社会保障（个人）卡规范
第 7 部分：应用流程

引言

本部分作为《社会保障（个人）卡规范》的第 7 部分，包括以下主要内容：

——社会保障应用的交易流程。该流程描述的是卡片插入终端并与终端相互作用后，所进行的交易处理过程。

1　适用范围

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

2　参考文件

3　定义

以下定义适用于本规范。

3.1　终端（Terminal）

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

3.2　命令（Command）

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.3　响应（Response）

IC 卡处理完成收到的命令报文后，返回给终端的报文。

3.4　交易（Transaction）

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.5　功能（Fuction）

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

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

内部封装一个或多个集成电路的 ID-1 型卡（如 ISO/IEC 7810、ISO/IEC 7811 第 1 至第 5 部分、ISO/IEC 7812 和 ISO/IEC 7813 中描述的）。

3.7　报文（Message）

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.8　报文鉴别代码（Message Authentication Code）

对交易数据及其相关参数进行运算后产生的代码，主要用于验证报文的完整性。

3.9　密钥（Key）

控制加密转换操作的符号序列。

3.10 社会保障应用（Social Security Application）

在人力资源和社会保障各专业领域管理和服务工作中的社会保障卡应用总称。

3.11 帐户划入（Wipe In Account）

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

3.12 医疗消费（Medical Treatment Consume）

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

3.13 帐户支付（Account Payment）

指持卡人从卡内基本医疗保险个人帐户中支付医疗费用。

3.14 个人自付（Individual Payment）

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

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

指持卡人在医疗消费中，基本医疗保险统筹基金支付的金额。

3.16 支付年度（Year of Payment）

指卡内基本医疗保险统筹基金支付累计金额所对应的结算年度。

3.17 年度起始日期（Starting Day）

指卡内基本医疗保险统筹基金支付所对应的结算年度起始日期。

4 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

AID	应用标识符（Application Identifier）
CIA	卡内医疗保险个人帐户（Individual Account for Medical Treatment on Card）
FCI	文件控制信息（File Control Information）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
ISO	国际标准化组织（International Organization for Standardization）
Lc	终端发出的命令数据的实际长度（Exact Length of Data Sent by the TAL in a Case 3 or 4 Command）
MAC	报文鉴别代码（Message Authentication Code）
PIN	个人密码（Personal Identification Number）
POS	服务网点终端（Point of Service）
PSAM	服务网点终端安全存取模块（Practice Secure Access Module）
SPFP	统筹基金支付累计（Social-pooling Fund Payment）
SPIP	个人自付累计（Accumulative Total of Individual Payment）
SSSE	社会保障系统环境（Social Security System Environment）
TAC	交易验证码（Transaction Authorization Cryptogram）

5 交易预处理

图 1 给出了对社会保障应用的所有交易类型共有的预处理流程。

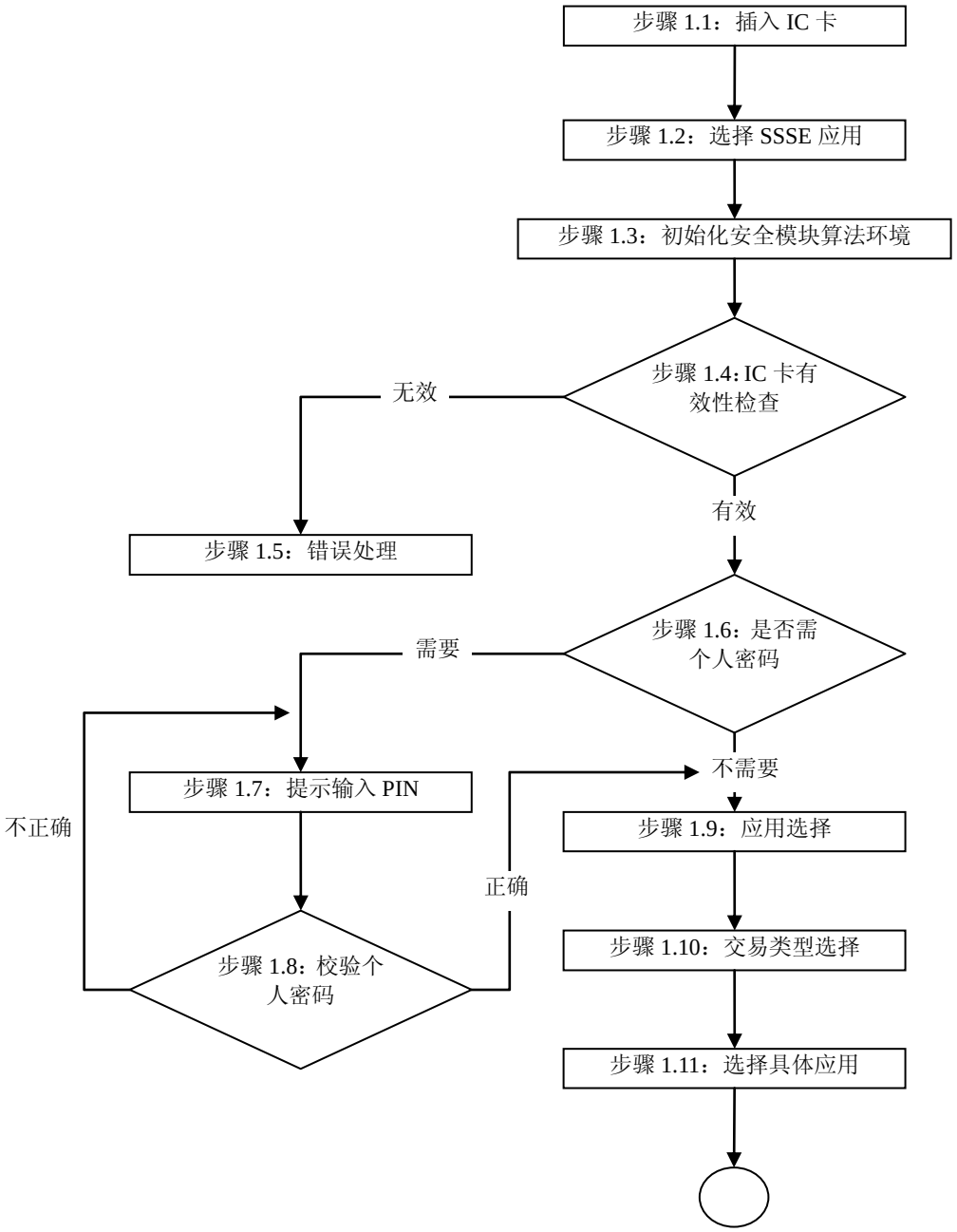

图 1　交易预处理流程

5.1　插入 IC 卡（步骤 1.1）

终端应具有检测 IC 卡是否已经插入读卡器的功能。如果 IC 卡已经插入，终端将继续执行步骤 1.2（见 5.2）。

5.2　选择社会保障应用环境 SSSE（步骤 1.2）

使用“SELECT”命令对社会保障应用环境进行选择。

5.3　初始化安全模块算法环境（步骤 1.3）

选择 SSSE 系统环境后，根据返回的 FCI 中的算法标识确定所采用的算法。如未读到算法标识，采用默认算法。

5.4 IC 卡有效性检查（步骤 1.4）

首先使用 IRK 对发卡方进行验证，步骤如下：

——终端产生两个 8 字节的随机数，按如下方式构成“INTERNAL AUTHENTICATION”命令的数据域：

随机数 $1_{(终端)}$ ‖ 随机数 $2_{(终端)}$ ‖ 密钥版本号（如果有的话）；

注：随机数 1 用于产生过程密钥，随机数 2 用于产生鉴别数据。

——终端发送“INTERNAL AUTHENTICATION”命令，卡将计算鉴别数据并回送；

——终端在收到鉴别数据后，进行比较验证。

如果验证不通过，则按 5.5 中的描述进行；如果验证通过，则用“READ RECORD”命令读取发卡机构数据，终端将对这些数据进行以下检查：

——该卡是否在终端存储的黑名单[①]之列（使用“卡的标识码”和“卡号”）；

——终端是否支持初始化机构编号；

——终端是否支持从 IC 卡回送的“卡的类别”所代表的卡类型；

——终端是否支持从 IC 卡回送的“规范版本”所代表的应用版本；

——卡是否在有效期内。

如果以上任一条件不满足，交易将按步骤 1.5（见 5.5）中的描述进行；否则，终端继续执行步骤 1.6（见 5.6）。

5.5 错误处理（步骤 1.5）

终端对交易预处理出错的处理方法不属于本规范的范围，但建议至少应根据《社会保障（个人）卡规范》第 2 部分：机电特性、逻辑接口与传输协议中的规定，将接口设备的所有触点置为静止状态。

