ICS 11.020
C 07

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS/T 543.3—2017

居民健康卡技术规范
第3部分：用户卡应用规范

Residents' health card technical specifications——
Part 3：Application specification of the user card

2017－07－25 发布　　2017－12－01 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

本标准按照GB/T 1.1 —2009给出的规则起草。

WS/T 543《居民健康卡技术规范》分为6个部分：

——第1部分：总则；

——第2部分：用户卡技术规范；

——第3部分：用户卡应用规范；

——第4部分：用户卡命令集；

——第5部分：终端技术规范；

——第6部分：用户卡及终端产品检测规范；

本部分为WS/T 543的第3部分。

本部分起草单位：国家卫生计生委统计信息中心、江苏省卫生和计划生育委员会信息中心、湖南省卫生和计划生育委员会信息中心、石家庄市卫生和计划生育委员会、北京市公共卫生信息中心、北京协和医院。

本部分主要起草人：孟群、胡建平、郝惠英、周红、刘晓强、唐凯、雷永贵、张俊、白和健、张文中、朱卫国、任杰、左云。

居民健康卡技术规范　第3部分：用户卡应用规范

1　适用范围

WS/T 543的本部分规定了居民健康卡的文件、数据项以及数据对象列表，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，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　识别卡带触点的集成电路卡 第4部分：用于交换的结构、安全和命令

WS/T 543.1　居民健康卡技术规范 第1部分：总则

WS/T 543.2　居民健康卡技术规范 第2部分：　用户卡技术规范

3　术语和缩略语

3.1　术语和定义

WS/T 543.1、WS/T543.2界定的以及下列术语和定义适用于本文件。

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。

3.2　缩略语

WS/T 543.2界定的以及下列缩略语和符号适用于本文件。

BER 基本编码规则（Basic Encoding Rules）

TLV 标签、长度、值（Tag Length Value）

4 文件、数据项、数据对象列表

4.1 文件结构

本标准中的文件组织结构遵循GB/T 16649.4相关要求，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1所示、居民健康卡文件内容见表1。

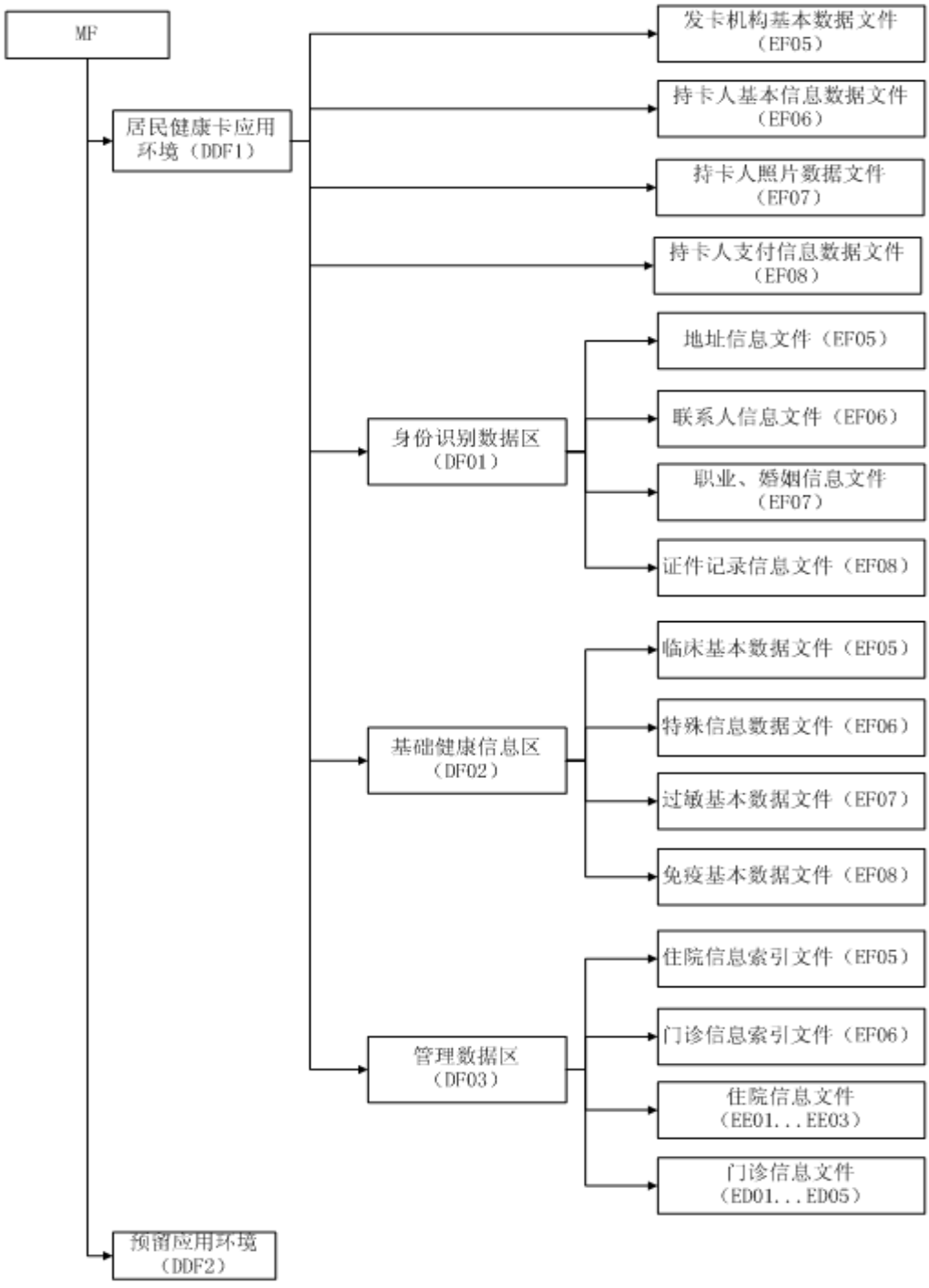

图1　居民健康卡文件结构示意图

表1　文件内容

文件内容	FID 值	备注
发卡机构基本数据文件	‘EF05’	变长记录文件
持卡人基本信息数据文件	‘EF06’	变长记录文件

表 1（续）

文件内容	FID 值	备注
持卡人照片数据文件	‘EF07’	二进制文件
持卡人支付信息数据文件	‘EF08’	变长记录文件
身份识别数据区 ADF	‘DF01’	AID = ‘915600013200’
地址信息文件	‘EF05’	变长记录文件
联系人信息文件	‘EF06’	变长记录文件
职业、婚姻信息文件	‘EF07’	变长记录文件
证件记录信息文件	‘EF08’	变长记录文件
基础健康数据区 ADF	‘DF02’	AID = ‘915600013201’
临床基本数据文件	‘EF05’	变长记录文件
特殊信息数据文件	‘EF06’	变长记录文件
过敏基本数据文件	‘EF07’	循环记录文件
免疫基本数据文件	‘EF08’	循环记录文件
管理数据区 ADF	‘DF03’	AID = ‘915600013202’
住院信息索引文件	‘EF05’	定长记录文件
门诊信息索引文件	‘EF06’	定长记录文件
住院信息文件	‘EE01’－ ‘EE03’	二进制文件
门诊信息文件	‘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。 注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2。

表2　发卡机构基本数据文件

标志	数据项	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	发卡机构公钥证书	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
注1：文件标识（FID）=‘EF05’。 注2：文件类型，变长记录。 注3：文件存取控制，读=自由，禁止改写。			

持卡人基本信息数据文件见表3。

表3　持卡人基本信息数据文件

标志	数据项	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
注1：文件标识（FID）=‘EF06’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DDF1}$，禁止改写。			

持卡人照片数据文件见表4。

表4　持卡人照片数据文件

标志	数据项	类型	长度
	照片	B	3074
注1：文件标识（FID）=‘EF07’。 注2：文件类型，二进制文件。 注3：文件存取控制，读=$RK1_{DDF1}$，改写=$UK1_{DDF1}$。 注4：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5。

表5　持卡人支付信息数据文件

标志	数据项	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
注1：文件标识（FID）=‘EF08’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DDF1}$，改写=$UK1_{DDF1}$。			

地址信息文件见表6。

表6　地址信息文件

标志	数据项	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
注1：文件标识（FID）=’EF05’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF01}$，改写=$UK1_{DF01}$。			

联系人信息文件见表7。

表7　联系人信息文件

标志	数据项	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
注1：文件标识（FID）=’EF06’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF01}$，改写=$UK1_{DF01}$。			

职业、婚姻信息文件见表8。

表8　职业、婚姻信息文件

标志	数据项	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
注1：文件标识（FID）=’EF07’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF01}$，改写=$UK1_{DF01}$。			

证件记录信息文件见表9。

表9　证件记录信息文件

标志	数据项	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
注1：文件标识（FID）=’EF08’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF01}$，改写=$UK1_{DF01}$。			

临床基本数据文件见表10。

表10　临床基本数据文件

标志	数据项	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
注1：文件标识（FID）=’EF05’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF02}$，改写=$UK1_{DF02}$。			

特殊信息数据文件见表11。

表11　特殊信息数据文件

标志	数据项	类型	长度
56	精神病标志	B	01
注1：文件标识（FID）=’EF06’。 注2：文件类型，变长记录。 注3：文件存取控制，读=$RK1_{DF02}$，改写=$UK2_{DF02}$。			

过敏基本数据文件见表12。

表12　过敏基本数据文件

标志	数据项	类型	长度
	过敏物质名称	ans	20
	过敏反应	ans	100
注1：文件标识（FID）=’EF07’。 注2：文件类型，循环记录（3 条）。 注3：文件存取控制，读=$RK1_{DF02}$，改写=$UK3_{DF02}$。			

免疫基本数据文件见表13。

表13　免疫基本数据文件

标志	数据项	类型	长度
	免疫接种名称	ans	20
	免疫接种时间	Cn	04
注1：文件标识（FID）=’EF05’。 注2：文件类型，循环记录（10 条）。 注3：文件存取控制，读=$RK1_{DF02}$，改写=$UK3_{DF02}$。			

