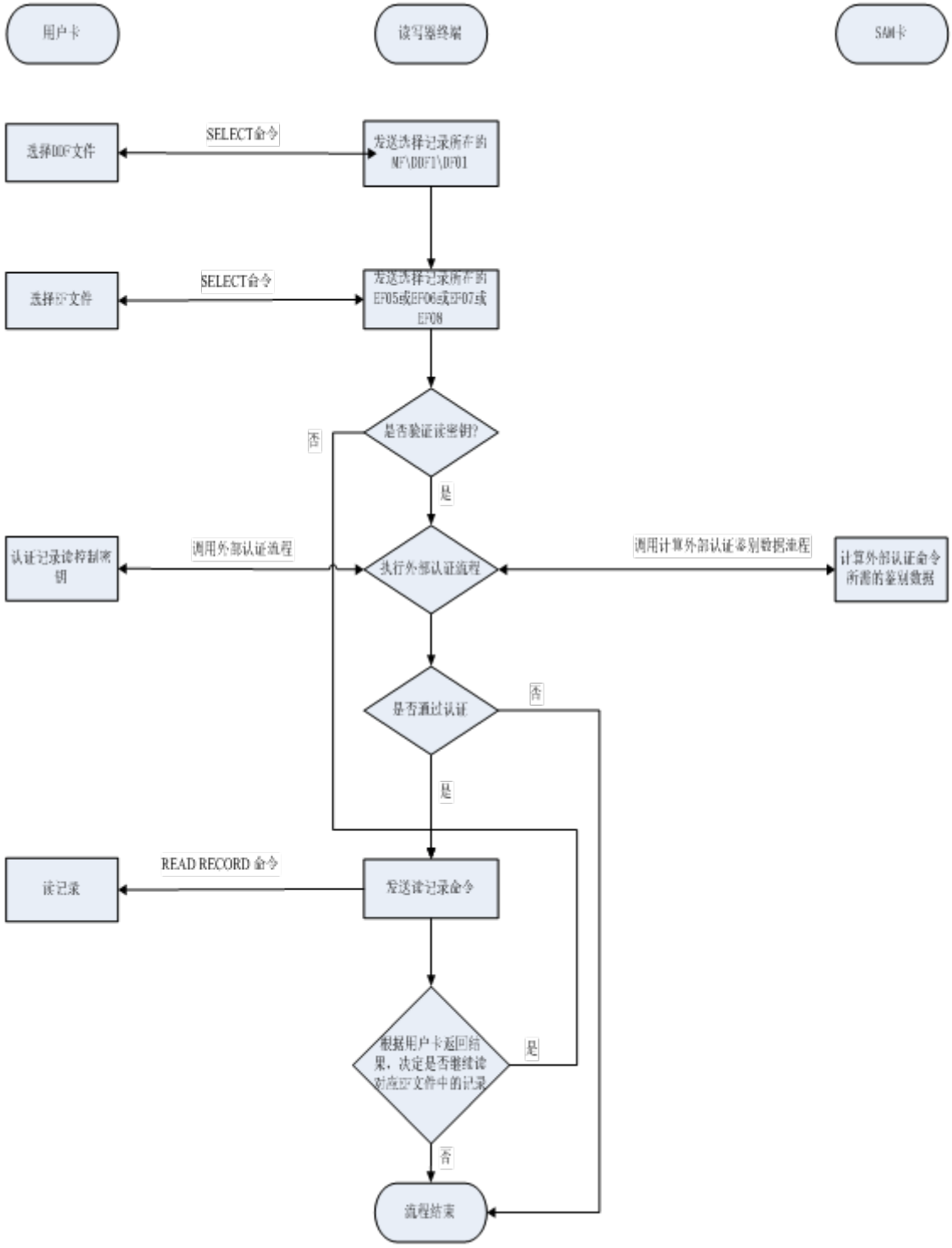

图 6-3 读 DF01 应用数据处理流程图

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WS XXXXX.3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WS XXXXX.1中定义的对应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WS XXXXX.1，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WS XXXXX.1 中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