5.6 是否需要个人密码（PIN）（步骤 1.6）

终端发送 Lc=‘00’的“VERIFY”命令，如果卡回送‘9000’，则转入步骤 1.9（见 5.9）继续执行；如果卡回送‘63Cx’，则按步骤 1.7（见 5.7）所述执行。

5.7 提示输入个人密码（PIN）（步骤 1.7）

终端将提示持卡人输入 PIN。

5.8 校验 PIN（步骤 1.8）

持卡人输入 PIN 后，终端将使用“VERIFY”命令来校验持卡人输入的 PIN 是否正确。

当 IC 卡收到校验（“VERIFY”）命令后，它将进行以下操作：

——检查 PIN 尝试计数器。如果 PIN 尝试计数器为零，此时 PIN 已锁定，因此不执行该命令。这种情况下，IC 卡回送状态码‘6983’（鉴别方式锁定）结束交易过程。

——如果 PIN 没有被锁定，则将命令数据中的 PIN 和 IC 卡中存放的 PIN 进行比较。

——如果以上两个 PIN 相同，IC 卡将 PIN 尝试计数器置为允许 PIN 重试的最大次数并回送状态码‘9000’。IC 卡必须记住 PIN 成功验证的结果，直到断电。交易处理按步骤 1.9（见

[①] 黑名单的详细情况，包括维护、格式、内容不在本规范范围之内。

5.9）中的描述继续进行。

——如果以上两个 PIN 不同，IC 卡将 PIN 尝试计数器减 1 并回送状态码‘63Cx’，这里‘x’是 PIN 尝试计数器的新值。在这种情况下，终端将检查 x 的值。如果‘x’是 0，将终止交易，且卡片自动锁定 PIN；否则，终端将提示重新输入 PIN 并重复以上过程。

5.9 应用选择（步骤 1.9）

应用选择的执行过程请参见《社会保障（个人）卡规范》第 3 部分：文件系统和应用选择。社会保障应用的应用标识符（AID）和应用标签参见《社会保障（个人）卡规范》第 6 部分：应用数据结构。

成功地选择了某个具体的社会保障应用后，IC 卡回送文件控制信息。

通过应用选择，终端可以建立 IC 卡所支持的应用列表。

5.10 交易类型选择（步骤 1.10）

终端应该具备让持卡人或操作员选择交易类型的功能。每次交易最多只能选择一种交易类型。

持卡人应能选择如下交易类型：查询应用信息、更改个人密码、联机更改应用信息。

操作员应能选择如下交易类型：查询应用信息、更改应用信息、卡片锁定、应用锁定。

5.11 选择具体的社会保障应用（步骤 1.11）

如果 IC 卡和终端同时支持一种具体的社会保障应用，则选择该应用。

如果 IC 卡仅支持一种具体的社会保障应用但该应用不被终端支持，则该过程终止。

如果 IC 卡和终端彼此都支持若干种具体的社会保障应用，终端应向持卡人（或操作员）提供明确选择一种具体的社会保障应用的过程，在这一过程中持卡人（或操作员）可以选定一种具体的社会保障应用进行交易。

6 查询应用信息

通过查询应用信息，持卡人（或操作员）可以获得社会保障卡中想了解的或与办理具体事务相关的信息。

这种交易对终端是否联网无任何要求，对某一具体的应用信息的读取操作权限仅受终端中的 PSAM 卡的控制。

发给出了查询应用信息的处理流程。

6.1 判断读取信息是否受控（步骤 2.1）

终端应该明确知道对某一具体的应用信息的读取操作是否受控。如果信息读取操作是不受控的，则转入步骤 2.8（见 6.8）；否则，继续按下述步骤执行。

6.2 发出“GET CHALLENGE”命令（步骤 2.2）

终端应发出“GET CHALLENGE”命令以获取产生鉴别数据所需的卡随机数。

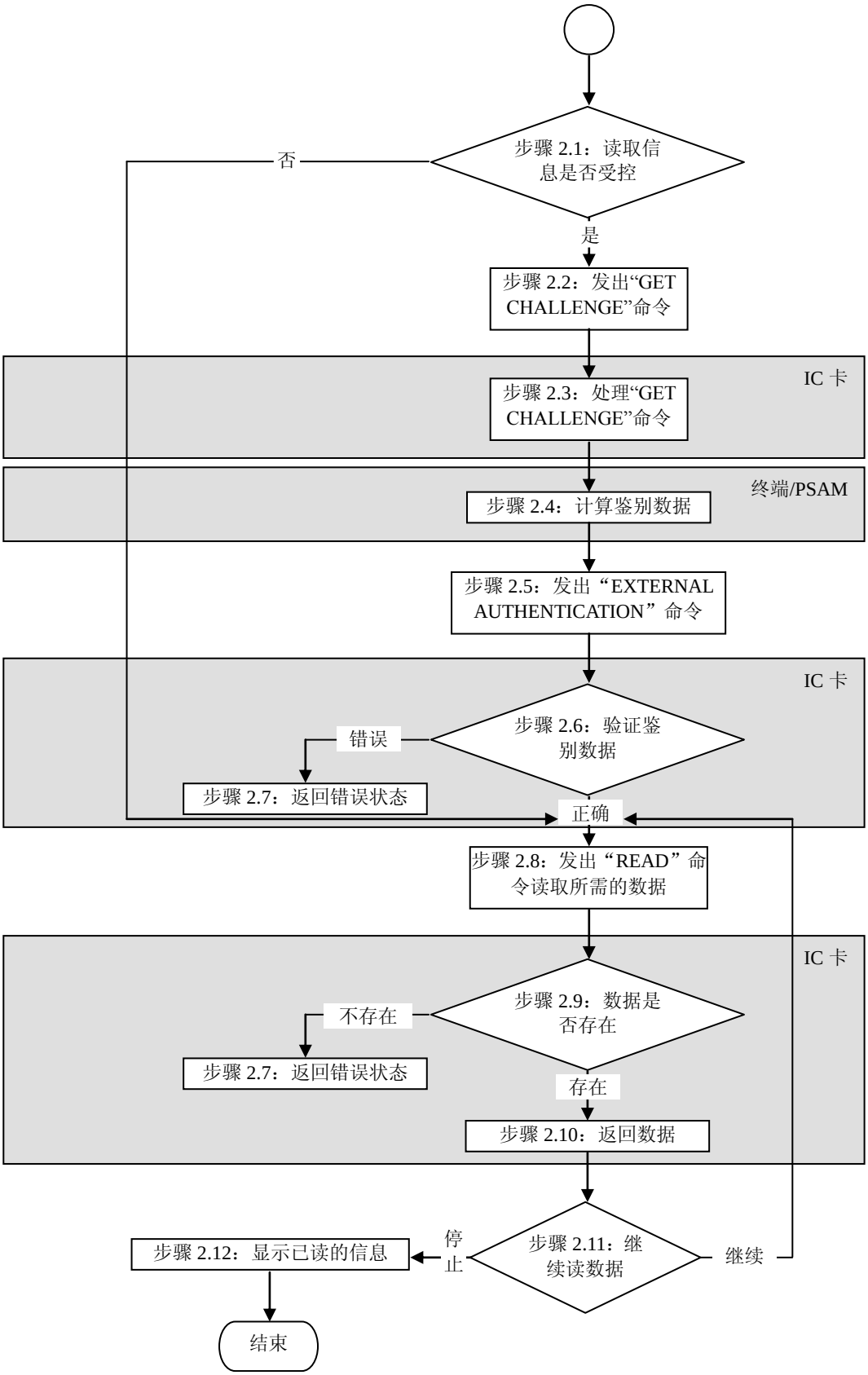

图 2　查询应用信息的处理流程

6.3 处理“GET CHALLENGE”命令（步骤 2.3）

收到“GET CHALLENGE”命令后，IC 卡将产生一个伪随机数$_{(ICC)}$，并将此随机数作为响应报文回送给终端。如果 IC 卡回送的状态码不是‘9000’，则交易终止。

