人社信息函〔2012〕38号

关于印发社会保障卡医保结算交易流程的通知

各省、自治区、直辖市及新疆生产建设兵团人力资源社会保障厅（局）:

为推动和规范社会保障卡的应用，实现“新医改”提出的参保人员就医“一卡通”目标，我们制定了《社会保障卡医保结算交易流程》，现印发给你们，请遵照执行。

二〇一二年五月二十八日

主题词：社会保障卡△ 医疗保险 通知

社会保障卡医保结算交易流程

本流程对社会保障卡医保结算交易的流程进行规定。

本流程中所涉及的卡内数据结构，见《社会保障卡文件结构和数据项（V2.0）》（人社信息函〔2012〕37 号）；所涉及的社会保障卡命令，见《社会保障（个人）卡规范》（LB002-2000）第一部分 IC 卡规范和第二部分应用规范的有关定义。

1　社会保障卡医保结算交易模式

社会保障卡医保结算交易有三种可供选择的模式：

模式 1：联网交易模式

模式 2：联网且支持临时脱网的交易模式

模式 3：脱网交易模式

用卡地区可选择且仅可以选择上述三种模式之一，作为本地社会保障卡医保结算交易模式。

选用联网交易模式（模式 1）时，执行本流程第 2 部分“联网医保结算交易流程”。

选用联网且支持临时脱网的交易模式（模式 2）时，执行本流程第 3 部分“支持临时脱网结算的联网医保结算交易流程”和第 4 部分“联网模式下的临时脱网医保结算交易流程”。

选用脱网交易模式（模式 3）时，按照《社会保障（个人）卡规范》（LB002-2000）第二部分关于医保结算脱网交易模式的规定执行，本流程不再重述。

2　联网医保结算交易流程

联网医保结算交易记录持卡人进行医保结算时的交易明细，包括但不限于医保个人账户结算、各险种的住院基金结算、门诊统筹结算、门诊病种统筹结算等，并提供交易 TAC 供后台进行认证清算。此交易必须提交个人密码（PIN）（如果持卡人设置）。

当进行联网医保结算交易时，命令报文、响应报文和交易明细文件中的“个人账户交易金额”为“0”，“个人自付金额”为本次结算的总金额，“统筹基金支付金额”为本次结算个人账户交易金额+统筹基金支付金额。图 1 给出了联网医保结算交易的处理流程。

2.1　读取卡内个人信息（步骤 2.1）

终端发出“READ RECORD”命令读取 IC 卡内的社会保障号码、姓名、社会保障卡卡号、结算险种参保地等个人信息。

2.2　后台预结算（步骤 2.2）

终端将读出的个人信息发送至后台进行预结算。预结算过程包括个人参保判断、个人账户交易金额、个人自费金额、统筹基金支付金额的计算等，具体过程不在本流程描述范围内。

预结算过程结束后后台将结果返回终端，预结算成功时继续步骤 2.3，预结算失败时本次交易失败退出。

2.3　发出“INITIALIZE FOR PURCHASE”命令（步骤 2.3）

终端发出“INITIALIZE FOR PURCHASE”命令启动医保结算交易，命令数据中的“个人账户交易金额”为“0”，“个人自付金额”为本次结算的总金额，“统筹基金支付金额”为