写DF01应用数据处理流程图如图6-4所示。

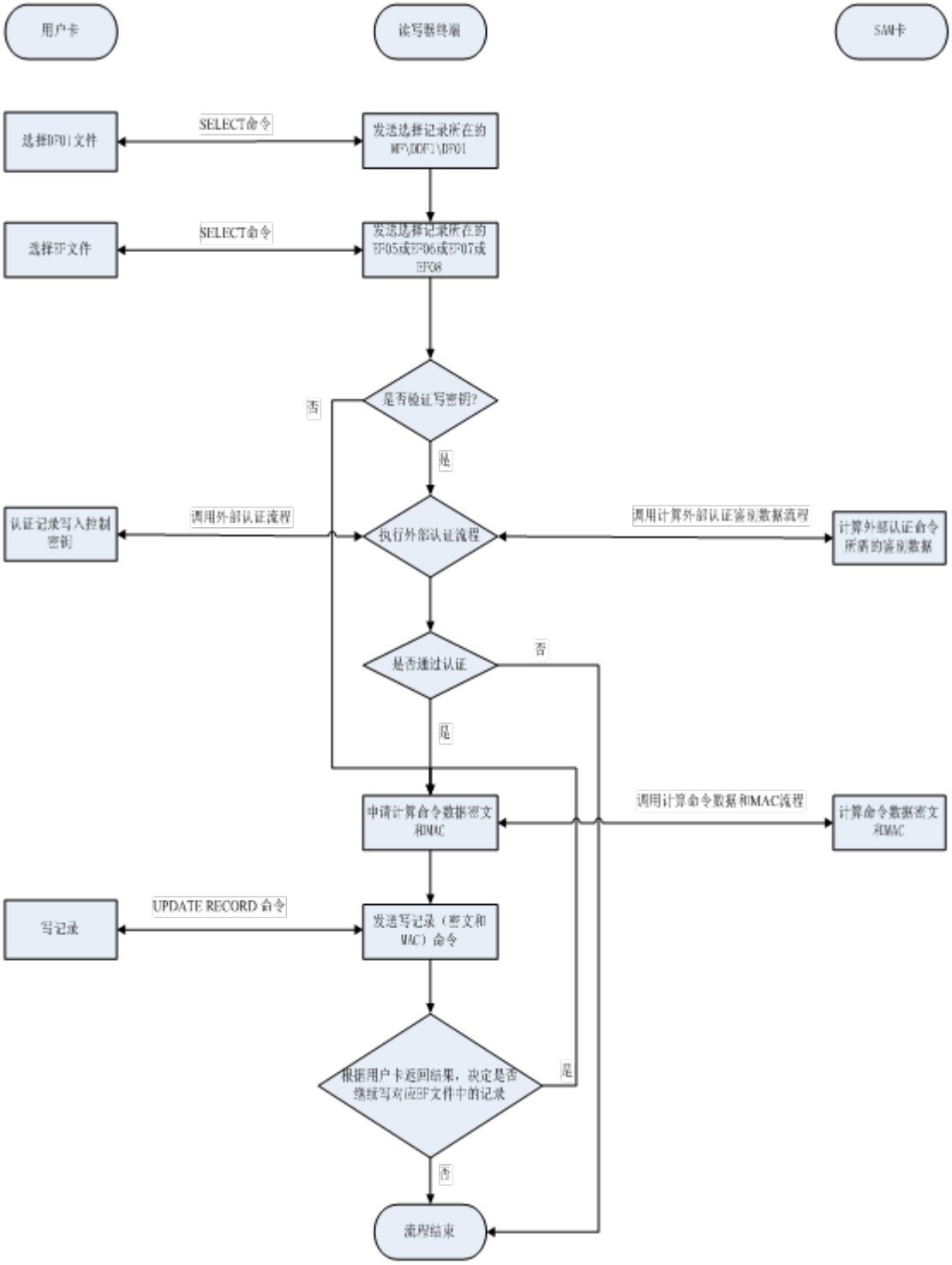

图 6-4 写 DF01 应用数据处理流程图

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WS XXXXX.3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 WS XXXXX.1 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 WS XXXXX.1，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