住院信息索引文件见表14。

表14　住院信息索引文件

标志	数据项	类型	长度
	住院记录有效标志	B	01
注1：文件标识（FID）=’EF05’。 注2：文件类型，定长记录（3 条）。 注3：文件存取控制，读=$RK1_{DF03}$，改写=$UK1_{DF03}$，擦除=$UK2_{DF03}$。			

门诊信息索引文件见表15。

表15　门诊信息索引文件

标志	数据项	类型	长度
	门诊记录有效标志	B	01
注1：文件标识（FID）=’EF06’。 注2：文件类型，定长记录（5 条）。 注3：文件存取控制，读=$RK1_{DF03}$，改写=$UK1_{DF03}$，擦除=$UK2_{DF03}$。			

住院信息文件见表16。

表16　住院信息文件

标志	数据项	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

表 16（续）

标志	数据项	类型	长度
	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

表 16（续）

标志	数据项	类型	长度
	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

表 16（续）

标志	数据项	类型	长度
	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

表 16（续）

标志	数据项	类型	长度
	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
注1：文件标识（FID）=’EF01’-’EF03’。 注2：文件类型，二进制。 注3：文件存取控制，读=$RK1_{DF03}$，改写=$UK1_{DF03}$。			

门诊信息文件见表17。

表17　门诊信息文件

标志	数据项	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

表 17（续）

标志	数据项	类型	长度
	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

表 17（续）

标志	数据项	类型	长度
	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

表 17（续）

标志	数据项	类型	长度
	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

表 17（续）

标志	数据项	类型	长度
	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

表 17（续）

标志	数据项	类型	长度
	交易信息签名	B	64
	SAM卡证书	B	190
注1：文件标识（FID）=’EF01’-’EF05’。 注2：文件类型，二进制。 注3：文件存取控制，读=$RK1_{DF03}$，改写=$UK1_{DF03}$。			

4.2 应用数据文件(ADF)

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。ADF的树形结构要求如下：

a) 能够将数据文件与应用联系起来；
b) 确保应用之间的独立性；
c) 可以通过应用选择实现对其逻辑结构的访问。

4.3 应用基本文件(AEF)

本文件中，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：

a) 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)；
b) 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名字在该卡内是唯一的。

5 卡操作

5.1 总体操作

5.1.1 总体操作流程

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。

a) 用户卡上电复位，卡片位于 MF 下；
b) 发送 SELECT 命令，选择居民健康卡应用环境 DDF1；
c) 执行内部认证流程，对卡进行内部认证；
d) 发送 SELECT 命令，选择 EF05；
e) 发送 READ RECORD 命令，读卡有效期；
f) 发送 SELECT 命令到各应用文件；

g） 根据各应用文件读写控制权限，选择是否进行外部认证；

h） 对相应文件进行读写操作；

i） 流程结束。

5.1.2 流程图

总体应用流程图如图2所示。

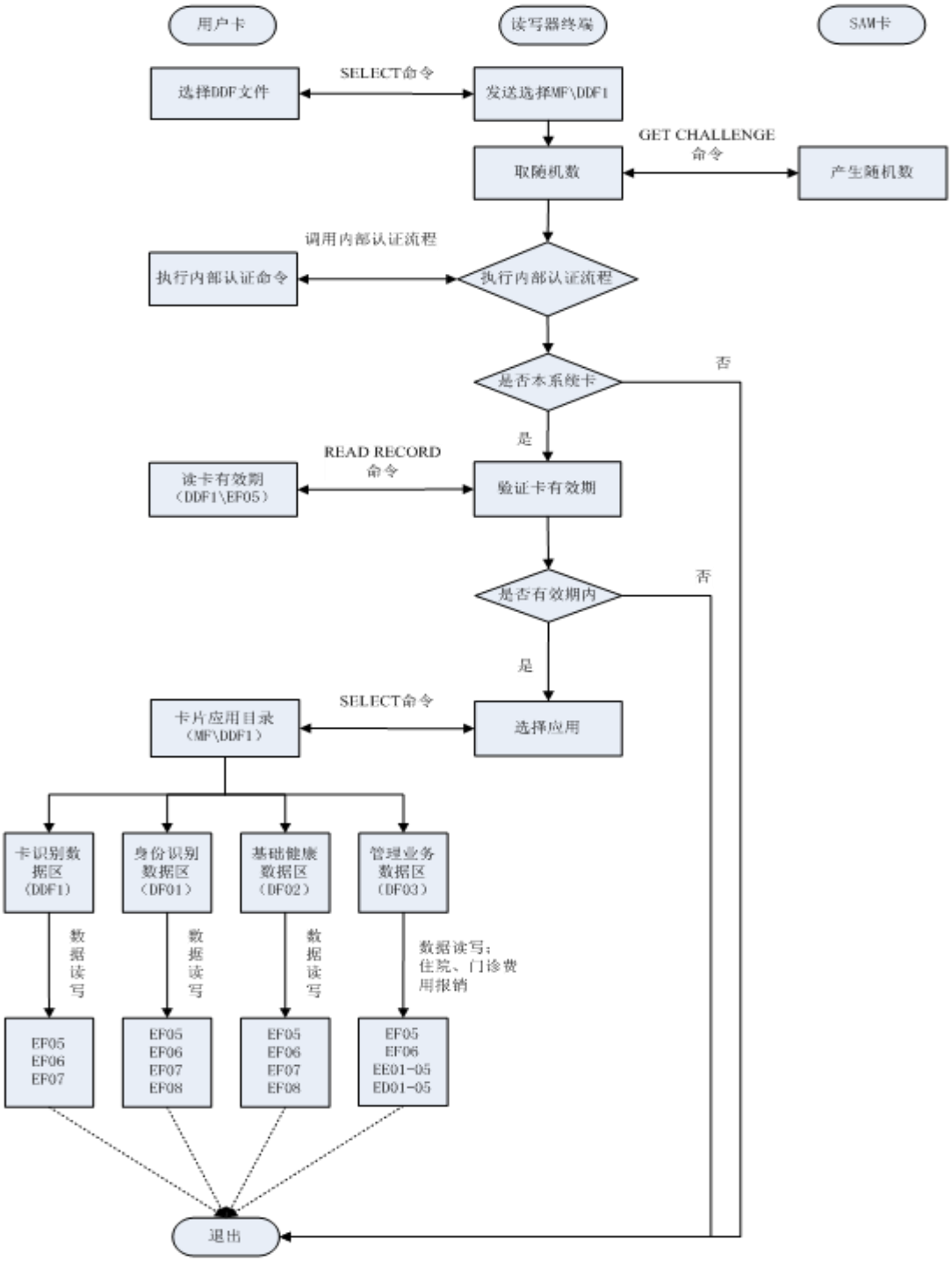

图2 总体应用流程图

5.2 内部认证

5.2.1 内部认证流程

内部认证流程如下：

a) 终端从 SAM 卡获取 8 字节随机数；
b) 定义 8 字节长度的鉴别所需的原始信息，如 1122334455667788；
c) 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；
d) 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；
e) 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；
f) 终端向 SAM 卡发送 CIPHER DATA 命令，加密原始信息；
g) 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；
h) 终端向用户卡发送 INTERNAL AUTHENTICTION 命令，得到返回值 B；
i) 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；
j) 流程结束。

