



(12)发明专利

(10)授权公告号 CN 102622642 B

(45)授权公告日 2017.08.01

(21)申请号 201110126993.3

(51)Int.Cl.

(22)申请日 2011.05.06

G06K 19/077(2006.01)

(65)同一申请的已公布的文献号

G06K 19/10(2006.01)

申请公布号 CN 102622642 A

G06Q 40/00(2012.01)

(43)申请公布日 2012.08.01

(56)对比文件

(30)优先权数据

CN 101258507 A, 2008.09.03,

13/019, 180 2011.02.01 US

US 7469339 B2, 2008.12.23,

(73)专利权人 金士顿数位股份有限公司

US 7469339 B2, 2008.12.23,

地址 美国加利福尼亚州

US 2008229105 A1, 2008.09.18,

(72)发明人 B·W·陈

CN 101258507 A, 2008.09.03,

(74)专利代理机构 上海专利商标事务所有限公司 31100

审查员 胡丽丽

代理人 郭蔚

权利要求书1页 说明书9页 附图15页

(54)发明名称

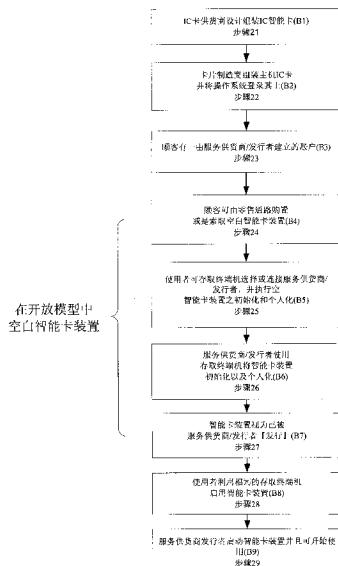
以及解密该发行者和该智能卡装置间的数据传输。

空白智能卡发行系统

(57)摘要

本发明揭露一种空白智能卡发行系统和方法。一方面而言，揭露一种发行智能卡装置(smart card device; SC)的方法和系统。该方法及系统包含由制造商提供智能卡装置的一初始阶段以及一身份验证阶段。该方法及系统亦包含发放智能卡装置，并于该智能卡装置发放后，由一发行者提供一第一次身份验证阶段给一特定使用者，且发行者开始给予特定顾客一智能卡装置的第一登录流程。该方法及系统更包含在该第一次身份验证阶段后，由该发行者提供该智能卡装置的另一身份验证阶段。因此，当该智能卡装置与该发行者两者互相验证身份后，该特定使用者及该发行者可完成登录流程。另一方面，本发明揭露了一种发行者利用智能卡装置数据传输的流程及系统。该流程及系统提供使用者登录一智能卡装置，且执行该智能卡装置与该发行者的互相身份验证。该流程与系统进一步包含在该互相身份验证后，建立一金钥，该金钥系作为加密

CN 102622642 B



1. 一种用来允许于一开放模式中发行一智能卡装置的系统,该智能卡装置包含一快闪储存装置及埋设于该快闪储存装置中的一智能卡集成电路,该系统包含:

一制造商的装置,用以提供该智能卡装置的一初始阶段以及提供该智能卡装置的一身份验证阶段;

一发行者的服务器,用以在发放该智能卡装置给一特定使用者后,经由一第一次身份验证阶段验证该智能卡装置,且该发行者的服务器用以经由一第一登录阶段来登录该智能卡装置,

其中一互相验证身份的发生包含该发行者的服务器经由第二次身份验证阶段对该智能卡装置的验证、及该智能卡装置对该发行者的服务器的验证,

其中该发行者的服务器用以经由第二登录阶段来为该特定使用者完成该智能卡装置的登录;以及

一远程存取终端机,其中在该特定使用者经由一零售通路购买该智能卡装置后,该特定使用者经由该远程存取终端机使用一登入阶段来初始化以及个人化该智能卡装置,以提供一个人化智能卡装置,其中该登入阶段连接至该发行者的服务器,以使该发行者的服务器提供该第一登录阶段及该第二登录阶段。

2. 根据权利要求1所述的系统,其特征在于,该智能卡装置系为该从零售通路购置的一空白装置。

3. 根据权利要求1所述的系统,其特征在于,该智能卡装置具有一与内容/服务供应者相关联的一账户,且该智能卡装置可被该内容/服务供应者发行。

4. 一种发行智能卡装置的方法,该方法包含:

由一制造商提供该智能卡装置的一初始阶段;

由该制造商提供该智能卡装置的一身份验证阶段;

发放该智能卡装置;以及

在发放该智能卡装置后,一特定使用者经由一存取终端机使用一登入阶段来远程地初始化以及个人化该智能卡装置,其中该登入阶段连接至一发行者的一服务器,其中该初始化以及个人化该智能卡装置包含:

由该发行者提供一第一次身份验证阶段给该特定使用者;

由该发行者来替该特定使用者启用该智能卡装置的一第一登录阶段;