读DF02应用数据处理流程图如图6-5所示。

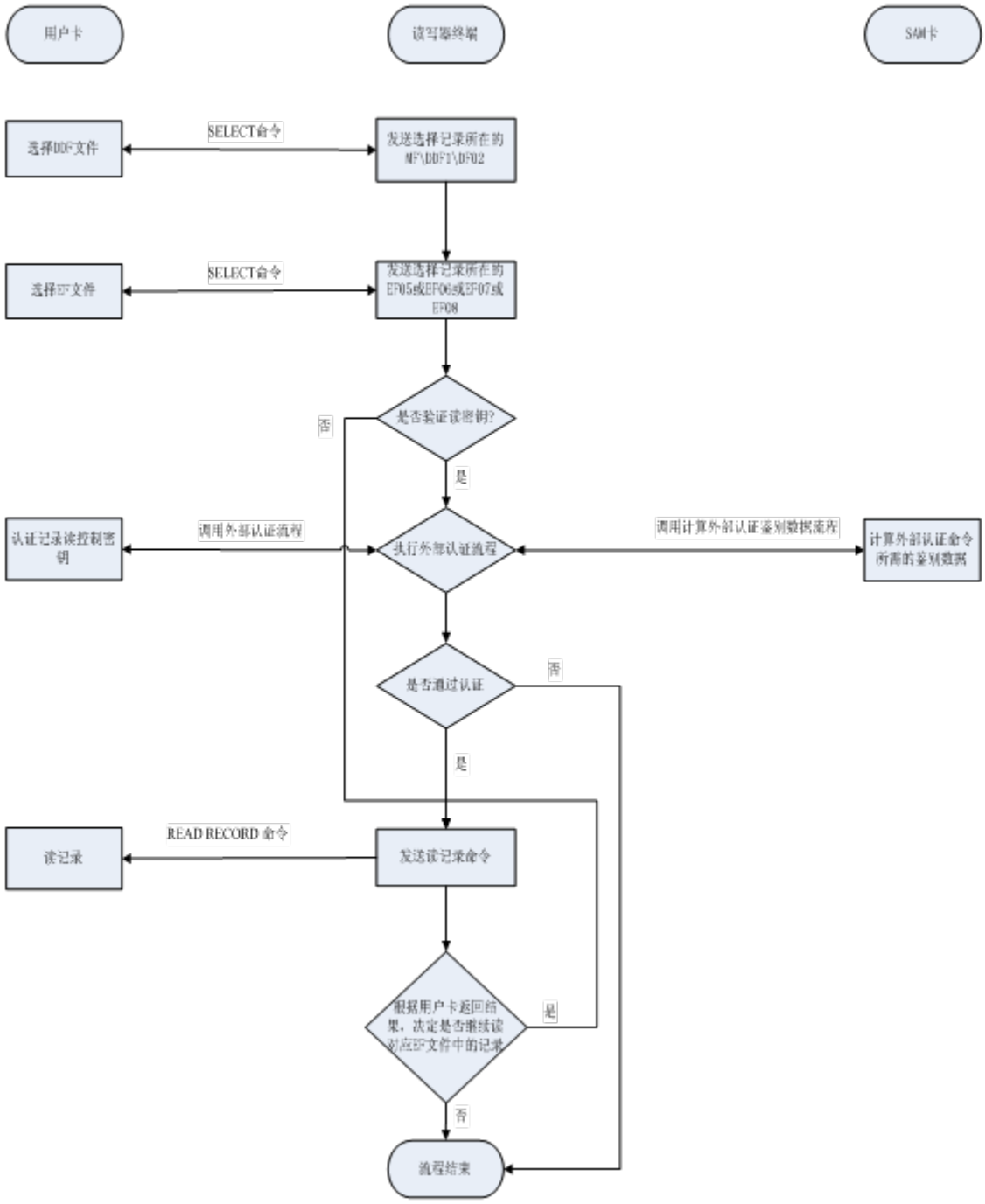

图 6-5 读 DF02 应用数据处理流程图

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WS XXXXX.3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WS XXXXX.1中定义的对应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WS XXXXX.1，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WS XXXXX.1中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