5.2.2 流程图

内部认证流程图如图3所示。

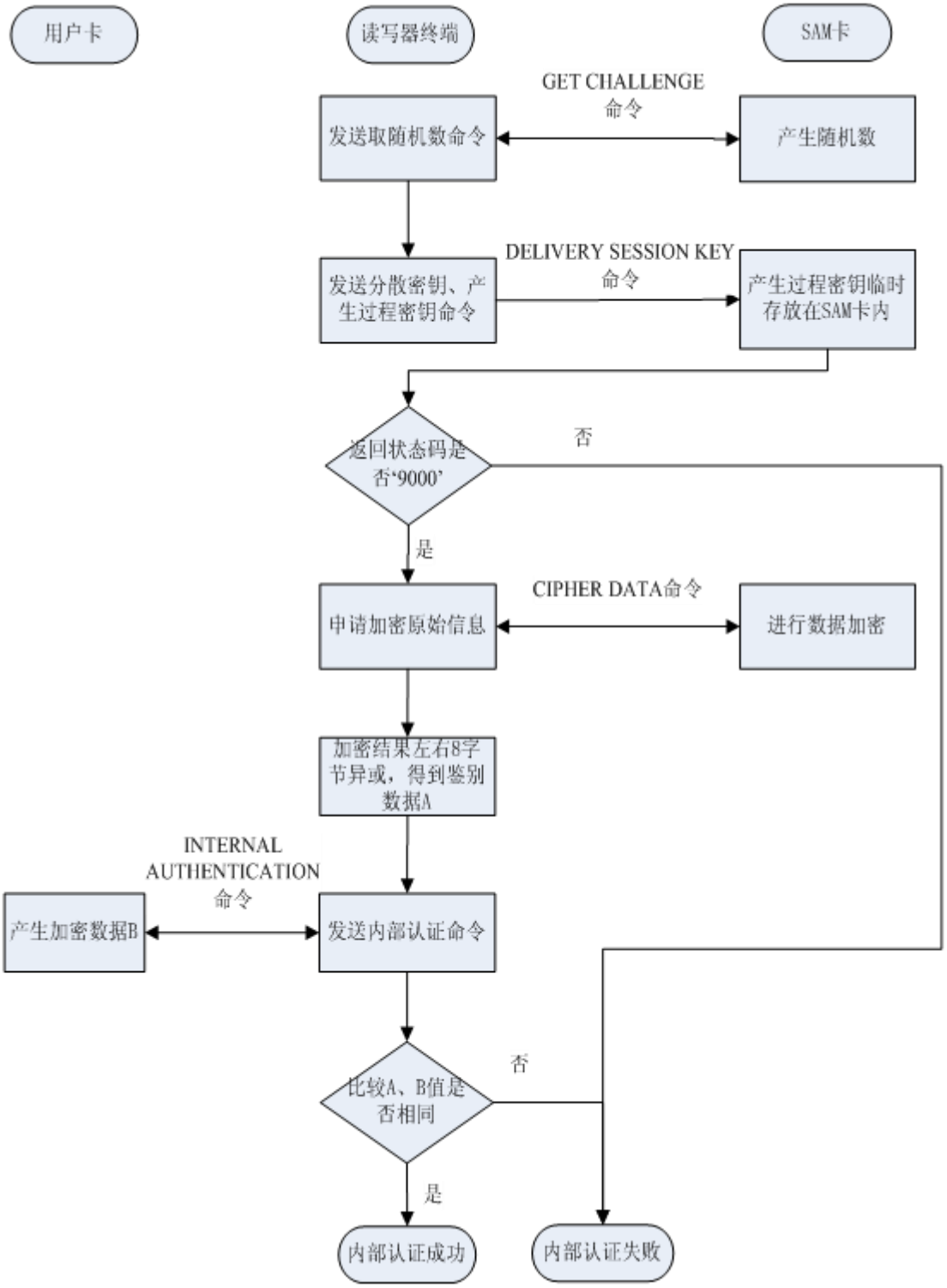

图3　内部认证流程图

5.3　外部认证

5.3.1　外部认证流程

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。

a) 定义 8 字节长度的鉴别所需的原始信息，如 1122334455667788；
b) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数；
c) 随机数做为 SAM 卡过程密钥产生因子；
d) 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；
e) 终端向 SAM 卡发送 CIPHER DATA 命令，加密原始信息；
f) 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；
g) 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；
h) 终端向用户卡发送 EXTERNAL AUTHENTICATION 命令；
i) 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；
j) 流程结束。

5.3.2 流程图

外部认证流程图如图4所示。

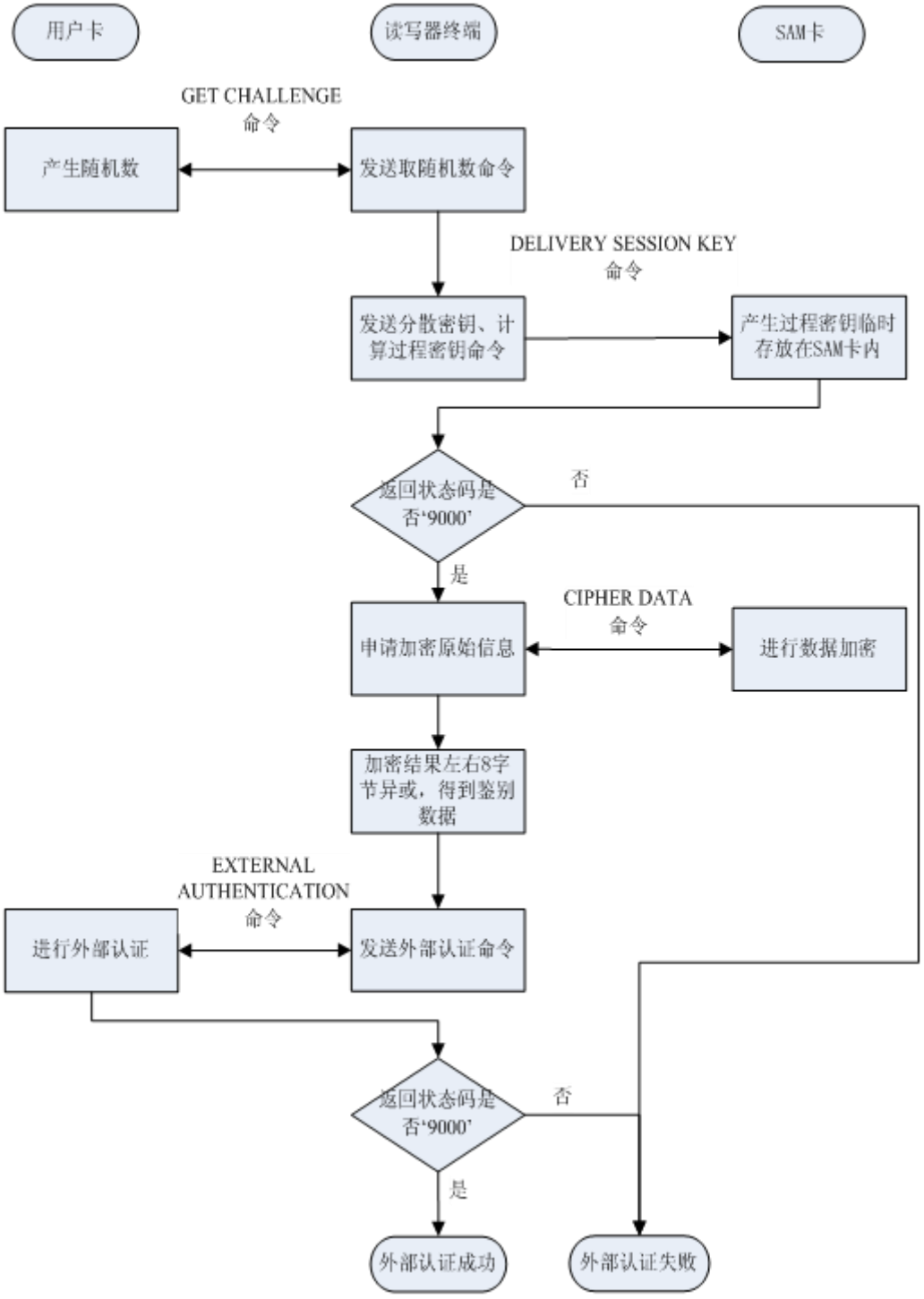

图4　外部认证流程图

5.4　应用锁定

5.4.1　概述

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。

5.4.2 应用锁定流程

应用锁定流程为：

a) 终端向用户卡发送 SELECT 命令，选择待锁定的应用区（DF）；
b) 终端执行外部认证流程，对该 DF 下的 LK 密钥进行外部认证；
c) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数；
d) 随机数做为 SAM 卡过程密钥产生因子；
e) 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；
f) 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；
g) 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

应用解锁流程为：

a) 终端向用户卡发送 SELECT 命令，选择被临时锁定的应用区（DF）；
b) 终端执行外部认证流程，对该 DF 下的 LK 密钥进行外部认证；
c) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数；
d) 随机数做为 SAM 卡过程密钥产生因子；
e) 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；
f) 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；
g) 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

5.6.1 概述

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。

5.6.2 卡锁定流程

卡锁定流程如下：

a) 终端向用户卡发送 SELECT 命令，选择待锁定的卡片根目录（MF）；
b) 终端执行外部认证流程，对 MF 下的 BK 密钥进行外部认证；
c) 终端向用户卡发送 GET CHALLENGE 命令，获得 8 字节随机数；
d) 随机数做为 SAM 卡过程密钥产生因子；
e) 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；
f) 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；
g) 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：

a) 通过外部认证，满足操作的安全状态；
b) 终端向用户卡申请一随机数；
c) 发送相应的应用维护命令，卡在收到命令后执行以下操作：
   1) 使用前一步骤产生的随机数，利用 WS/T 543.2 中描述的方式产生过程密钥（核对一下章节是否正确）；
   2) 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/T 543.2 中描述。

6 卡业务应用

6.1 卡识别应用(对应 MF\DDF1 数据区)

6.1.1 卡识别数据区

卡识别数据区包括EF05、EF06、EF07和EF08文件。

6.1.2 读卡识别数据区信息

6.1.2.1 概述

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

6.1.2.2 处理流程

流程具体如下：
a) 终端根据应用执行的情况决定从用户卡读取哪些记录；
b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS/T 543.1 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/T 543.1，外部认证命令处理过程参见本文档的对应章节）；
d) 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；
e) 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；
f) 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。