本次结算个人账户交易金额+统筹基金支付金额。

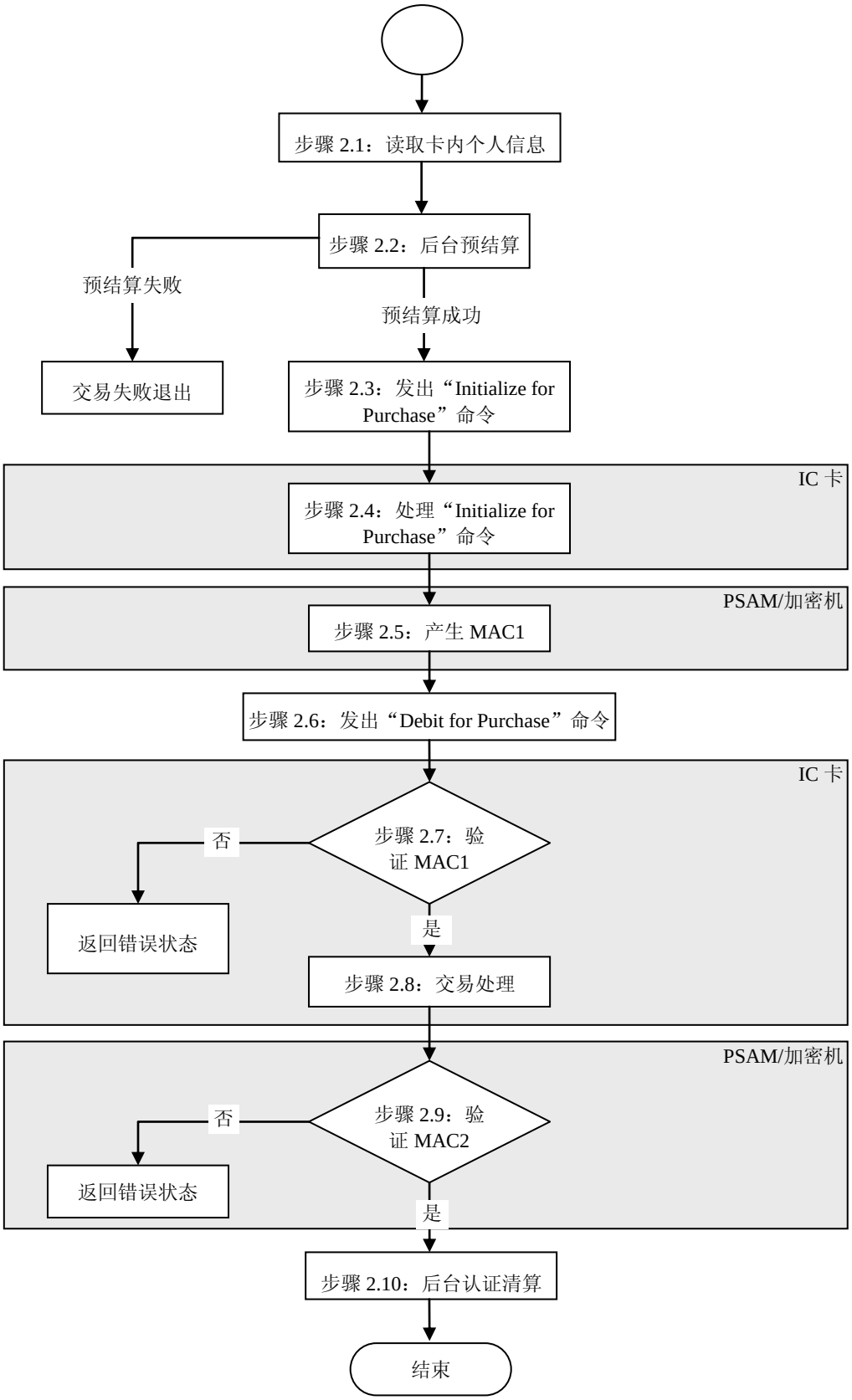

图 1　联网医保结算交易的处理流程

2.4　处理“INITIALIZE FOR PURCHASE”命令（步骤 2.4）

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。对以上错误终端采取的措施不在本流程范围之内。

在通过上述检查之后，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） ‖ 交易序号 ‖ 终端交易序号的最右两个字节

2.5 产生 MAC1（步骤 2.5）

使用伪随机数（ICC）和 IC 卡回送的交易序号，终端通过安全存取模块（PSAM）或加密机产生一个过程密钥（SESPK）计算出一个报文鉴别码（MAC1），供 IC 卡来验证终端的合法性。

用 SESPK 对以下数据进行加密产生 MAC1（按所列顺序）：

- 零金额
- 本次交易总金额
- 个人账户交易金额+统筹基金支付金额
- 交易类型
- 终端机编号
- 交易时间（终端）

2.6 发出“DEBIT FOR PURCHASE”命令（步骤 2.6）

终端发出“DEBIT FOR PURCHASE”命令。

2.7 验证 MAC1（步骤 2.7）

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 2.8。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流程范围之内。

2.8 交易处理（步骤 2.8）

IC 卡累计年度内的个人自付金额（实为本次交易金额）、统筹基金支付金额（实为个人账户交易金额+统筹基金支付金额）。

然后将交易序号加 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）供终端对 IC 卡进行合法性检查。用 SESPK 对以下数据加密产生 MAC2：