写DF02应用数据处理流程图如图6-6所示。

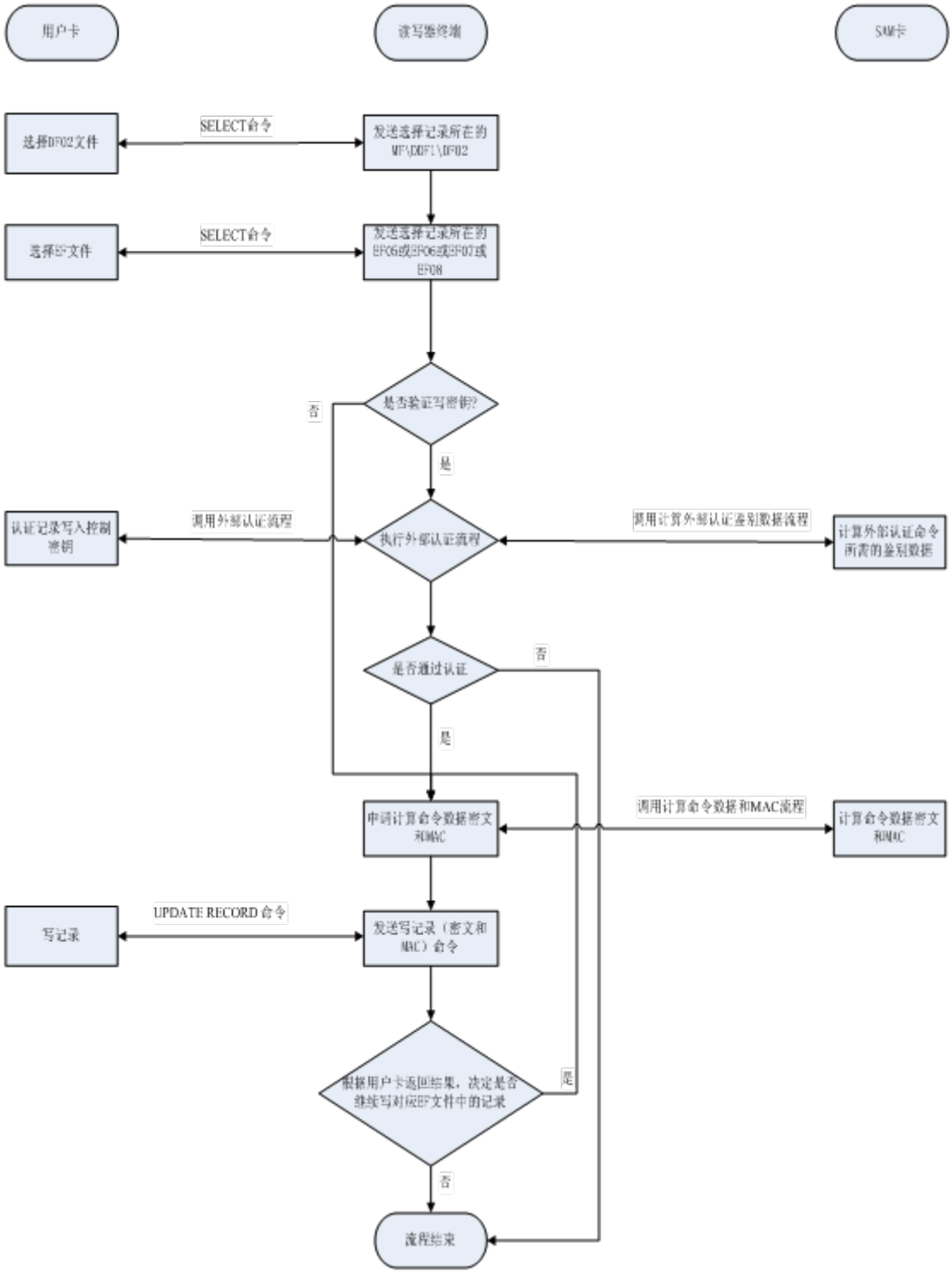

图 6-6 写 DF02 应用数据处理流程图

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 WS XXXXX.1 中 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WS XXXXX.3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，写入住院索引信息文件第RN条记录。