6.1.2.3 流程图

读卡识别数据流程图如图5所示。

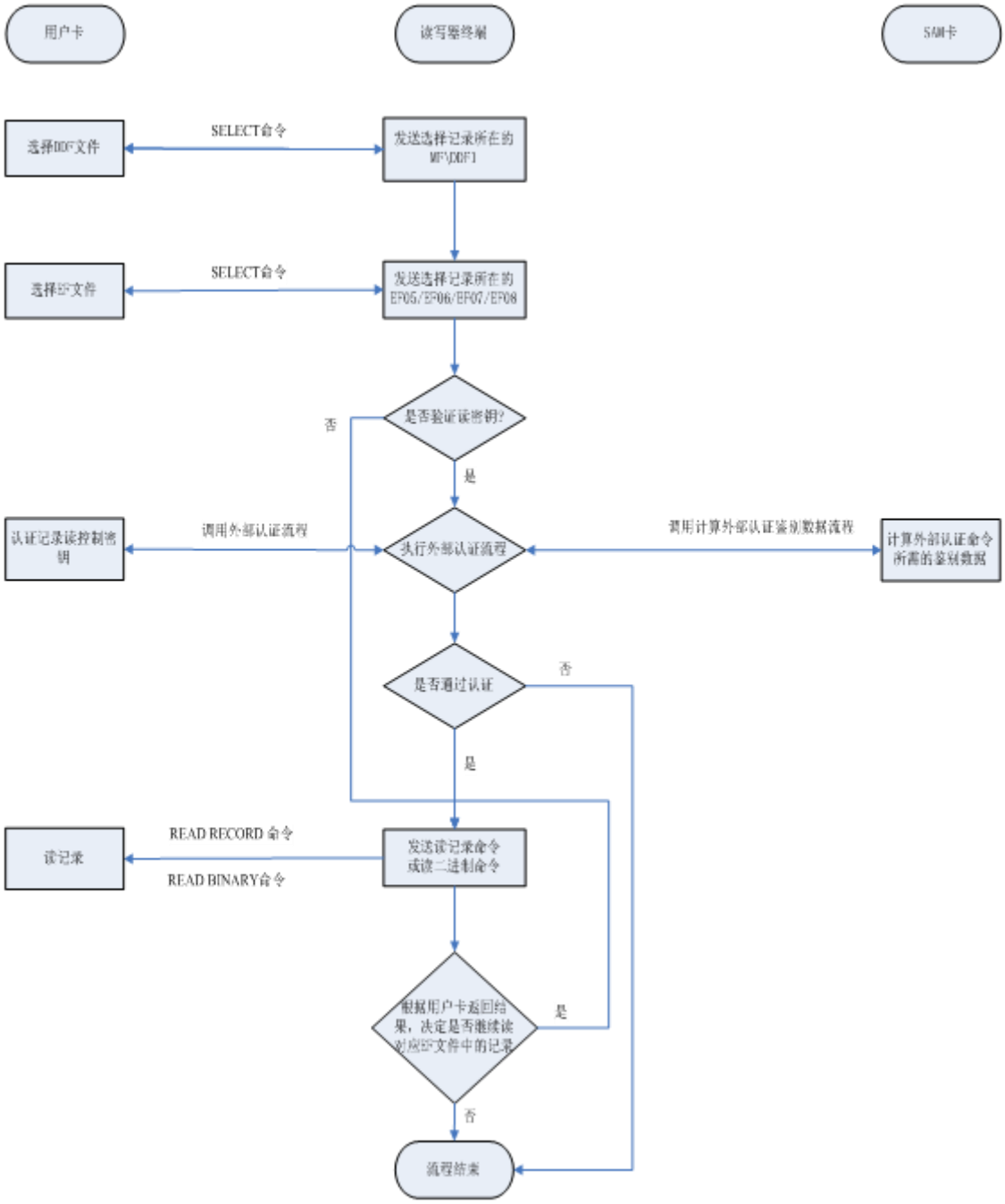

图5　读卡识别数据流程图

6.1.3　写卡识别数据区信息

6.1.3.1　概述

更新用户卡中MF\DDF1中的基本文件(即EF07和EF08)数据。

6.1.3.2　处理流程

流程具体如下：

a)　终端根据应用执行的情况决定更新用户卡中哪些记录；

b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS/T 543.2 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/T 543.2，外部认证命令处理过程参见本文档的对应章节）；
d) 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 STKDDF1 计算密文及 MAC；终端发送 UPDATE BINARY 命令更新 EF07 数据；
e) 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/T 543.2 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；
f) 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。

6.1.3.3 流程图

写卡识别数据处理流程图如图6所示。

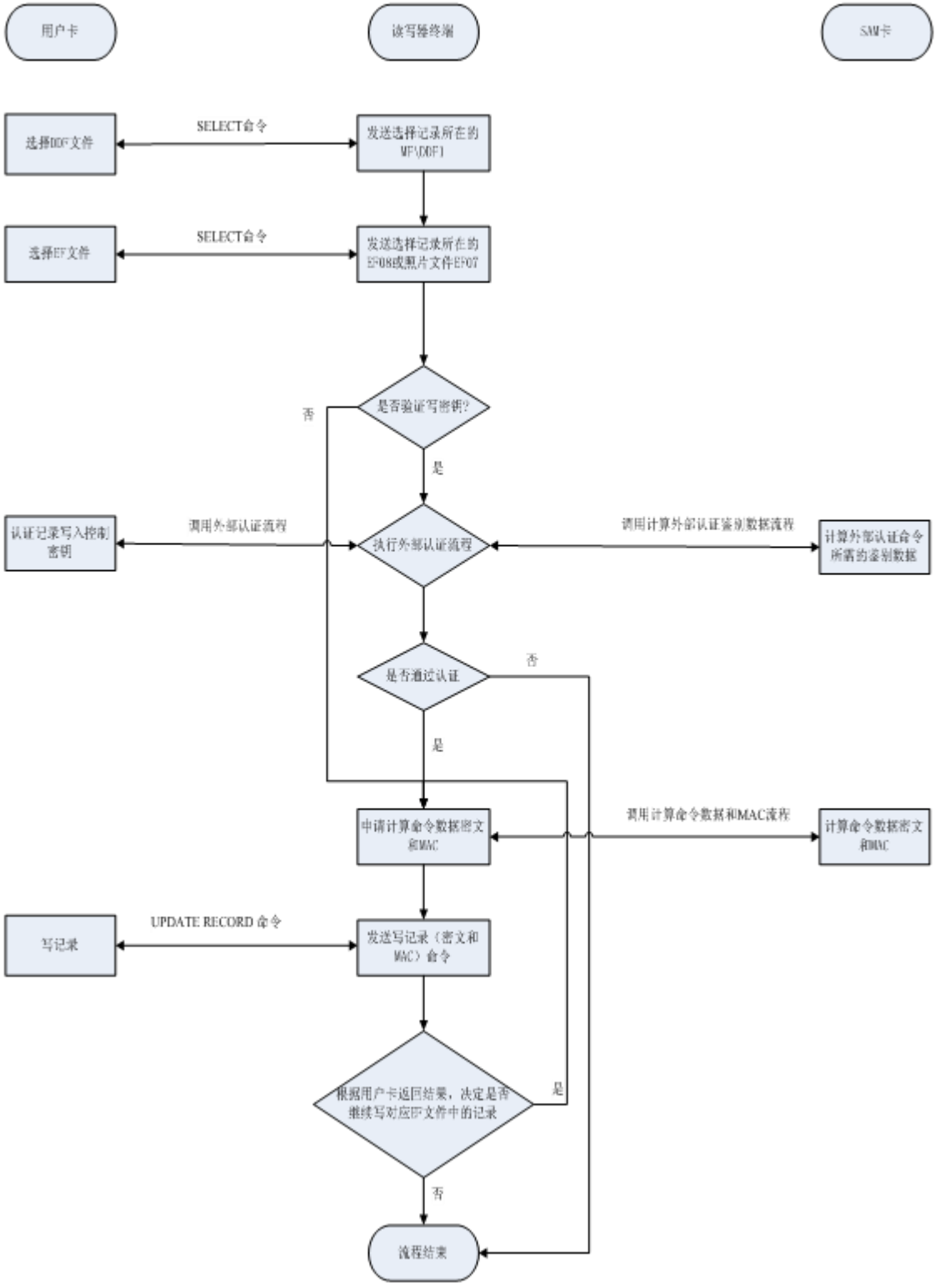

图6　写卡识别数据处理流程图

6.2　身份识别应用（对应 DDF1\DF01 数据区）

6.2.1　身份识别数据区

身份识别数据区包括EF05、EF06、EF07和EF08文件。

6.2.2 读 DF01 应用数据

6.2.2.1 概述

读取用户卡中的 DF01 应用数据。

6.2.2.2 处理流程

流程具体如下：

a) 终端根据应用执行的情况决定从用户卡读取哪些记录；
b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS/T 543.2 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/T 543.2，外部认证命令处理过程参见本文档的对应章节）；
d) 终端发送 READ RECORD 命令读取指定记录；
e) 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；
f) 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。