- 零金额
- 本次交易总金额
- 个人账户交易金额+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。MAC2 和 TAC 以明文形式通过“DEBIT FOR PURCHASE”命令的响应报文从 IC 卡送到终端。下面是用来生成 TAC 的数据：

- 零金额

- 本次交易总金额
- 个人账户交易金额+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）

对医保结算交易，IC 卡将用以下数据组成的一个记录更新交易明细文件（DF04 EF08）：

- 交易序号
- 交易类型
- 终端机编号
- 交易时间（终端）
- 零金额
- 本次交易总金额
- 个人账户交易金额+统筹基金支付金额

若该次结算属工伤医疗、生育医疗和医疗救助范围，同时更新特殊医疗结算记录文件（DF04 EF15）

2.9 验证 MAC2（步骤 2.9）

终端将收到的 MAC2 传送给 PSAM 卡或加密机，PSAM 卡或加密机要验证 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流程范围之内。

2.10 后台认证清算（步骤 2.10）

终端将收到的 TAC 传送给后台，后台对 TAC 进行认证（该认证可实时进行也可事后进行），若认证成功则后台执行交易清算过程并将成功结果返回给终端，若认证不成功则后台将失败结果返回给终端。

3 支持临时脱网结算的联网医保结算交易流程

支持临时脱网结算的联网医保结算交易，正常情况下采用联网交易，当网络出现故障时，可在获得许可的终端临时采用脱网交易。临时脱网交易时各地区可自行定义一个固定的脱网医保结算金额上限和脱网医保结算次数上限，脱网医保结算累计金额和脱网医保结算累计次数均在上限范围内时才可进行临时脱网结算交易。

临时脱网交易仅限本地区的社会保障卡，外地区的社会保障卡不能进行临时脱网交易。

支持临时脱网结算的联网交易记录持卡人进行医保结算时的交易明细，包括但不限于医保个人账户结算、各险种的住院基金结算、门诊统筹结算、门诊病种统筹结算等，并提供交易 TAC 供后台进行认证清算，并且都必须提交个人密码（PIN）（如果持卡人设置）。

图 2 给出了支持临时脱网结算的联网医保结算交易处理流程。

3.1 读取卡内个人信息和脱网交易信息（步骤 3.1）

终端发出“READ RECORD”命令读取 IC 卡内的社会保障号码、姓名、社会保障卡卡号、结算险种参保地等个人信息，同时读取脱网医保结算累计金额等临时脱网交易信息。