6.4 计算鉴别数据（步骤 2.4）

终端在得到 IC 卡回送的随机数$_{(ICC)}$后，将进行以下操作：

——产生一个随机数$_{(终端)}$或向 PSAM 卡请求一个随机数$_{(PSAM)}$。

——使用预先设定的控制密钥和密钥版本号（可选），要求 PSAM 卡计算并返回鉴别数据。如果 PSAM 卡中不存在所需的控制密钥或不支持密钥版本号，则 PSAM 卡应该除了回送表示“密钥找不到”或“不支持密钥版本”的状态码外不回送任何其他数据，此时终端应终止命令的处理过程。

6.5 发出“EXTERNAL AUTHENTICATION”命令（步骤 2.5）

终端应发出“EXTERNAL AUTHENTICATION”命令启动控制权限认证。

命令报文中的数据域按以下方式构成：

鉴别数据 ‖ 随机数$_{(终端)}$或随机数$_{(PSAM)}$ ‖ 密钥版本号（如果有的话）

6.6 验证鉴别数据（步骤 2.6）

收到“EXTERNAL AUTHENTICATION”命令响应报文后，IC 卡将进行以下操作：

——检查指定密钥的尝试计数器。如果其值为零，则该密钥已锁定，因此不执行该命令。这种情况下，IC 卡回送状态码‘6983’（鉴别方式锁定）结束交易过程。

——如果密钥没有被锁定，则使用随机数$_{(ICC)}$ （由“GET CHALLENGE”命令产生）按照《社会保障（个人）卡规范》第 4 部分：安全机制描述的方式产生过程密钥。

——使用该过程密钥按照《社会保障（个人）卡规范》第 4 部分：安全机制描述的方式计算出 IC 卡内部的鉴别数据，并与命令数据中的鉴别数据进行比较。

——如果以上两个鉴别数据相同，IC 卡将该密钥的尝试计数器置为它所允许的重试最大次数并回送状态码‘9000’。IC 卡必须记住该密钥成功鉴别的结果，直到断电或选择了其他应用。交易处理按步骤 2.8（见 6.8）中的描述继续进行。

——如果以上两个鉴别数据不同，IC 卡将该密钥的尝试计数器减 1 并回送状态码‘63Cx’，这里‘x’是该密钥尝试计数器的新值。在这种情况下，终止该交易。如果‘x’是 0，卡片自动锁定该密钥。

6.7 回送错误状态（步骤 2.7）

如果 IC 卡不接受交易过程中的命令或在处理命令过程中诊断出问题，它都应向终端回送错误状态并结束交易。此时终端所做的处理不在本规范范围内。

6.8 发出“READ”命令（步骤 2.8）

根据应用数据的存储格式，终端应发出“READ BINARY”或“READ RECORD”命令来读取所需的应用信息。至于终端如何区分应用数据的存储格式，本规范不作规定。

6.9 处理“READ”命令（步骤 2.9）

收到“READ”命令后，IC 卡将按命令报文的参数寻找终端所请求的数据。如果数据存在，则按 6.10 中的描述继续进行，否则应按步骤 2.7（见 6.7）中的描述操作。

6.10 返回数据（步骤 2.10）

在成功找到数据后，IC 卡通过“READ”命令的响应报文将数据返回给终端。

6.11 判断是否还需继续读数据（步骤 2.11）

终端在成功读取一条信息后，应根据交易的要求，判断是否还要读取更多的数据。如果需要继续读取数据，则转入步骤 2.8（见 6.8）继续进行，否则按步骤 2.12（见 6.12）中的描述操作。