6.2.2.3 流程图

读DF01应用数据处理流程图如图7所示。

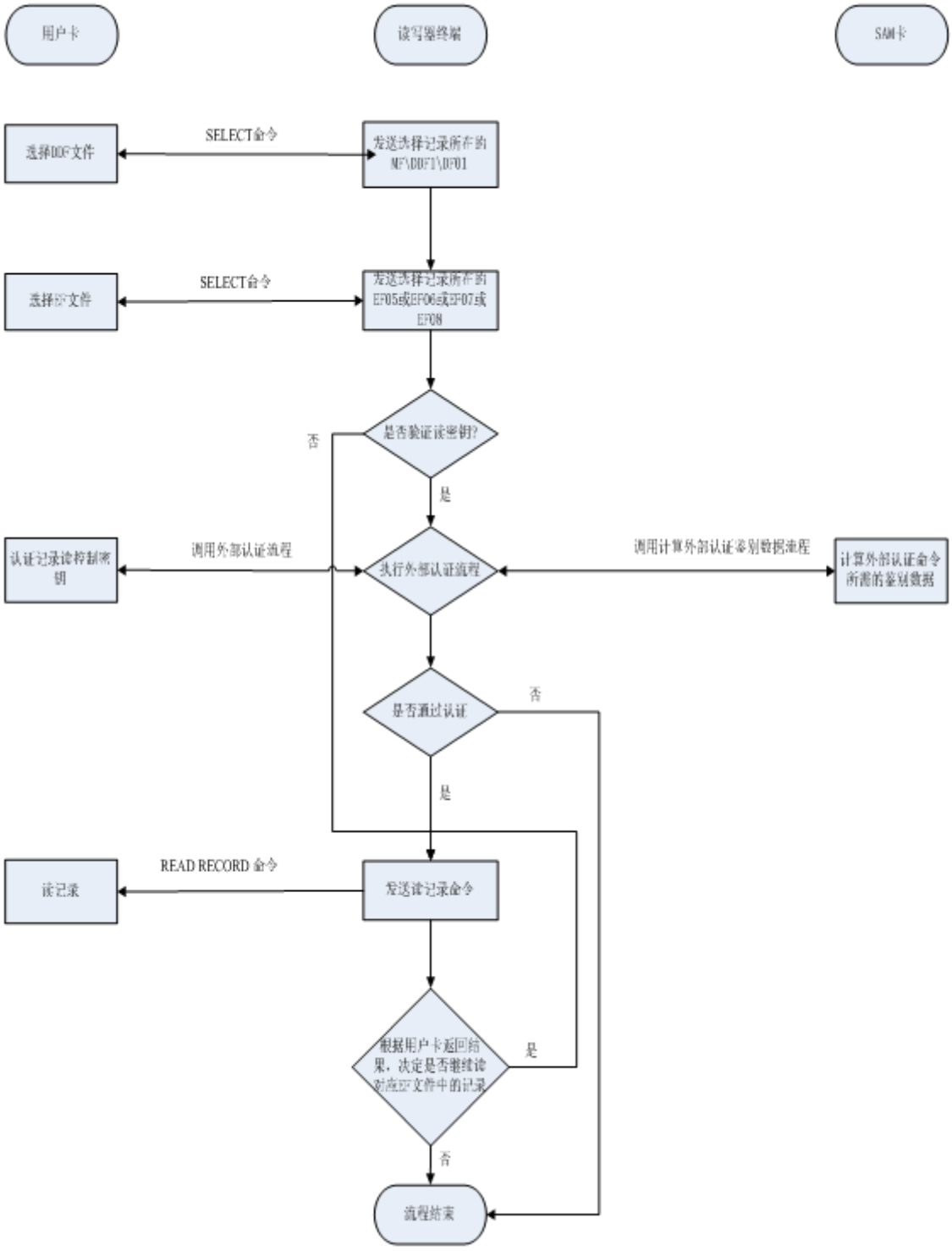

图7　读 DF01 应用数据处理流程图

6.2.3　写 DF01 应用数据

6.2.3.1　概述

更新用户卡中的DF01应用数据。

6.2.3.2　处理流程

流程具体如下：

a) 终端根据应用执行的情况决定更新用户卡中哪些记录；
b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS/T 543.2 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/T 543.2，外部认证命令处理过程参见本文档的对应章节）；
d) 终端发送带密文+MAC 安全报文的 UPDATE RECORD 命令更新指定记录；
e) 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/T 543.2 中描述），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；
f) 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。

6.2.3.3 流程图

写DF01应用数据处理流程图如图8所示。

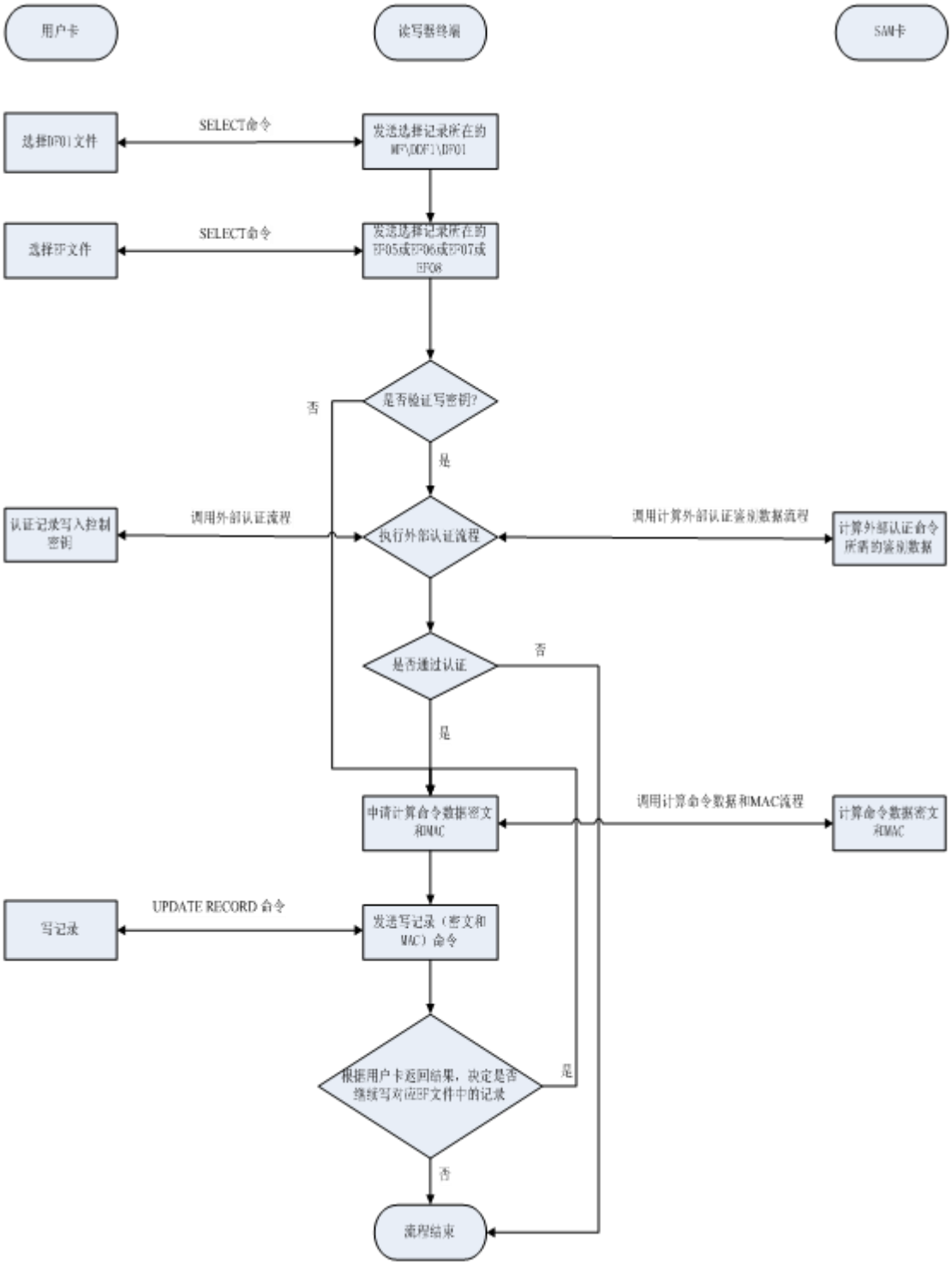

图8　写 DF01 应用数据处理流程图

6.3　基础健康数据应用（对应 DDF1\DF02 数据区）

6.3.1　基础健康数据区

基础健康数据区包括EF05、EF06、EF07和EF08文件。

6.3.2 读 DF02 应用数据

6.3.2.1 概述

读取用户卡中的DF02应用数据。

6.3.2.2 处理流程

流程具体如下：

a) 终端根据应用执行的情况决定从用户卡读取哪些记录；
b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS 543.2 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/T 543.2，外部认证命令处理过程参见本文档的对应章节）；
d) 终端发送 READ RECORD 命令读取指定记录；
e) 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；
f) 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。

6.3.2.3 流程图

读DF02应用数据处理流程图如图9所示。

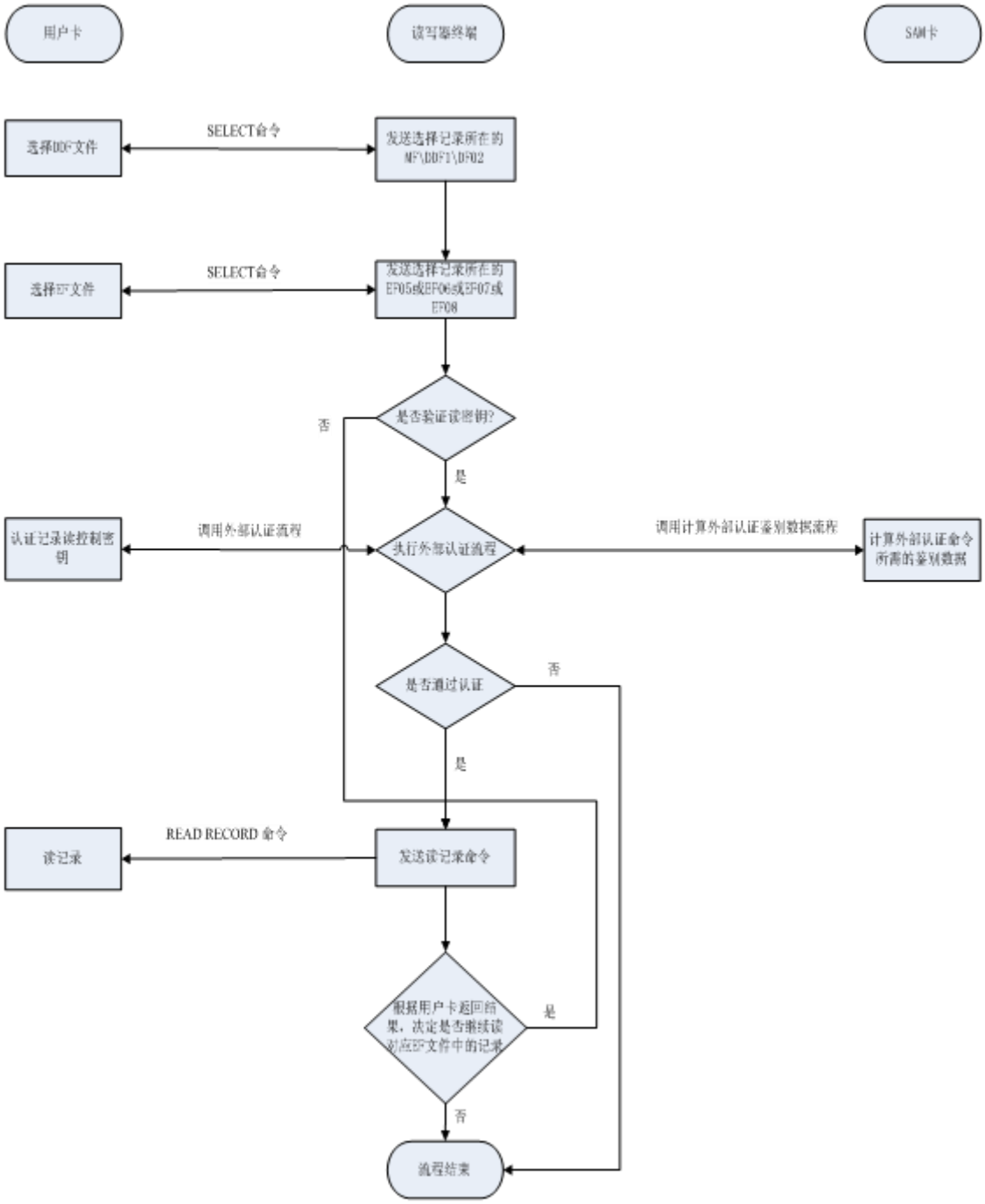

图9　读 DF02 应用数据处理流程图

6.3.3　写 DF02 应用数据

6.3.3.1　概述

更新用户卡中的DF02应用数据。

6.3.3.2　处理流程

流程具体如下：

a)　终端根据应用执行的情况决定更新用户卡中哪些记录；

b) 终端选择对应记录所在的 DF 文件，然后再选对应的 EF 文件；
c) 终端根据应用执行情况和 WS/T 543.2 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/T 543.2，外部认证命令处理过程参见本文档的对应章节）；
d) 终端发送带密文+MAC 安全报文的 UPDATE RECORD 命令更新指定记录；
e) 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/T 543.2 中描述），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。
f) 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。