(10) 流程结束。

6.4.1.4 流程图

住院信息记录流程图如图6-7所示。

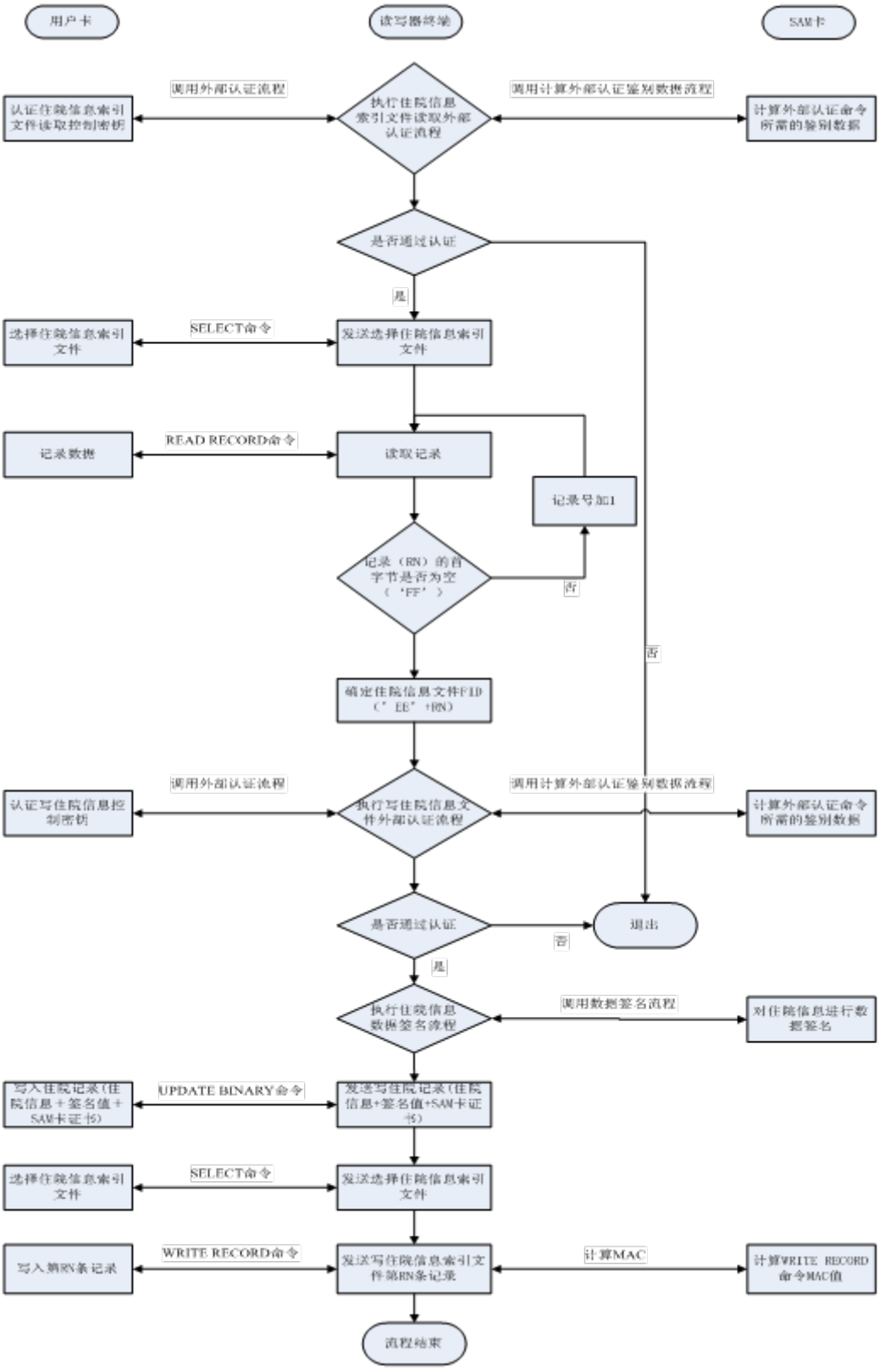

图 6-7 住院信息记录流程图

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WS XXXXX.3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

门诊信息记录流程图如图6-8所示。

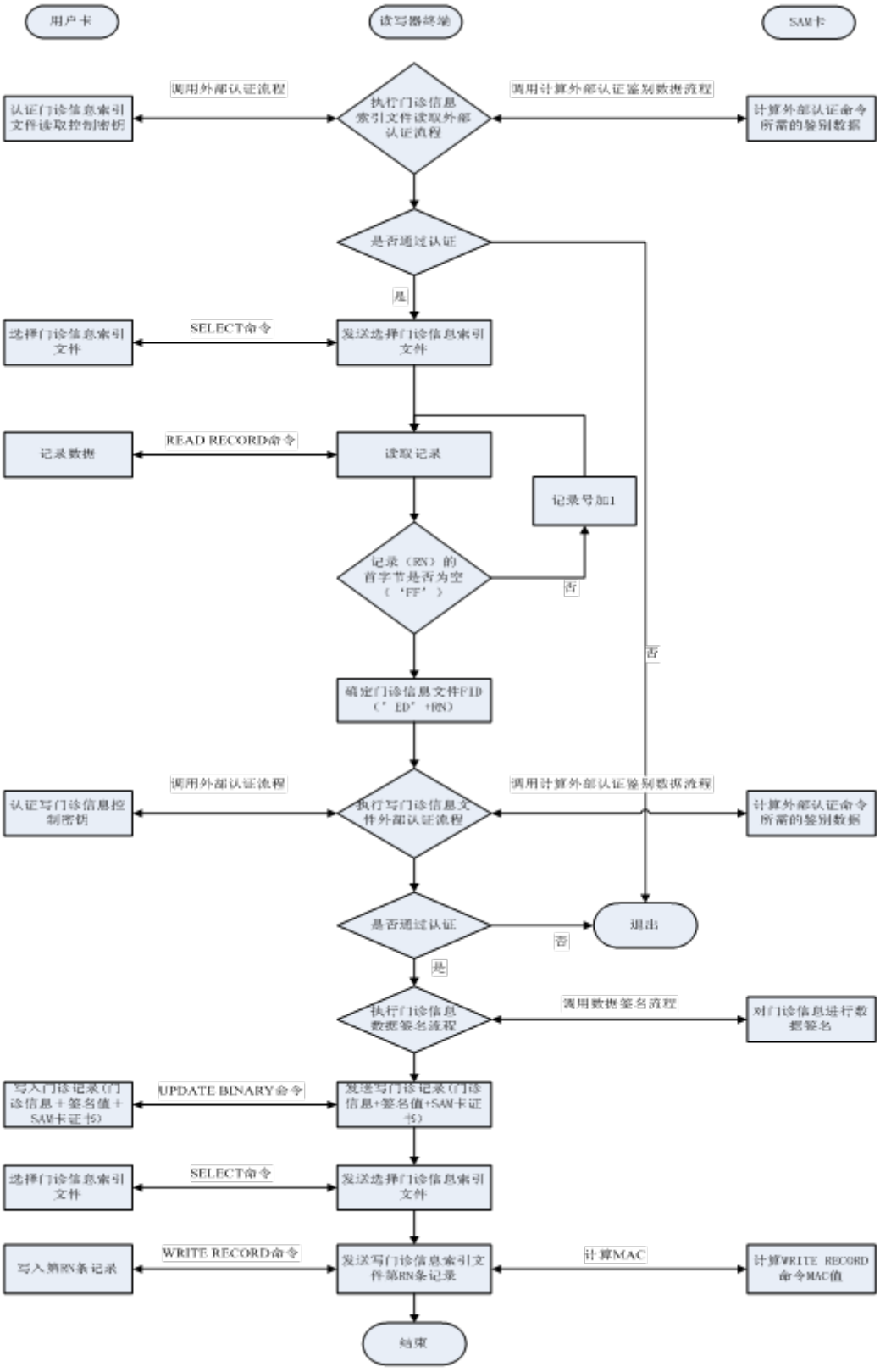

图 6-8 门诊信息记录流程图

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WS XXXXX.3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