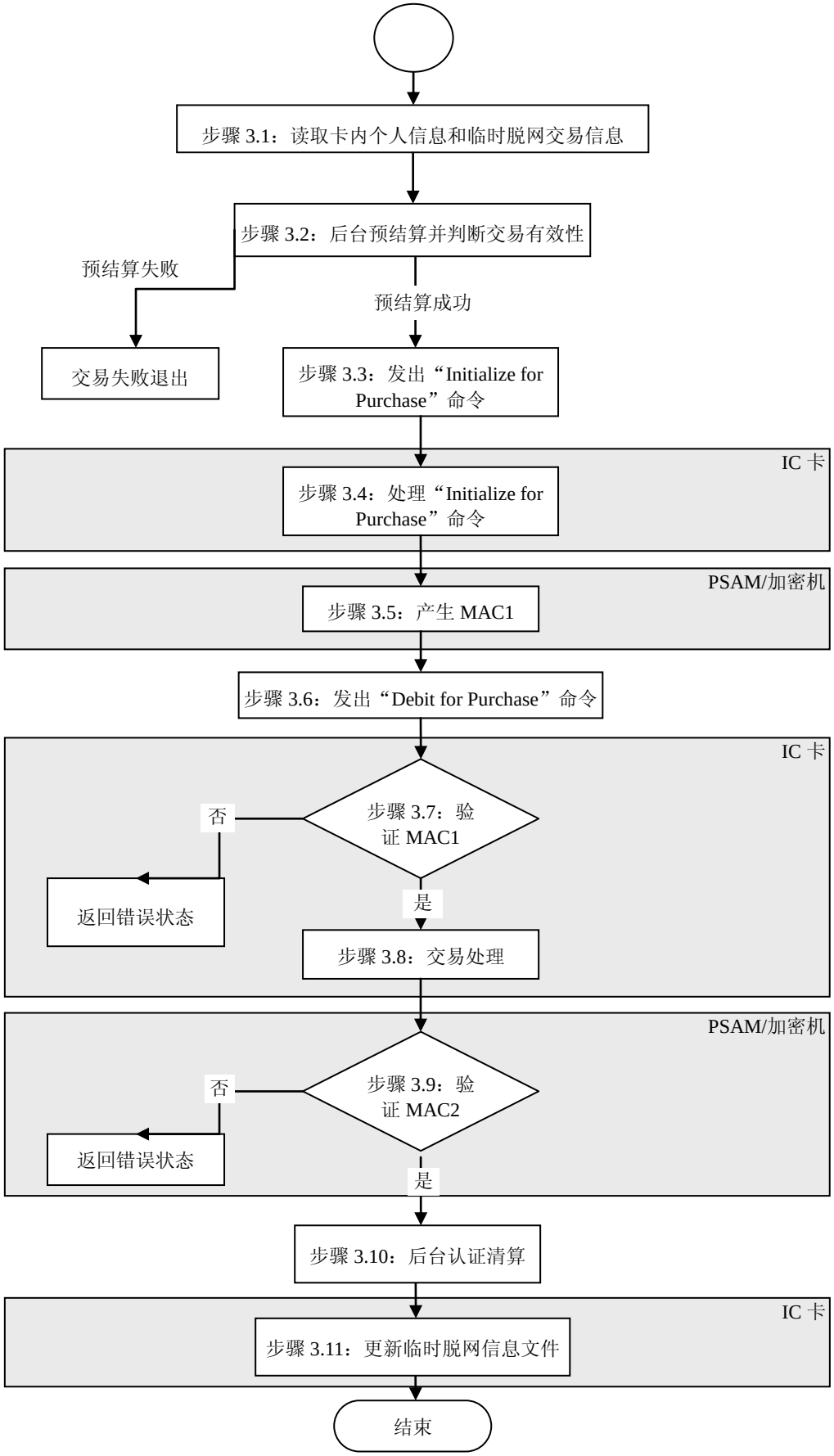

图 2　支持临时脱网结算的联网医保结算交易处理流程

3.2　终端预结算并判断交易有效性（步骤 3.2）

终端将读出的个人信息和临时脱网交易信息发送至后台。

后台首先进行预结算，预结算过程包括个人参保判断、个人账户交易金额、个人自费金额、统筹基金支付金额的计算等。

预结算失败时本次交易失败退出。

预结算成功后进行本次交易有效性判断，后台根据本次个人账户交易金额、卡内脱网医保结算累计金额、脱网医保结算累计次数、个人账户余额等判断本次联网交易是否可以进行，并将判断结果返回给终端。

3.3　发出“INITIALIZE FOR PURCHASE”命令（步骤 3.3）

终端收到本次交易有效返回时，发出“INITIALIZE FOR PURCHASE”命令启动医保结算交易，命令数据中的“个人账户交易金额”为“0”，“个人自付金额”为本次结算的总金额，“统筹基金支付金额”为个人账户交易金额+统筹基金支付金额。

终端收到本次交易无效时，本次交易失败结束。

3.4　处理“INITIALIZE FOR PURCHASE”命令（步骤 3.4）

同 2.4。

3.5　产生 MAC1（步骤 3.5）

同 2.5。

3.6　发出“DEBIT FOR PURCHASE”命令（步骤 3.6）

同 2.6。

3.7　验证 MAC1（步骤 3.7）

同 2.7。

3.8　交易处理（步骤 3.8）

同 2.8。

3.9　验证 MAC2（步骤 3.9）

同 2.9。

3.10　后台认证清算（步骤 3.10）

终端将收到的 TAC 传送给后台，后台对 TAC 进行认证，若认证成功则后台执行交易清算过程。同时判断并生成准许脱网医保结算标识、脱网医保结算累计金额、脱网医保结算累计次数，将结果返回给终端，若认证不成功则后台将失败结果返回给终端。