6.3.3.3 流程图

写DF02应用数据处理流程图如图10所示。

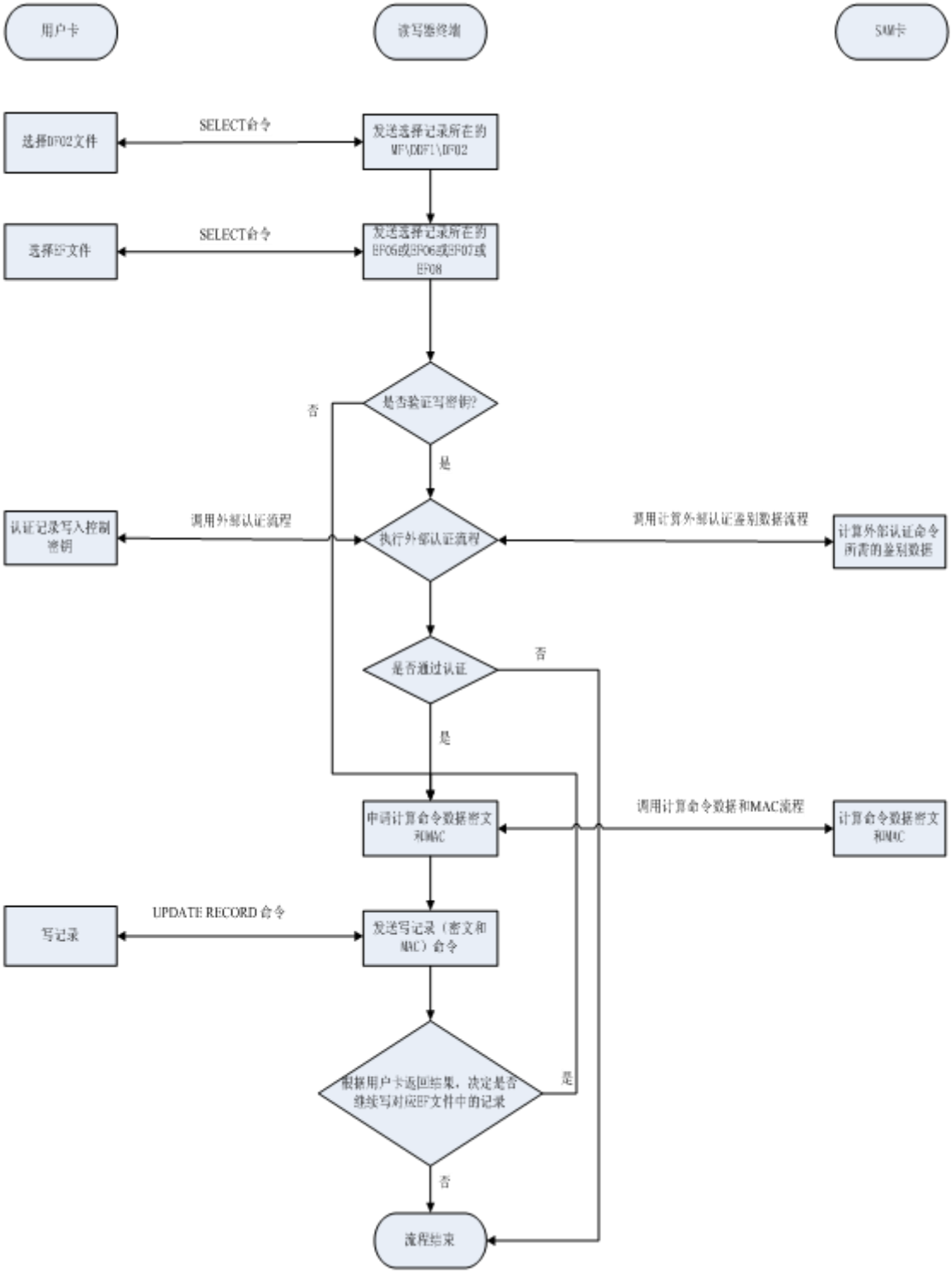

图10　写 DF02 应用数据处理流程图

6.4　管理业务应用(对应 DDF1\DF03 数据区)

6.4.1　管理业务数据区

管理业务数据区包括读写用户卡中住院信息索引文件（DF03\EF05）及住院信息（DF03\EE01-03）、门诊信息索引文件（DF03\EF06）及门诊信息（DF03\ED01-05）。MAC的计算方法和步骤参见WS/T 543.2中描述。

6.4.2 记录住院信息

6.4.2.1 概述

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

6.4.2.2 记录住院信息流程

流程具体如下：

a) 终端获得住院信息索引文件读权限；
b) 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）；
c) 如果没有空记录，则无法记录住院信息，流程结束；
d) 终端获得住院信息文件写权限；
e) 终端向用户卡发送 SELECT 命令，选择住院信息文件；
f) 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；
g) 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；
h) 终端向用户卡发送 SELECT 命令，选择住院信息索引文件；
i) 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；
j) 流程结束。

6.4.2.3 流程图

住院信息记录流程图如图11所示。

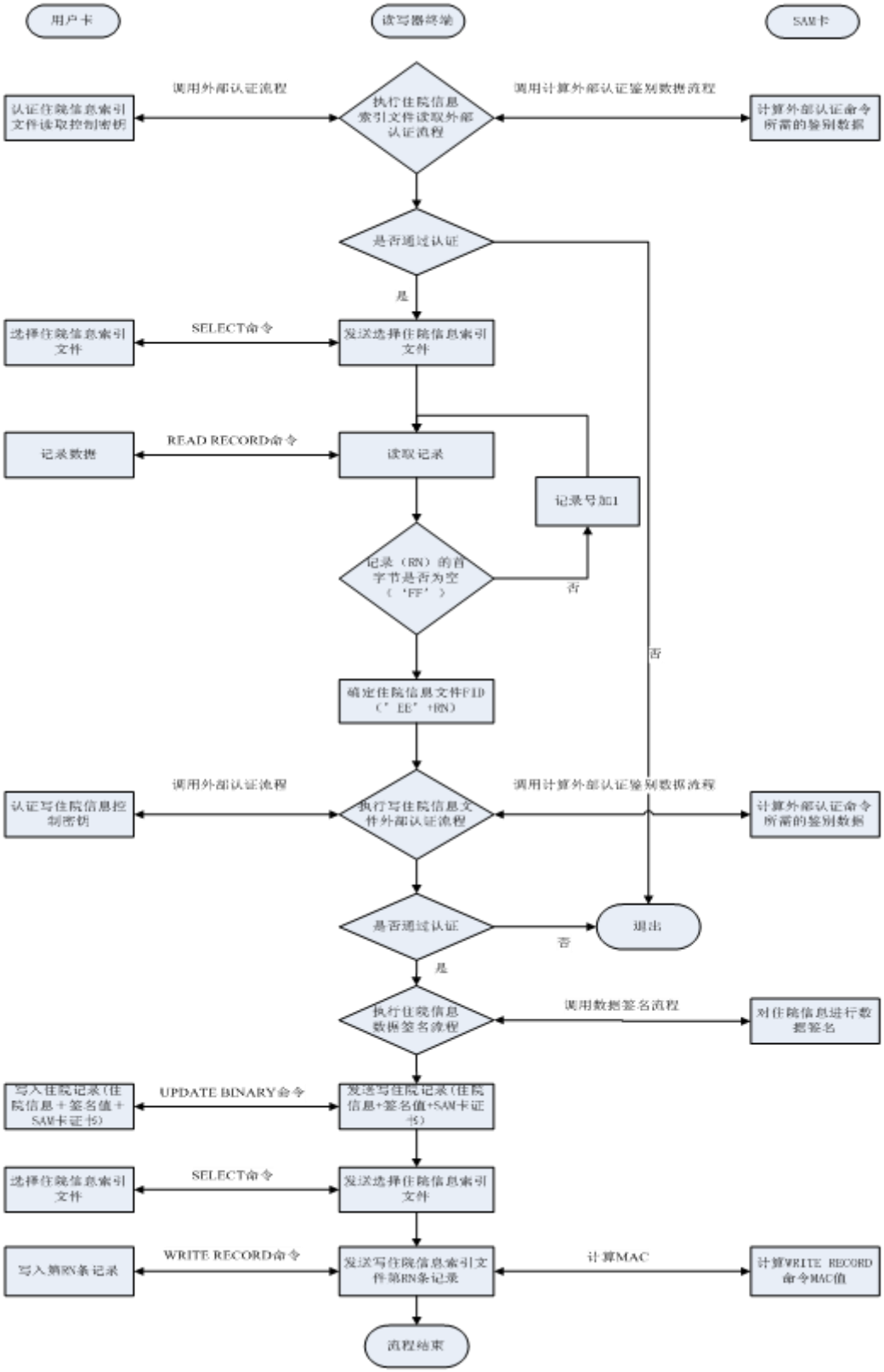

图11　住院信息记录流程图

6.4.3　记录门诊信息

6.4.3.1　概述

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

6.4.3.2 记录门诊信息流程

流程具体如下：

a) 终端获得门诊信息索引文件读权限；
b) 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）；
c) 如果没有空记录，则无法记录门诊信息，流程结束；
d) 终端获得门诊信息文件写权限；
e) 终端向用户卡发送 SELECT 命令，选择门诊信息文件；
f) 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；
g) 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；
h) 终端向用户卡发送 SELECT 命令，选择门诊信息索引文件；
i) 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；
j) 流程结束。