6.12 显示已读的数据（步骤 2.12）

终端将已读取的信息通过显示设备提供给持卡人或业务管理部门的操作员。这些信息的显示格式超出了本规范的范围。

7 操作员更新应用信息

通过更新应用信息，业务管理部门的操作员可以在社会保障卡中记录持卡人办理具体事务时产生变动的相关信息。

这种交易对终端是否联网无任何要求，对某一具体的应用信息的更新操作仅受终端中的 PSAM 卡的控制。

转入步骤 3.8（见 7.3）给出了操作员更新应用信息的处理流程。

7.1 判断更新信息是否受控（步骤 3.1）

终端应该明确知道对某一具体的应用信息的更新操作是否受控。如果信息更新操作是不受控的，则转入步骤 3.8（见 7.3）；否则，继续按下述步骤执行。

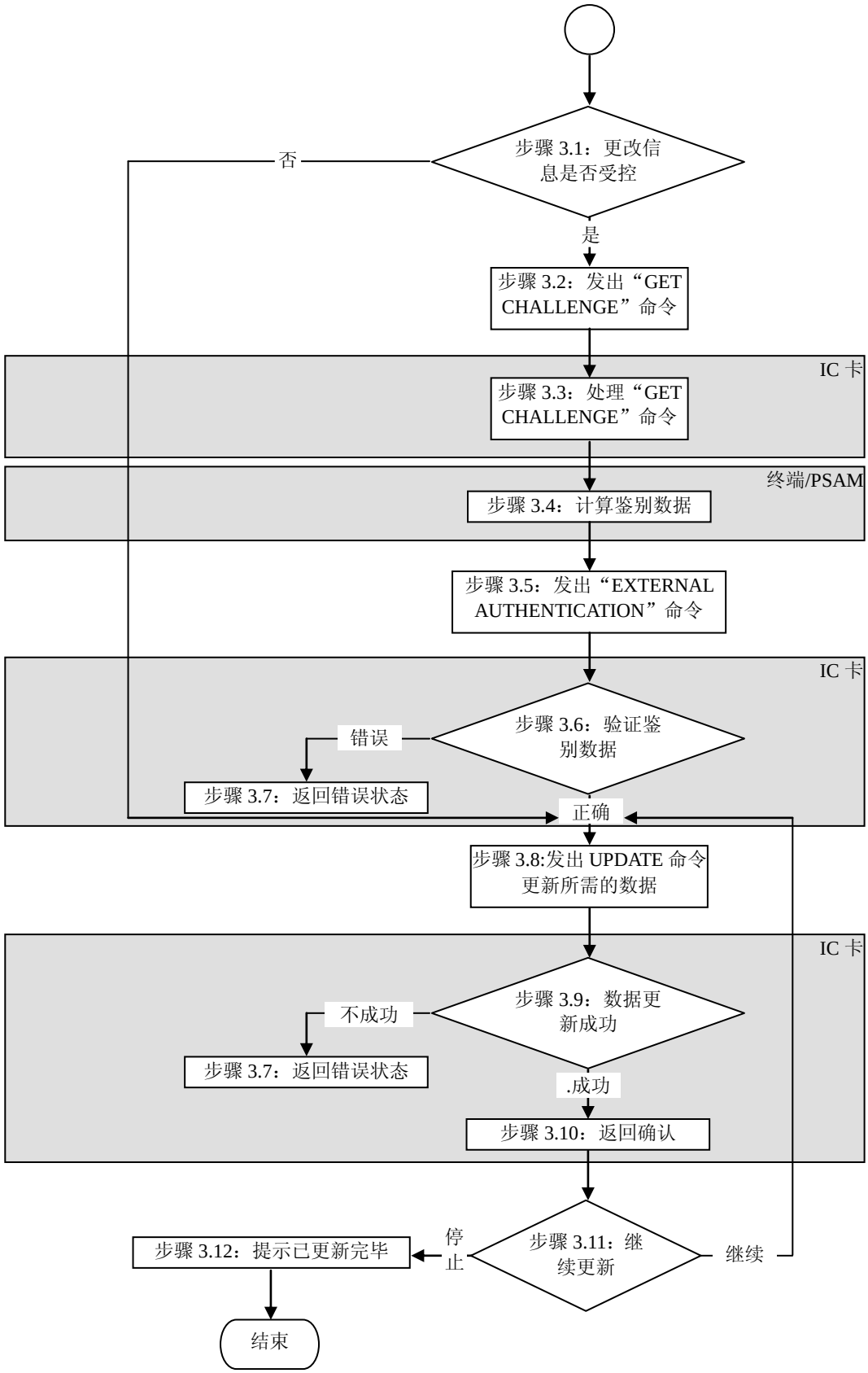

图 3　操作员更新应用信息的处理流程

7.2 更新操作权限的鉴别（步骤 3.2~步骤 3.7）

更新操作权限的鉴别过程与“查询应用信息”的步骤 2.2~步骤 2.7 相同（见 6 查询应用信息）。

7.3 发出“UPDATE”命令（步骤 3.8）

根据应用数据的存储格式，终端应发出“UPDATE BINARY”或“UPDATE RECORD”命令来更新所需的应用信息。至于终端如何区分应用数据的存储格式，本规范不作规定。如果具体应用要求使用安全报文，则应按《社会保障（个人）卡规范》第 4 部分：安全机制中的方法来计算和传递（本规范定义的应用不使用安全报文方式）。

7.4 处理“UPDATE”命令（步骤 3.9）

如果具体应用要求使用安全报文，IC 卡首先必须确认 MAC 是有效的。如果 MAC 有效，IC 卡继续执行交易处理；否则，IC 卡将向终端回送状态码’6987’（MAC 丢失）或’6988’（MAC 不正确）并终止交易。交易因安全报文出错而终止时，终端应采取的相应措施不在本规范范围内。

IC 卡将按命令报文的参数寻找所需更新数据的存储地址。如果找到存储地址并且确认正确记录后，则按步骤 3.10（见 7.5）中的描述继续进行；否则执行步骤 3.7（见 7.2）。

7.5 返回确认（步骤 3.10）

在成功更新数据后，IC 卡应向终端回送状态码‘9000’（正常）或‘63Cx’（经过‘x’次尝试后完成）来确认数据更新操作的完成。

7.6 判断是否还需继续更新数据（步骤 3.11）

终端在成功更新一条信息后，应根据交易的要求，判断是否还要更新更多的数据。如果需要继续更新数据，则转入步骤 3.8（见 7.3）继续进行，否则按 7.7 中的描述操作。

7.7 提示已更新完毕（步骤 3.12）

终端在确认应用要求的所有数据都已更新完成后，将通过适当的设备向业务管理部门的操作员提示交易完成。

8 持卡人联网更新信息

通过联网更新应用信息，持卡人可以在服务点终端（POS）上将主机系统内已经更改的信息下载至卡上。

该交易除受主机的控制外，还受终端中的 PSAM 卡的控制。

图 4 给出了持卡人联网更新应用信息的处理流程。

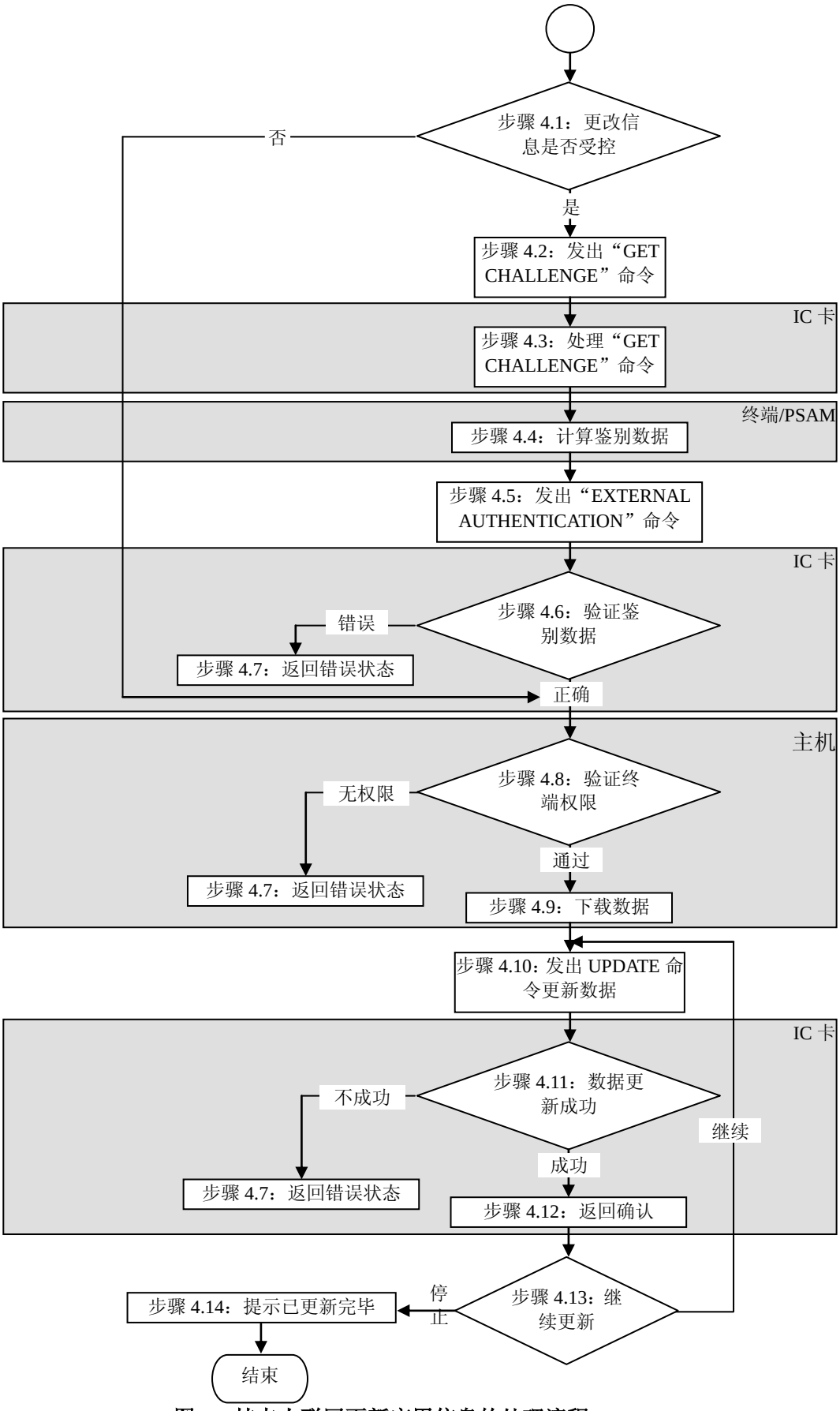

图 4　持卡人联网更新应用信息的处理流程

8.1 更新操作权限的鉴别过程（步骤 4.1~步骤 4.7）

该交易的更新操作权限的鉴别过程与“操作员更新应用信息”的步骤 3.1~步骤 3.7 相同（见 7 操作员更新应用信息）。

8.2 验证终端权限（步骤 4.8）

主机在收到终端请求下载数据的报文后，应根据具体应用的设定验证终端从主机下载相关应用数据的权限。如果主机拒绝交易，则应向终端发送一个拒绝报文，结束交易处理；如果主机允许交易，则按所描述的继续进行。

主机与终端之间的报文格式和主机与终端之间合法性或权限的验证方法都超出了本规范的范围。

8.3 下载数据（步骤 4.9）

主机应将终端所请求的数据按照特定的报文格式一次性全部传递给终端。在此过程中的数据安全要求以及终端如何安全地临时存放所下载的数据都超出了本规范的范围。

8.4 数据更新过程（步骤 4.10~步骤 4.14）

该交易的数据更新过程与“操作员更新应用信息”的步骤 3.8~步骤 3.12 相同（见 7 操作员更新应用信息）。

9 更改个人密码

更改个人密码功能可以让持卡人在任意一个支持该交易的终端上更改其个人密码（PIN）。

改 PIN 后，IC 卡应向终端回送状态码‘9000 给出了更改个人密码（PIN）的处理流程。

9.1 提示输入原有 PIN（步骤 5.1，可选）

终端通过显示设备提示持卡人输入原有的 PIN。

9.2 提示输入新的 PIN（步骤 5.2）

终端通过显示设备提示持卡人输入新的 PIN，并接收该 PIN。

9.3 提示确认新的 PIN（步骤 5.3）

在持卡人输入新的 PIN 后，终端应通过显示设备提示持卡人再次输入该新的 PIN，并将两次输入的结果进行比较。如果比较结果相同，则按所述继续进行；如果比较结果不一致，则向持卡人提示出错信息并结束交易。