住院费用提取及报销流程图如图6-9所示。

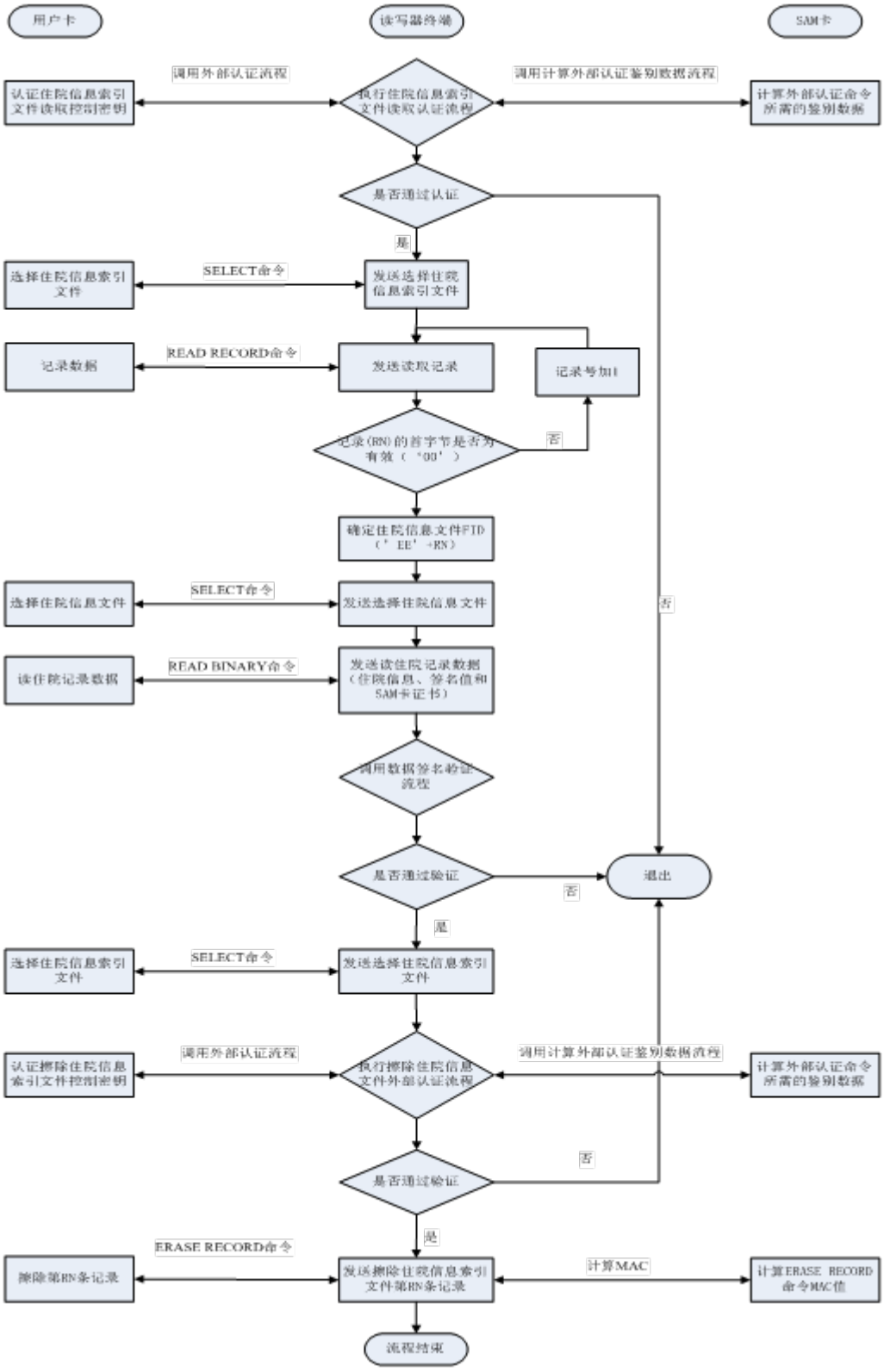

图 6-9 住院费用提取及报销流程图

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WS XXXXX.3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