3.11　更新医疗保险临时脱网结算信息文件

终端使用后台返回的准许脱网医保结算标识、脱网医保结算累计金额、脱网医保结算累计次数更新 IC 卡的医疗保险临时脱网结算信息文件。

4　联网模式下的临时脱网医保结算交易流程

联网模式下的临时脱网医保结算交易仅限于医保个人账户结算，并提供交易 TAC 供后台进行认证清算，并且都必须提交个人密码（PIN）（如果持卡人设置）。

图 3 给出了联网模式下的临时脱网医保结算交易处理流程。

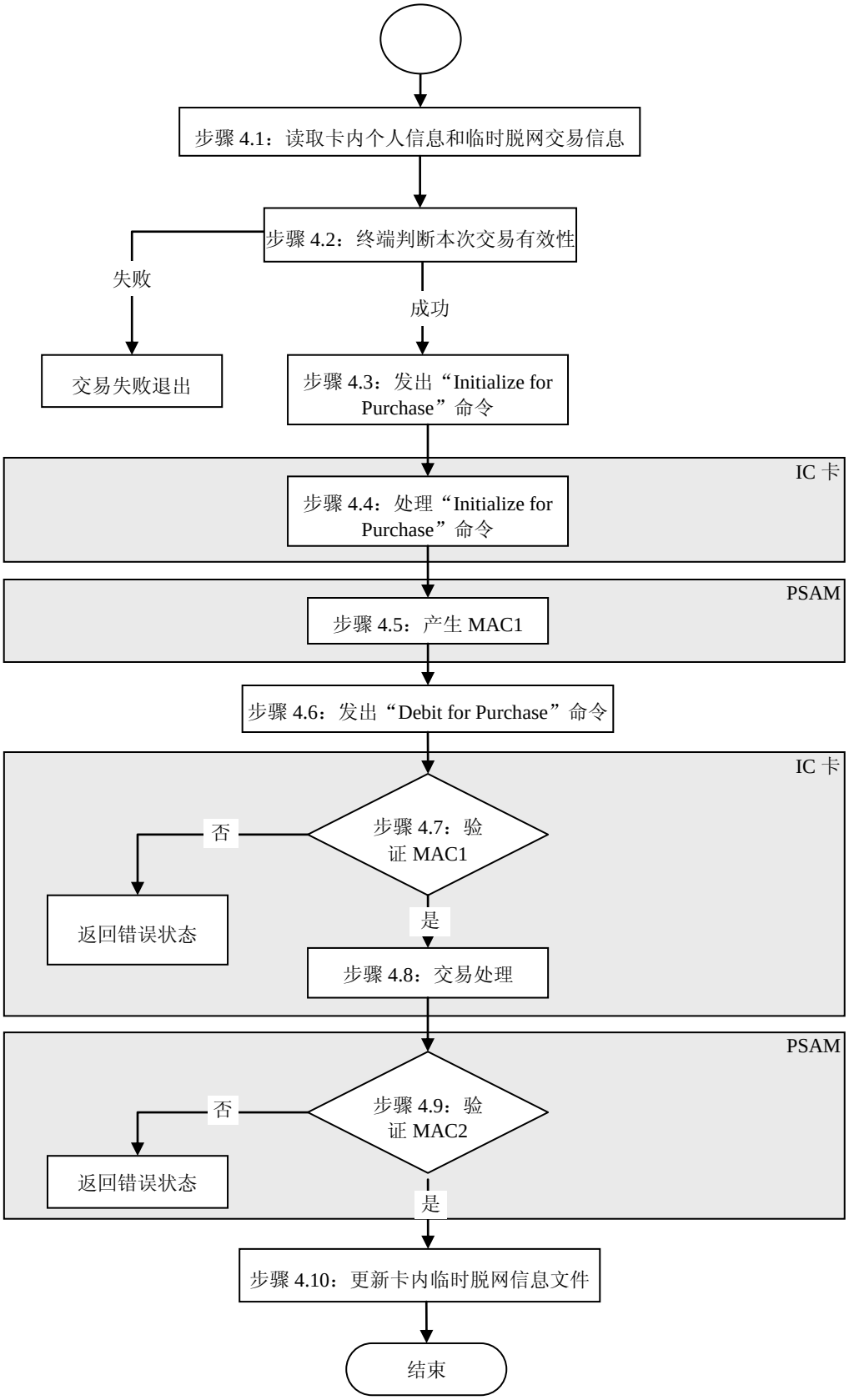

图 3　联网模式下的临时脱网医保结算交易处理流程

4.1　读取卡内个人信息（步骤 4.1）

终端发出“READ RECORD”命令读取 IC 卡内的社会保障号码、姓名、社会保障卡卡号、结算险种参保地等个人信息，同时读出准许脱网医保结算标识、脱网医保结算累计金额、脱网医保结算累计次数等临时脱网交易信息。