9.4 发出“CHANGE PIN”命令（步骤 5.4）

终端应发出“CHANGE PIN”命令来更新 IC 卡中的 PIN。

9.5 用新的 PIN 替换原来的 PIN（步骤 5.5）

当 IC 卡接到“CHANGE PIN”命令时，它将进行以下操作：

——验证当前 PIN 是否锁定。

——验证原有 PIN。

——将 IC 卡上的 PIN 改为命令报文中的新 PIN。

——将 PIN 尝试计数器置为 PIN 重试的最大次数。

9.6 判断修改是否正确（步骤 5.6）

IC 卡应确认新的 PIN 已被正确记录。如果记录正确则按步骤 5.8（见 9.8）中的描述继

续进行；否则执行步骤 5.7（见 9.7）。

9.7　返回错误状态（步骤 5.7）

如果 IC 卡不接受“CHANGE PIN”命令或在处理命令过程中诊断出问题，它都应向终端回送错误状态并结束交易。此时终端所做的处理不在本规范范围内。

9.8　返回确认（步骤 5.8）

在成功更改 PIN 后，IC 卡应向终端回送状态码‘9000’（正常）来确认操作完成。终端应以合适的方式将此信息传达给持卡人。

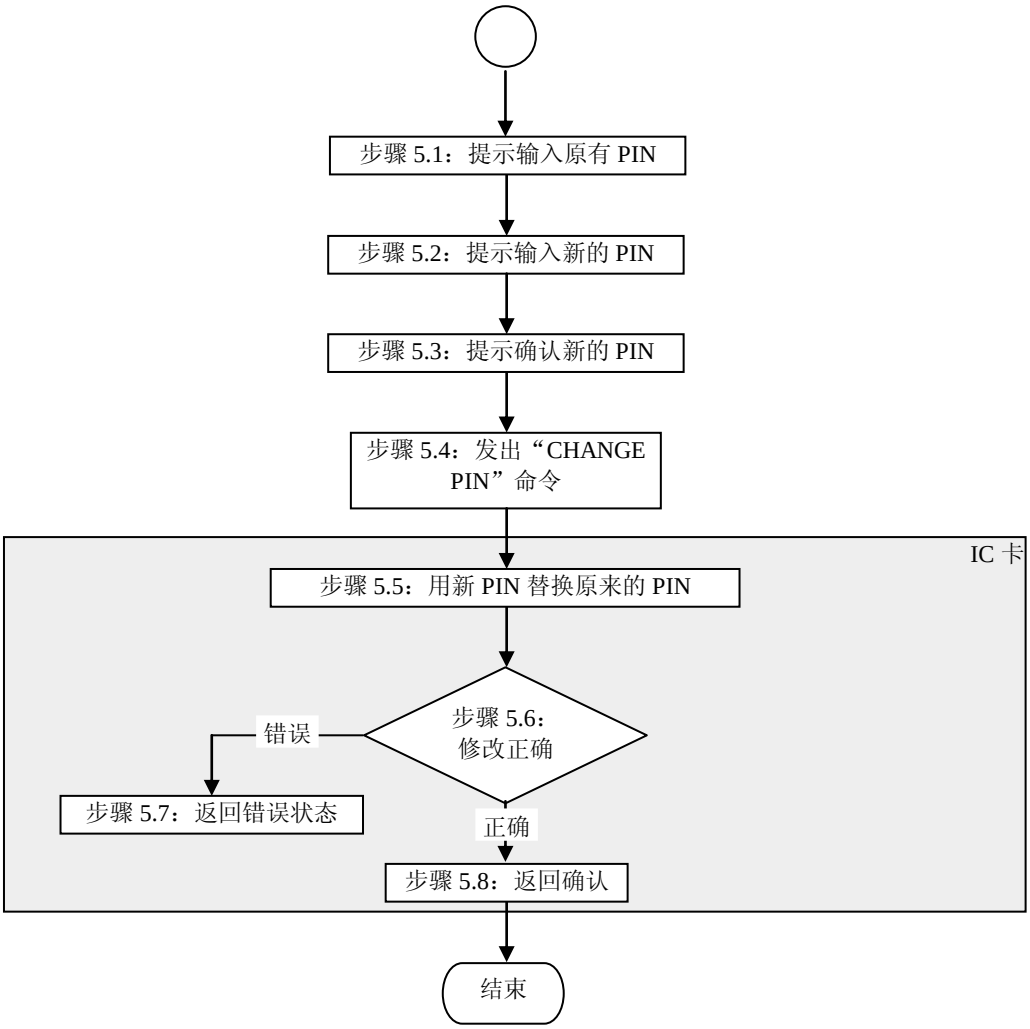

图 5　更改个人密码的处理流程

10　初始化医疗保险支付

在进行医疗保险支付以前，需判断是否符合医疗保险支付条件和医疗保险用卡方式。

8 持卡人联网更新信息中的规定继给出了初始化医疗保险支付的处理流程。

10.1　查询卡中医疗保险基本信息数据（步骤 6.1）

终端按照 6 查询应用信息中规定的处理流程，查询卡中医疗保险基本信息数据。

10.2　判断是否符合医疗保险支付条件（步骤 6.2）

终端根据地方实际政策判断是否符合医疗保险支付条件，条件不满足，则执行步骤 6.4（见 10.4）。

10.3　检查医疗保险用卡方式标志（步骤 6.3）

终端检查医疗保险用卡方式标志，如标志为 1，则执行步骤 6.6（见 10.6）；如标志为 2，则执行步骤 6.5（见 10.5）。

10.4　回送错误状态（步骤 6.4）

条件不满足时终端所做的处理不属于本规范的内容。

10.5　选择医疗保险处理交易类型（步骤 6.5）

在判断卡内医疗保险应用采用脱网处理方式后，选择交易类型。终端应具备让持卡人选择医疗保险处理交易类型的功能，每次交易最多只能选择一种交易类型。持卡人能选择的交易类型有：帐户划入、医疗消费、查询帐户余额、查询交易明细。