门诊费用提取及报销流程图如图6-10所示。

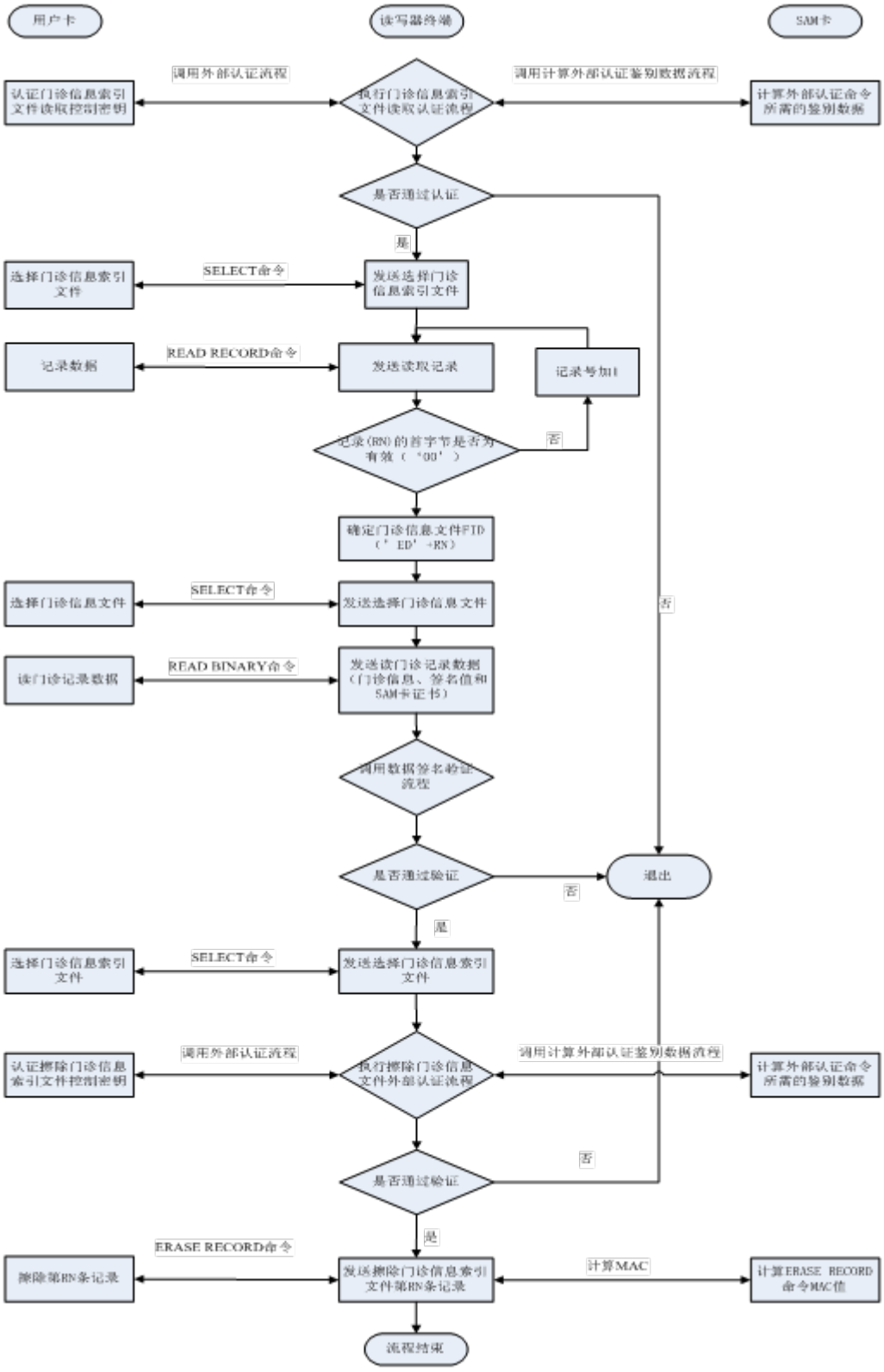

图 6-10 门诊费用提取及报销流程图

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 WS XXXXX.3 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