4.2　终端判断本次交易有效性（步骤 4.2）

终端根据准许脱网医保结算标识、脱网医保结算累计金额、脱网医保结算累计次数进行交易有效性判断。若准许脱网医保结算标识为 1，并且脱网医保结算累计金额+本次结算金额小于本地区脱网医保结算金额上限，并且脱网医保结算累计次数+1 小于本地区脱网医保结算次数上限，则本次脱网交易可以进行，执行步骤 2.3。否则本次脱网交易终止。

4.3　发出“INITIALIZE FOR PURCHASE”命令（步骤 4.3）

终端发出“INITIALIZE FOR PURCHASE”命令启动医保结算交易，命令数据中的“个人账户交易金额”为“0”，“个人自付金额”为本次结算的总金额，“统筹基金支付金额”为个人账户交易金额+统筹基金支付金额即为本次结算的总金额。

4.4　处理“INITIALIZE FOR PURCHASE”命令（步骤 4.4）

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。对以上错误终端采取的措施不在本流程范围之内。

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） ‖ 交易序号 ‖ 终端交易序号的最右两个字节

4.5　产生 MAC1（步骤 4.5）

使用伪随机数（ICC）和 IC 卡回送的交易序号，终端通过安全存取模块（PSAM）产生一个过程密钥（SESPK）计算出一个报文鉴别码（MAC1），供 IC 卡来验证终端的合法性。

用 SESPK 对以下数据进行加密产生 MAC1（按所列顺序）：

- 零金额
- 本次交易总金额
- 个人账户交易金额+统筹基金支付金额
- 交易类型
- 终端机编号
- 交易时间（终端）

4.6　发出“DEBIT FOR PURCHASE”命令（步骤 4.6）

终端发出“DEBIT FOR PURCHASE”命令。

4.7　验证 MAC1（步骤 4.7）

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 4.8。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流程范围之内。

4.8　交易处理（步骤 4.8）

IC 卡累计年度内的个人自付金额（实为本次交易金额）、统筹基金支付金额（实为本次交易总金额）。

然后将交易序号加 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）供终端对 IC 卡进行合法性检查。用 SESPK 对以下数据加密产生 MAC2：

- 零金额
- 本次交易总金额
- 个人账户交易金额+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。MAC2 和 TAC 以明文形式通过“DEBIT FOR PURCHASE”命令的响应报文从 IC 卡送到终端。下面是用来生成 TAC 的数据：

- 零金额
- 本次交易总金额
- 个人账户交易金额+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）

对医保结算交易，IC 卡将用以下数据组成的一个记录更新交易明细追加到 DF04 EF08 文件中：

- 交易序号
- 交易类型
- 终端机编号
- 交易时间（终端）
- 零金额
- 本次交易总金额
- 个人账户交易金额+统筹基金支付金额

若该次结算属工伤医疗、生育医疗和医疗救助范围，同时更新特殊医疗结算记录文件（DF04 EF15）

4.9 验证 MAC2（步骤 4.9）

终端将收到的 MAC2 传送给 PSAM 卡，PSAM 卡要验证 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流程范围之内。

4.10 更新卡内医疗保险临时脱网结算信息文件（步骤 4.10）

终端使用脱网医保结算累计金额+本次结算总金额更新卡内医疗保险临时脱网结算信息文件中的脱网医保结算累计金额数据项，使用脱网医保结算累计次数+1 更新医疗保险临时脱网结算信息文件中的脱网医保结算累计次数数据项。同时将个人信息、TAC 和生成 TAC 的数据保存，待能联网时上传给后台，后台根据这些信息进行 TAC 的验证并进行清算。