10.6　联网更新应用信息（步骤 6.6）

在判断卡内医疗保险应用采用联网处理方式后，按照 8 持卡人联网更新信息中的规定继续执行。

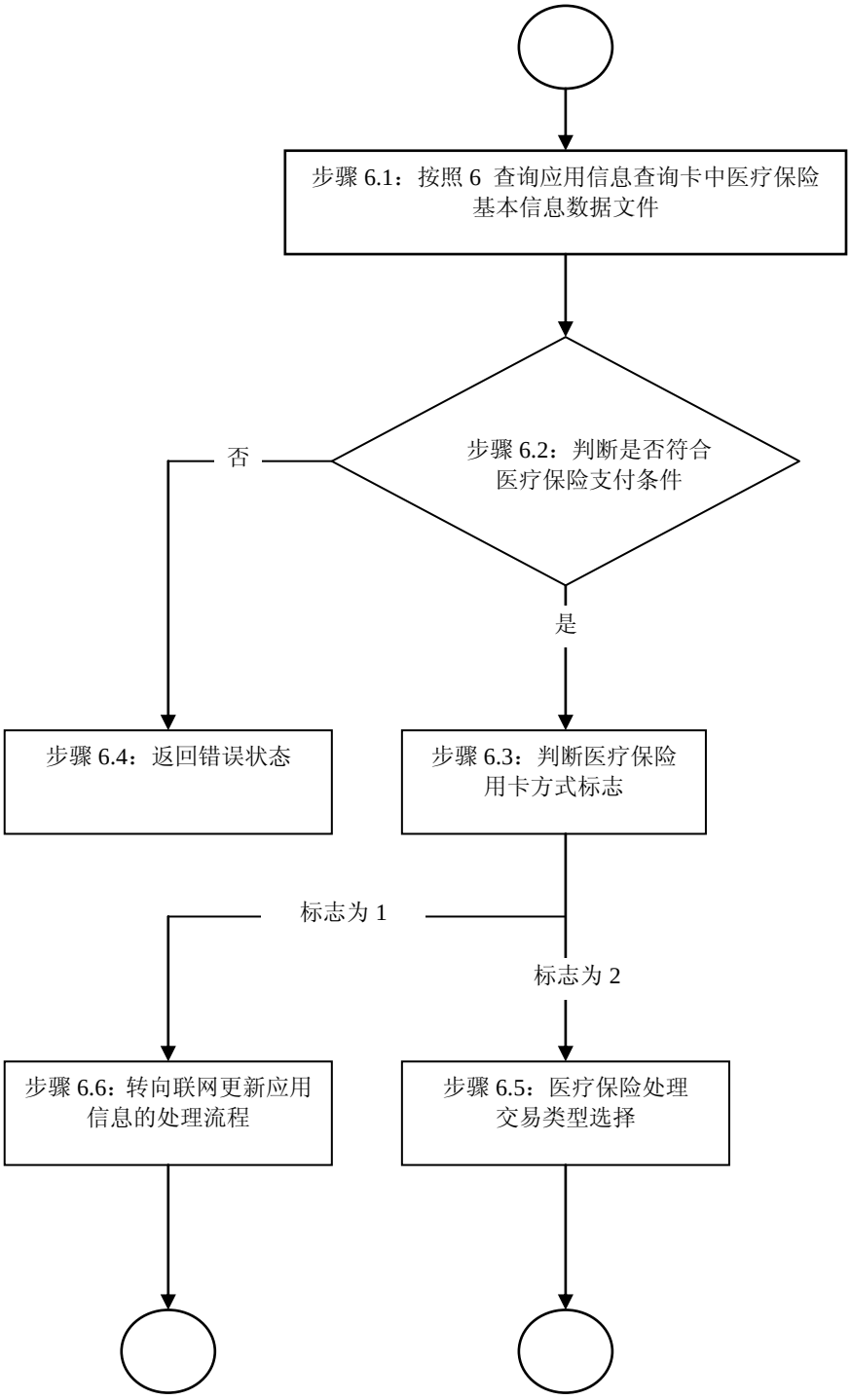

图 6　初始化医疗保险支付的处理流程

11　帐户划入交易

通过帐户划入交易，持卡人可将其在基本医疗保险个人帐户上的资金划入卡内基本医疗保险个人帐户中。这种交易必须在终端上联网进行，并要求提交个人密码（PIN）（如果持卡人设置）。

图 7 给出了帐户划入交易的处理流程。

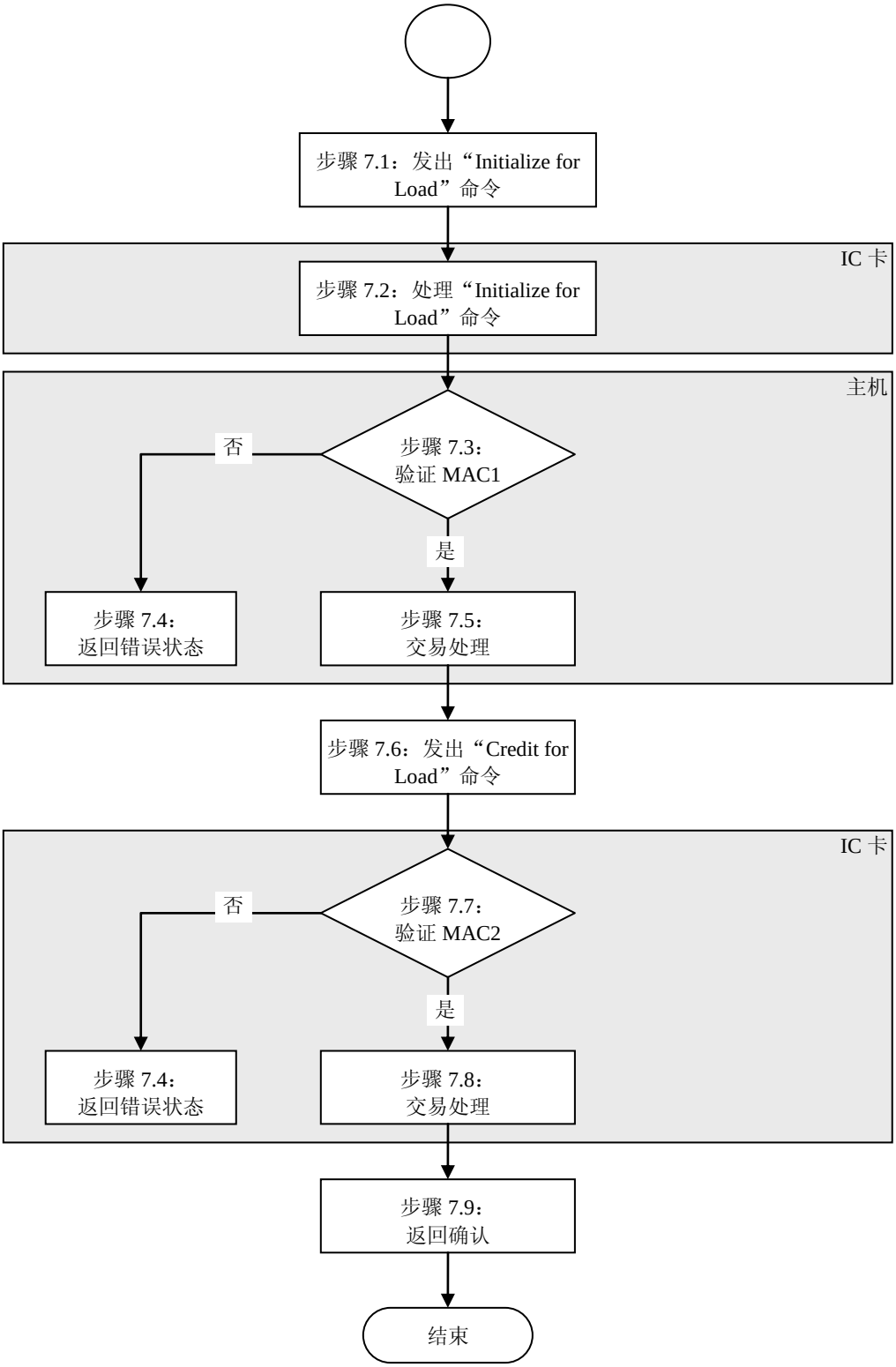

图 7　帐户划入交易的处理流程

11.1　发出“INITIALIZE FOR LOAD”命令（步骤 7.1）

终端应发出“INITIALIZE FOR LOAD“指令启动帐户划入交易。

11.2　处理“INITIALIZE FOR LOAD“命令（步骤 7.2）

收到“INITIALIZE FOR LOAD”命令后，IC 卡将进行以下操作：

——检查是否支持命令中包含的密钥索引号。如果不支持，则回送状态码‘9403’（不支持的密钥索引），但不回送任何其他数据，同时终止命令的处理过程。

——IC 卡产生一个伪随机数$_{(ICC)}$，过程密钥 SESLK 和一个报文鉴别码（MAC1），用来供主机验证帐户划入交易及 IC 卡的合法性。

SESLK 是用于卡内基本医疗保险个人帐户划入交易的过程密钥。该过程密钥是用 DLK 密钥产生的。用来产生过程密钥 SESLK 的输入数据如下：

SESLK：伪随机数$_{(ICC)}$‖基本医疗保险个人帐户划入交易序号‖‘8000’

用 SESLK 对以下数据加密产生 MAC1（按所列顺序）：

- 基本医疗保险个人帐户余额
- 交易金额
- 交易类型
- 终端机编号

IC 卡将把命令 “INITIALIZE FOR LOAD”的响应报文送给终端处理。如果 IC 卡回送的状态码不是‘9000’，则交易终止。

11.3 验证 MAC1（步骤 7.3）

收到“INITIALIZE FOR LOAD”命令响应报文后，终端把响应报文数据传给主机。主机将生成 SESLK 并确认 MAC1 是否有效。如果 MAC1 有效， 交易处理将按步骤 7.5（见 11.5）中的描述继续执行。否则，交易处理将执行步骤 7.4（见 11.4）。