数据签名流程图如图7-1所示。

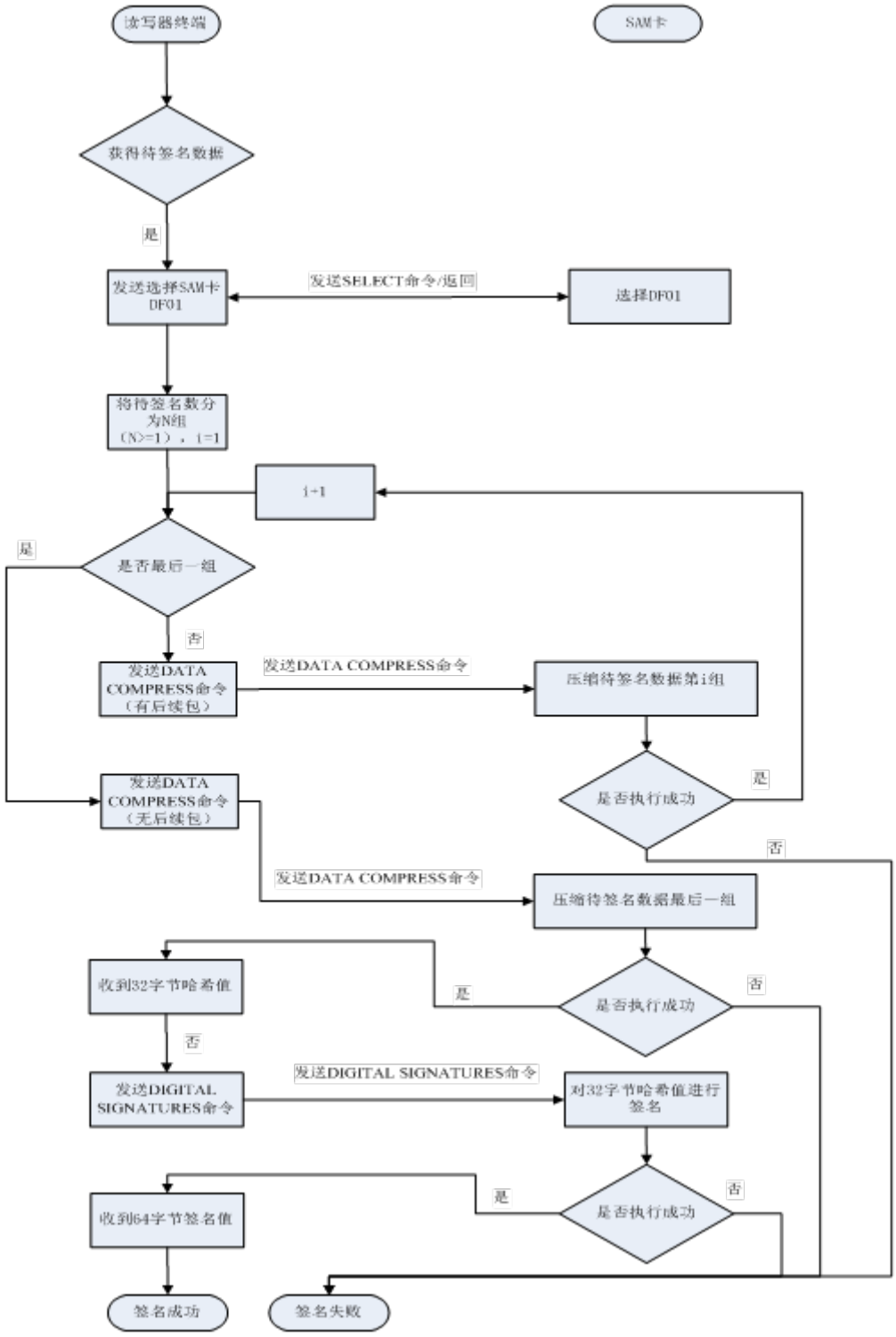

图 7-1 数据签名流程图

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WS XXXXX.3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WS XXXXX.1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

数据签名验证流程图如图7-2所示。

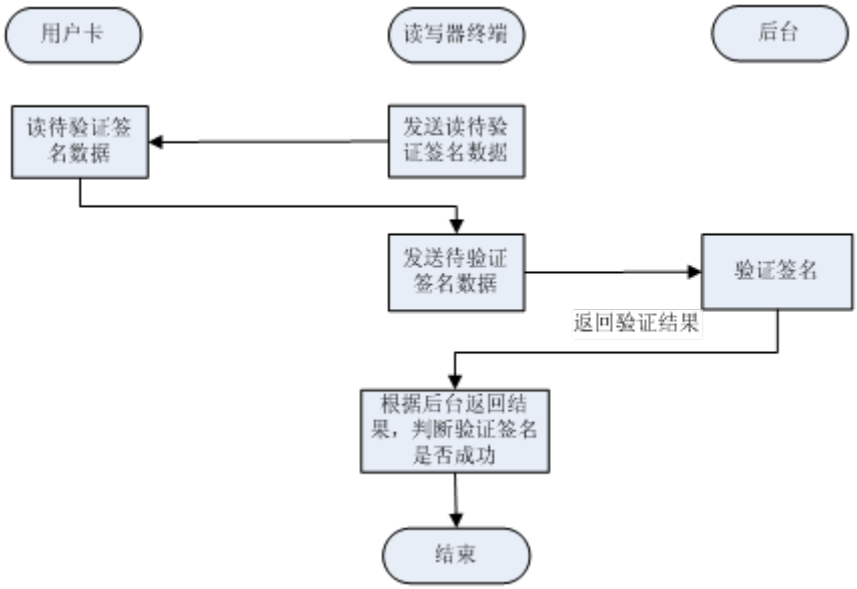

图 7-2 数据签名验证流程图