6.4.3.3 流程图

门诊信息记录流程图如图12所示。

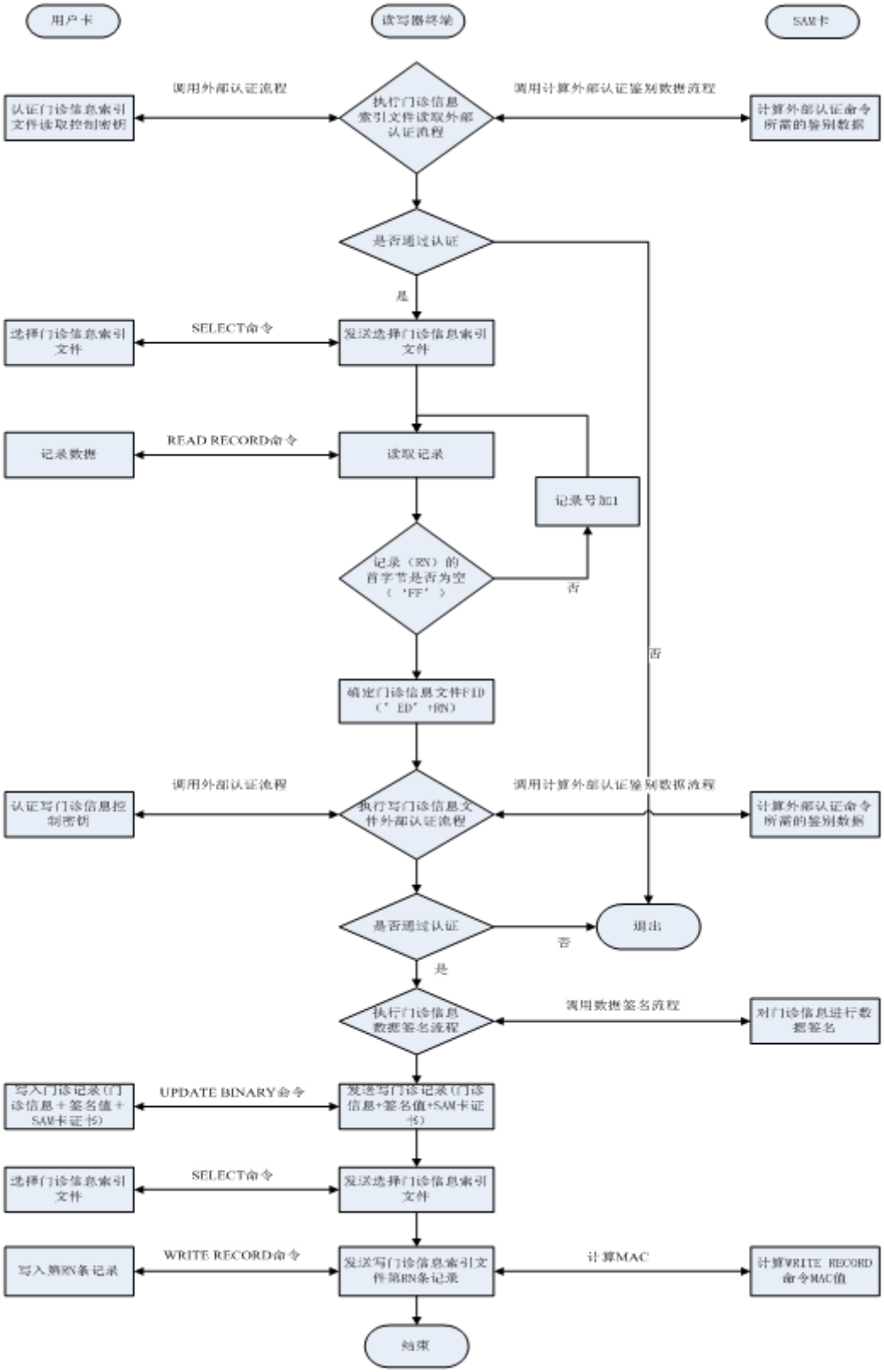

图12　门诊信息记录流程图

6.4.4　住院费用信息提取及费用报销

6.4.4.1　概述

本文件描述了住院费用提取及报销的简易流程。

6.4.4.2 住院费用信息提取及报销流程

流程具体如下：

a) 终端获得住院信息索引文件（DF03\EF05）读权限；
b) 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）；
c) 终端向用户卡发送 SELECT 命令，选择住院信息文件；
d) 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）；
e) 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；
f) 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；
g) 终端获得住院信息索引文件擦除权限；
h) 终端向用户卡发送 SELECT 命令，选择住院信息索引文件；
i) 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；
j) 流程结束。

6.4.4.3 流程图

住院费用提取及报销流程图如图13所示。

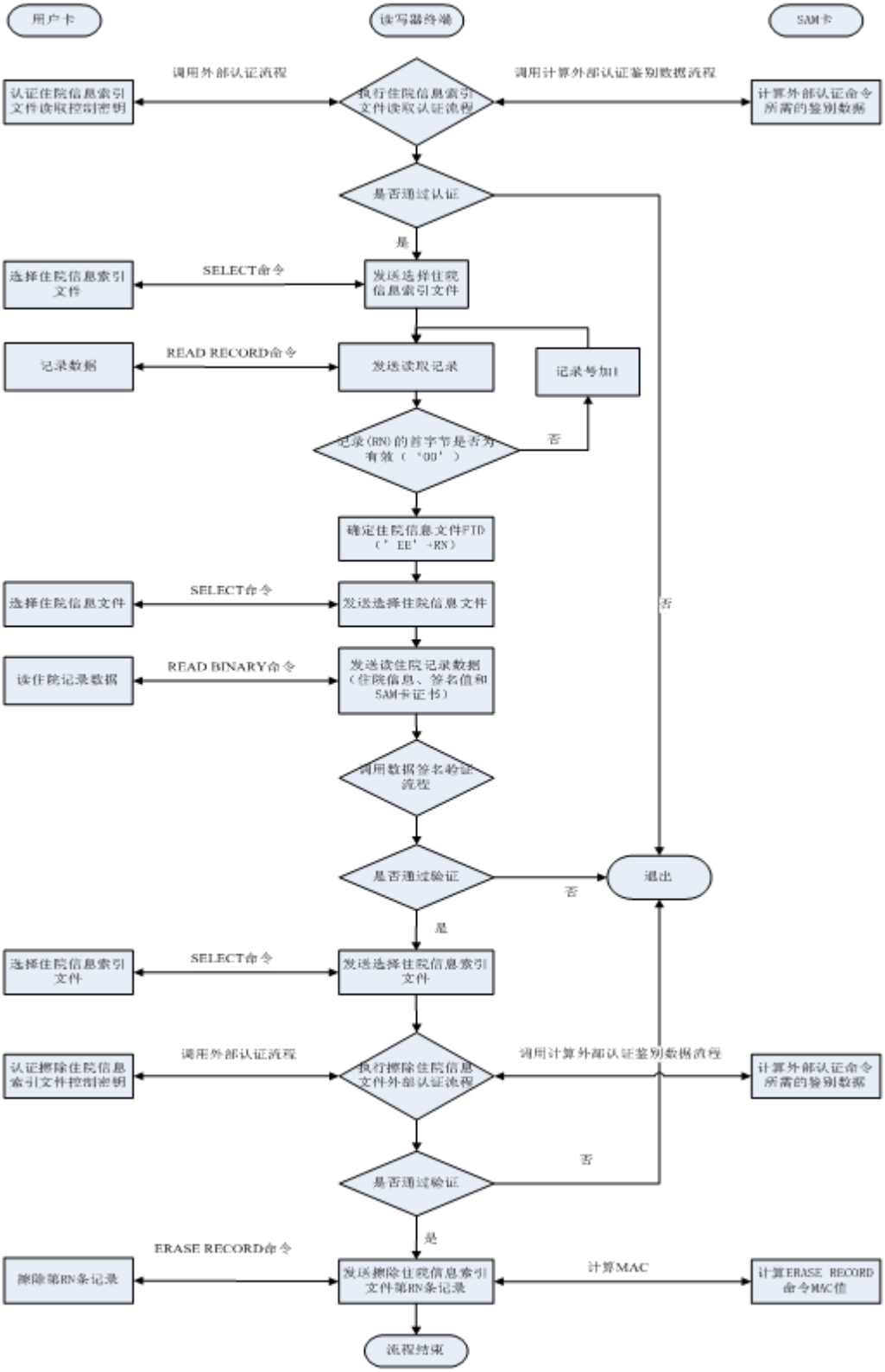

图13　住院费用提取及报销流程图

6.4.5　门诊费用信息提取及报销

6.4.5.1　概述

本文件描述了门诊费提取及报销的简易流程。

6.4.5.2 门诊费用提取及报销流程

流程具体如下：

a) 终端获得门诊信息索引文件（DF03\EF06）读权限；
b) 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）；
c) 终端向用户卡发送 SELECT 命令，选择门诊信息文件；
d) 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）；
e) 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；
f) 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；
g) 终端获得门诊信息索引文件擦除权限；
h) 终端向用户卡发送 SELECT 命令，选择门诊信息索引文件；
i) 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；
j) 流程结束。