11.4 回送错误状态（步骤 7.4）

如果不接受帐户划入交易，则主机应通知终端。回送给终端的报文格式和内容，以及终端所做的处理不在本规范范围之内。

11.5 交易处理（步骤 7.5）

在确认能够进行帐户划入交易后，主机从持卡人基本医疗保险个人帐户中扣减帐户划入金额。

主机产生一个报文鉴别码（MAC2），用于 IC 卡对主机进行合法性检查。用 SESLK 对以下数据加密产生 MAC2（按所列顺序）：

- 交易金额
- 交易类型
- 终端机编号
- 交易时间（主机）

成功地进行了帐户划入交易后，主机将基本医疗保险个人帐户划入交易序号加 1，并向终端发送一个帐户划入交易接受报文，其中包括 MAC2 和交易时间（主机）。

11.6 发出“CREDIT FOR LOAD”命令（步骤 7.6）

终端收到主机发来的帐户划入交易接受报文后，发出“CREDIT FOR LOAD”命令更新卡内基本医疗保险个人帐户。

11.7 验证 MAC2（步骤 7.7）

收到“CREDIT FOR LOAD”命令后，IC 卡必须确认 MAC2 的有效性。如果 MAC2 有效，交易处理将执行步骤 7.8（见 11.8）。否则将向终端回送状态码‘9302’（MAC 无效）。终

端对错误所应采取的措施不在本规范范围之内。

11.8 交易处理（步骤 7.8）

IC 卡将基本医疗保险个人帐户划入交易序号加 1，并且把交易金额累加到基本医疗保险个人帐户余额上。IC 卡必须成功地完成以上所有操作或者一个也不完成。

在基本医疗保险个人帐户划入交易中，IC 卡用以下数据组成的一个记录更新交易明细：

- 基本医疗保险个人帐户划入交易序号
- 交易类型
- 终端机编号
- 交易时间（主机）
- 交易金额

TAC 的计算不采用过程密钥方式，它用 DTK 直接对以下数据进行加密运算来产生（按所列顺序）：

- 基本医疗保险个人帐户余额
- 基本医疗保险个人帐户划入交易序号（加 1 前）
- 交易金额
- 交易类型
- 终端机编号
- 交易时间（主机）

11.9 返回确认（步骤 7.9）

在成功完成步骤 7.8 后，IC 卡通过“CREDIT FOR LOAD”命令的响应报文将 TAC 回送给终端。主机可以不马上验证 TAC。

12 医疗消费交易

医疗消费交易允许持卡人使用卡内基本医疗保险个人帐户进行医疗消费，并记录个人自付和统筹基金支付累计金额。此交易可以在医疗机构终端（POS）上脱网进行。使用卡内基本医疗保险个人帐户进行的医疗消费交易必须提交个人密码（PIN）（如果持卡人设置）。

本规范对该项应用提供两种方式供选择：或者选择仅支持个人帐户处理模式，或者选择个人帐户、个人自付、统筹基金支付三种医疗消费同时存在的处理模式。

当交易明细文件的记录长度为 20 字节时，表示仅支持个人帐户处理模式，命令报文和响应报文中的“个人自付金额”、“统筹基金支付金额”、“支付年度”和“年度起始日期”数据项无意义，建议补十六进制‘0’。否则表示支持个人帐户、个人自付、统筹基金支付三种医疗消费同时存在的处理模式。图 8 给出了医疗消费交易的处理流程。

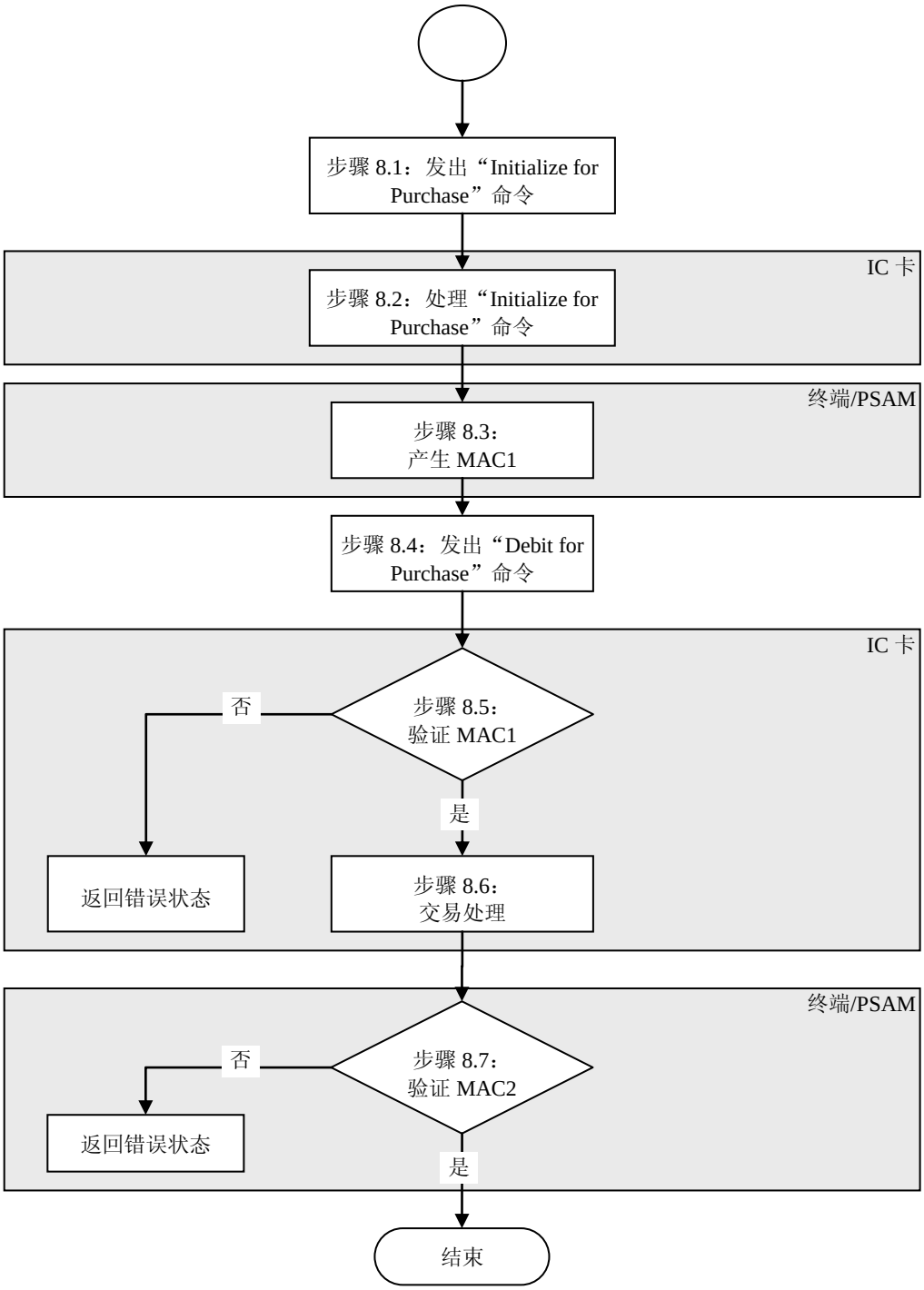

图 8　医疗消费交易的处理流程

12.1　发出“INITIALIZE FOR PURCHASE”命令（步骤 8.1）

终端发出“INITIALIZE FOR PURCHASE”命令启动医疗消费交易。

12.2　处理“INITIALIZE FOR PURCHASE”命令（步骤 8.2）

IC 卡收到“INITIALIZE FOR PURCHASE”命令后，将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态码‘9403’（不支持的密钥索引），但不回送其他数据。

——若为帐户支付，检查卡内基本医疗保险个人帐户余额是否大于或等于个人帐户交易

金额。如果小于个人帐户交易金额，IC 卡回送状态码‘9401’（资金不足），但不回送其他数据。对以上错误终端采取的措施不在本规范范围之内。

在通过以上检查之后，IC 卡将产生一个伪随机数$_{(ICC)}$和过程密钥。过程密钥是利用 DPK 产生的。用于产生该过程密钥的输入数据如下：

SESPK：伪随机数$_{(ICC)}$ ‖ 医疗消费交易序号 ‖ 终端交易序号的最右两个字节

12.3 产生 MAC1（步骤 8.3）

使用伪随机数$_{(ICC)}$和 IC 卡回送的医疗消费交易序号，终端的安全存取模块（PSAM）将产生一个过程密钥（SESPK）和一个报文鉴别码（MAC1），供 IC 卡来验证 PSAM 的合法性。

用 SESPK 对以下数据进行加密产生 MAC1（按所列顺序）：

- 个人帐户交易金额
- 个人自付金额
- 统筹基金支付金额
- 交易类型
- 终端机编号
- 交易时间（终端）

12.4 发出“DEBIT FOR PURCHASE”命令（步骤 8.4）

终端发出“DEBIT FOR PURCHASE”命令。

12.5 验证 MAC1（步骤 8.5）

在收到“DEBIT FOR PURCHASE”命令后，IC 卡将验证 MAC1 的有效性。如果 MAC1 有效，交易处理将继续执行步骤 8.6（见 12.6）。否则将向终端回送错误状态码‘9302’（MAC 无效）。终端对错误状态的处理不在本规范范围之内。

12.6 交易处理（步骤 8.6）

IC 卡从基本医疗保险个人帐户余额中扣减帐户支付的金额；并累计个人自付金额、统筹基金支付金额。在做累计前，IC 卡先根据交易日期与卡内“支付年度”、“年度起始日期”进行判断，方法如下：

计算 n = 当前交易日期（yyyymmdd）-（支付年度（yyyy）×10000+年度起始日期）；

如果 n<10000，则实际交易时间正处于卡内记载的结算年度内，IC 卡在“年度个人自付累计金额”和“年度统筹基金支付累计金额”上分别累加上本次个人自付和统筹基金支付的金额；

否则，IC 卡改写“支付年度”为实际结算年度，并将“年度个人自付累计金额”改为本次个人自付金额，将“年度统筹基金支付累计金额”改为本次统筹基金支付金额；

然后将医疗消费交易序号加 1，并继续更新交易明细。

IC 卡必须成功地完成以上所有步骤或者一个也不完成。只有金额或序号的更新均成功后，交易明细才可更新。

IC 卡产生一个报文鉴别码（MAC2）供 PSAM 对 IC 卡进行合法性检查。IC 卡将通过“DEBIT FOR PURCHASE”命令响应报文回送以下数据给 PSAM，作为产生 MAC2 的输入数据，用 SESPK 对以下数据加密产生 MAC2：

- 个人帐户交易金额

- 个人自付金额
- 统筹基金支付金额

TAC 不采用过程密钥方式而是直接用密钥 DTK 来产生。TAC 将被写入终端交易明细，以便后来传给主机进行交易验证。下面是用来生成 TAC 的数据，它们以明文形式通过“DEBIT FOR PURCHASE”命令的响应报文从 IC 卡送到终端：

- 个人帐户交易金额
- 个人自付金额
- 统筹基金支付金额
- 交易类型
- 终端机编号
- 终端交易序号
- 交易时间（终端）

对医疗消费交易，IC 卡将用以下数据组成的一个记录更新交易明细：

- 医疗消费交易序号
- 交易类型
- 终端机编号
- 交易时间（终端）
- 个人帐户交易金额
- 个人自付金额
- 统筹基金支付金额

12.7 验证 MAC2（步骤 8.7）

在收到从 IC 卡（经过终端）传来的 MAC2 后，PSAM 要验证 MAC2 的有效性。MAC2 验证的结果被传送到终端以便采取必要的措施。终端采取的措施不在本规范范围之内。

13 应用维护功能

应用维护包括卡片锁定、应用锁定、PIN 修改/解锁。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：

——通过外部认证（过程见 0~0），满足操作的安全状态；

——终端向卡申请一随机数 $_{(ICC)}$；

——发送相应的应用维护命令，卡在收到命令后执行以下操作：

- 使用前一步骤产生的随机数 $_{(ICC)}$，利用《社会保障（个人）卡规范》第 4 部分：安全机制中描述的方式产生过程密钥；
- 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。

13.1 卡片锁定

终端应发出“CARD BLOCK”命令来锁定卡片。

命令的成功执行将使 IC 卡中的所有应用无效。在这种情况下，进行应用选择将会回送状态码‘6A81’（功能不被支持）。

外部认证和 MAC 认证失败并不导致相应密钥锁定。

13.2 应用锁定

终端应发出“APPLICATION BLOCK”命令来锁定应用。

该命令的用法和作用由发卡方和应用提供方商议决定。

该命令的成功执行将导致 IC 卡中特定的应用无效。在这种状态下：

——选择此应用时，对“SELECT”命令 IC 卡回送状态码‘9303’（ 应用被永久锁定）。

——在应用被选择后，除用“SELECT”命令选择其他应用外，IC 卡对其他命令只回送状态码‘9303’（ 应用被永久锁定）。

外部认证和 MAC 认证失败并不导致相应密钥锁定。

13.3 PIN 修改/解锁

终端应发出“PIN CHANGE/UNBLOCK”命令对 PIN 解锁。

如果 PIN 连续数次（具体次数由发卡方自行决定）解锁失败，则解锁密钥被锁定。

14 防拔

卡片必须能够在交易处理中的任何情况下，甚至是在更新 EEPROM 过程中掉电的情况下，保持数据的完整性。这就需要在每次更新数据前对数据进行备份，并且在重新加电后自动地触发恢复机制。这种恢复机制不应要求终端通过向 IC 卡发出命令报文来实现，而且一旦 IC 卡确认更新数据已完成，则备份数据必须被丢弃。

在终端还未收到所发出命令的响应之前，卡片被突然拔出后，终端应提醒持卡人重新插入卡片。之后终端将检查卡的识别码和卡号来确认插入的卡片和前面拔出的卡片是否同一张卡。如果是同一张卡，终端应通过执行“查询应用数据”（见 6）的交易获取相关的应用信息，然后通过比较数据内容来判断数据更改是否完成。

在终端发给 IC 卡一个命令以更新卡内基本医疗保险个人帐户（帐户划入或医疗消费）、个人自付金额、统筹基金支付金额时，卡片总会回送一个 MAC 或/和 TAC，以证明更新已经发生。

IC 卡必须在更新金额前计算 MAC 或/和 TAC，一旦金额更新成功，必须保证可以通过“GET TRANSACTION PROOF”命令获得此 MAC 或/和 TAC。如果防拔恢复已使金额恢复到更新前的数值，那么有关的加密数据不必再保留。接到更改 CIA、SPIP、SPFP 的命令，如“DEBIT FOR PURCHASE”，“CREDIT FOR LOAD”命令时，这些加密数据可能被丢弃。

如果在命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。这种情况，终端应负责用“GET TRANSACTION PROOF”命令进行恢复。

如果卡片正在处理时被突然拔出，终端应提醒持卡人重新插入卡片。之后终端将检查发卡方标识和应用标识号以确认插入的卡片是否是同一张卡，如果是同一张卡，终端发出“GET TRANSACTION PROOF”命令。如果 MAC 或/和 TAC 返回，终端即完成交易处理；如果 MAC 或/和 TAC 无法回送，则说明 IC 卡中的金额没有被修改。交易可以用适当的初始化命令重新开始。

15 TAC 的计算

TAC 的计算参照《社会保障（个人）卡规范》第 4 部分：安全机制，数据块的产生方法同 MAC 计算中数据块的产生方法，TAC 的算法同 MAC 算法。对于 8 字节分组密码算法，过程密钥由 DTK 密钥的左右 8 字节进行异或运算产生；对于 16 字节分组密码算法，过程密钥直接采用 DTK 密钥。