6.4.5.3 流程图

门诊费用提取及报销流程图如图14所示。

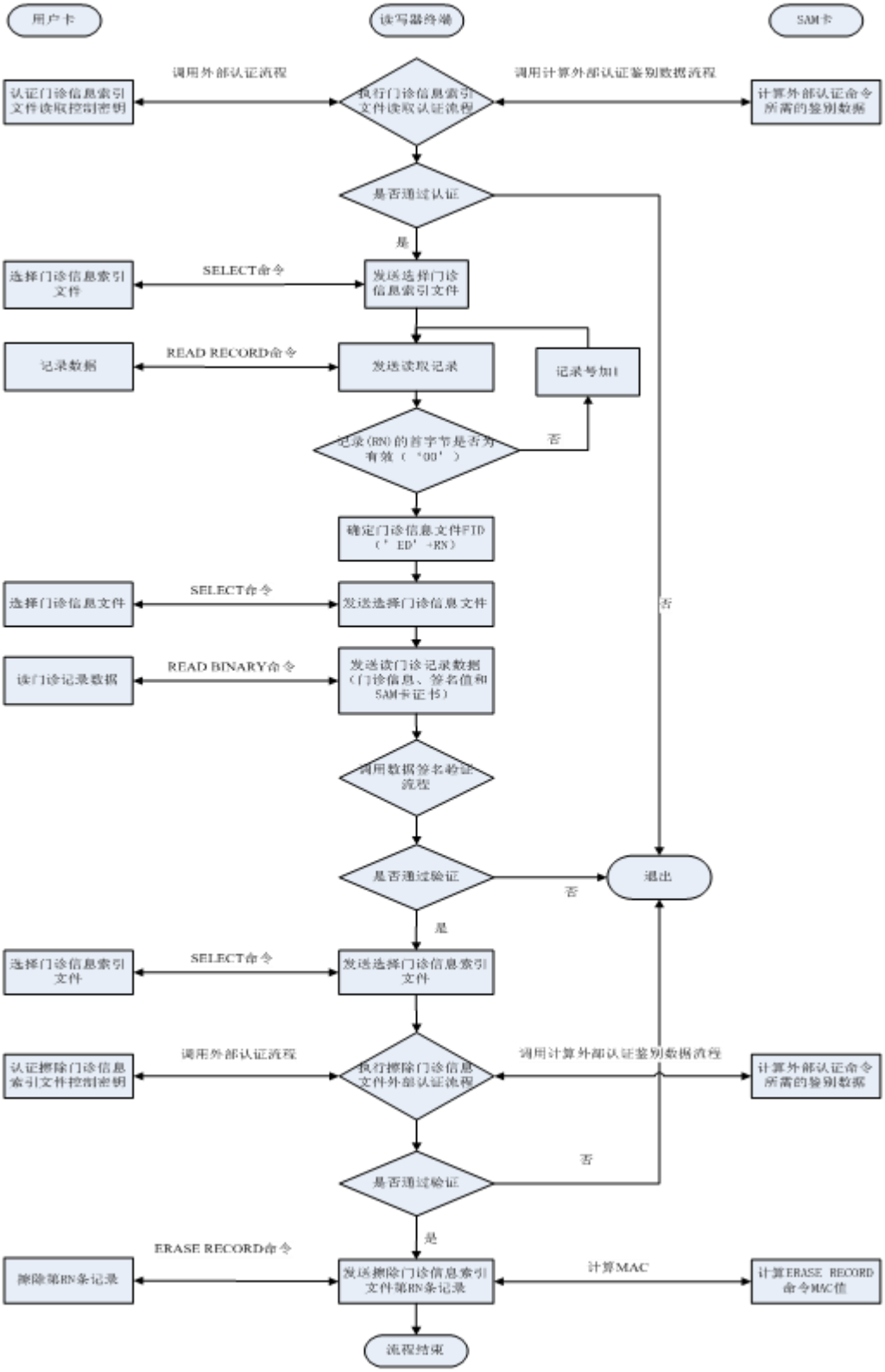

图14　门诊费用提取及报销流程图

7　数据签名和验证

7.1 数据签名

7.1.1 概述

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 数据签名流程

流程具体如下：

a) 终端获得需签名的住院（或门诊）信息数据；
b) 终端向 SAM 卡发送 SELECT 命令，选择 SAM 卡 DF01 目录；
c) 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；
d) 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；
e) 流程结束。

7.1.3 流程图

数据签名流程图如图15所示。

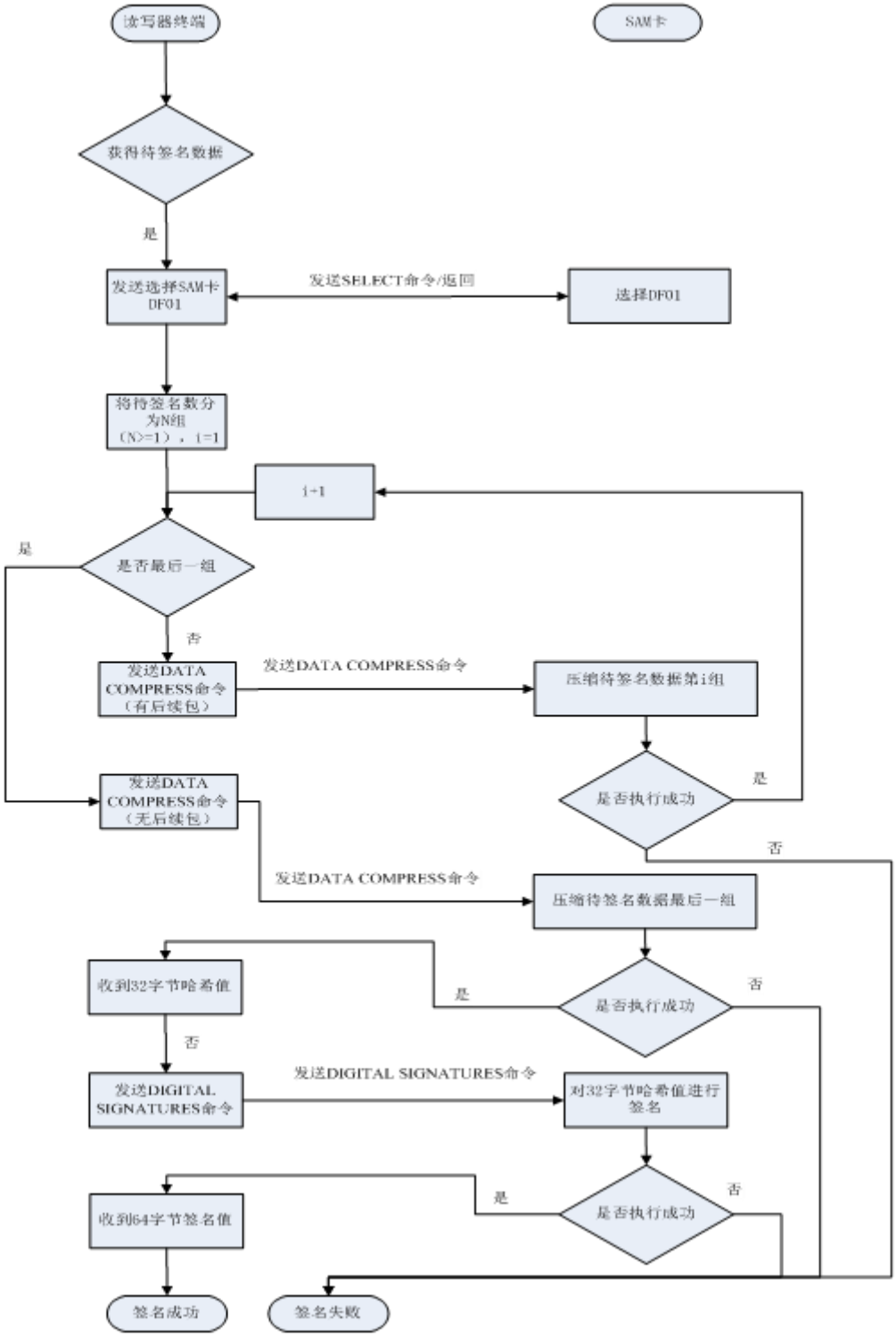

图15　数据签名流程图

7.2　数据签名验证

7.2.1　概述

本文件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 数据签名验证流程

证书密钥的使用参见WS/T 543.2中描述：

a) 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；
b) 后台将验证结果发送到终端；
c) 终端根据返回结果判断数据签名验证是否成功；
d) 流程结束。

7.2.3 流程图

数据签名验证流程图如图16所示。

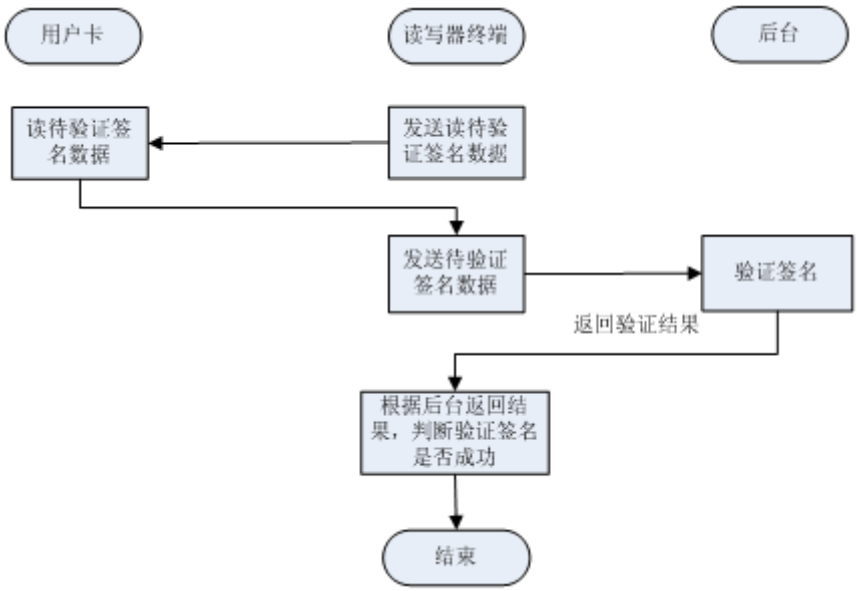

图16 数据签名验证流程图