在该第一次身份验证阶段后,由该发行者提供该智能卡装置的第二次身份验证阶段;以及

由该智能卡装置提供该发行者的一身份验证,其中当该智能卡装置与该发行者两者互相验证身份后,该特定使用者及该发行者可完成登录流程。

5. 根据权利要求4所述的方法,其特征在于,该智能卡装置系为一从零售通路购置的一空白装置。

6. 根据权利要求5所述的方法,其特征在于,该智能卡具有一与内容/服务供应者相关联的一账户,且该智能卡装置可被该内容/服务供应者发行。

空白智能卡发行系统

【技术领域】

[0001] 本发明涉及一种空白智能卡系统,更具体而言,涉及一种提供空白芯片卡(IC卡)作为商业用途的方法及系统。

【背景技术】

[0002] 智能卡技术已于金融业行之有年,此技术使得金融业可核发给客户一具有智能芯片卡的银行卡(亦被称为IC卡),此种科技仰赖公开金钥基础建设(public key infrastructure;PKI)本身的稳定性以及其它领域已被证实的加密机制,来达成一个安全可以执行e化交易服务的平台。至于IC卡持有者亦为一个达成认证机制完善性的要素之一,IC卡持有者可利用拥有的顾客账户信息作为其中一种身份验证,更甚,使用个人辨识码(PIN)以及密码作为身份验证并登入及操作财务账户。持有者可通过ATM自动贩卖机或是网络的方式登入及操作。一般而言,会提供顾客一USB智能卡读取机,搭配网络的方式操作。考虑到信息安全的问题,此种IC卡总是由银行直接交予使用者。IC卡发行的步骤包含:

[0003] 1.使用者先于银行中建立一个新的账户。

[0004] 2.银行利用卡片制造机初始一张空白的IC卡。

[0005] 3.银行个人化IC卡,将使用者的账户信息导入IC卡之中。

[0006] 4.将IC卡邮寄至使用者。

[0007] 5.使用者利用电话或是网络启动此IC卡。

[0008] IC卡相较于其它传统的专属的加密以及解密机制而言,具有一些特殊以及稳定的特征:

[0009] 1.几乎能够达成防拷贝。

[0010] 2.现今的IC智能卡已被证实可防窜改(tamper-resistant)。

[0011] 3.IC智能卡的优缺点已被了解以及确认。

[0012] 4.此市场在过去二十年已经被拓展出来。

[0013] 随着USB装置的普及以及成本降低,很显然的可将一IC智能卡埋设于一标准的USB装置之中,IC智能卡亦被称为智能卡装置(Smart card device)。此种智能卡装置则可汰换掉前述的USB智能卡读取机以及IC卡。此种智能卡装置的架构可与现今使用USB读取机以及IC卡的方式使用模式全然兼容。若智能卡装置被正确的初始化、个人化和发行,即无理由不可提供现今IC卡的任一或全部的功能。进一步而言,IC智能卡更包含一附加的优点,就是内置的闪存(internal flash storage),此内存可被用于保护数据内容跟传递数据。因此,此优点拓展了IC卡可应用的领域。利用设置于USB智能卡装置中的IC智能卡本身防拷贝特性,内容拥有者可存储一独特的金钥及/或一组金钥,并可使用于加密以及解密媒体内容或一软件封包,特别指其上传送给顾客时所加设的保护及保全措施。

[0014] 基于与IC卡相同的商业发行模式,一特定的智能卡装置可被一指定内容拥有者发行给每个或全部的顾客。此智能卡装置可在自动贩卖机或是网络上操作,顾客可通过智能卡装置取得自身账户内容或是服务。此类型的内容或服务包含但不以此为限:音讯、影像、

软件封包、游戏、电子书和金融产品。智能卡装置是一个被垄断的市场以及应用，且以现今的商业模式在金融业运作良好。但，智能卡装置的市场及应用尚被许多要素所箝制：

- [0015] 1. IC智能卡仅能被特定发行者初始化、个人化跟发行。
- [0016] 2. 能发行IC卡的银行有限。
- [0017] 3. 具有高度数据安全疑虑。
- [0018] 4. IC卡上面发行者的名称可轻易辨识。
- [0019] 5. 顾客的个人身份证明标示于IC卡之上。
- [0020] 再言之，若特定的发行者使用与IC卡相同的发行方式，这些要素会同样的伴随着智能卡装置。
- [0021] 缘，此种商业模式下的信息内容的特性为拥有无限制数量的内容拥有者，因此上述所言的模块下，智能卡装置发行者仅能应用于一受限的范畴。一种可让智能卡装置应用范围扩大的机制，是亟需且可产生以下益处：
 - [0022] 1. 一个内容空白的智能卡装置可被购置于零售管道。
 - [0023] 2. 其智能卡装置可被此领域的顾客初始化以及个人化。
 - [0024] 3. 智能卡装置可由内容/服务提供者提供一账户建立设定。
 - [0025] 4. 此智能卡装置被视为由该内容/服务提供者所发行。
 - [0026] 5. 此新商业模式依然伴随着全部的数据安全问题。
 - [0027] 6. 发行者的名称通过电子以及实体上的辨识。
 - [0028] 7. 个人身份证明亦通过电子以及实体上的辨识。
- [0029] 鉴于此，人们所亟需的系统以及方法应需克服以上的问题，本发明即可达成以上需求。

【发明内容】

[0030] 本发明揭露一种空白智能卡发行系统和方法。一方面而言，揭露一种发行智能卡装置 (smart card device; SC) 的方法和系统。该方法及系统包含一由制造商提供智能卡装置的一初始阶段以及一身份验证阶段。该方法及系统亦包含发放智能卡装置，并于该智能卡装置发放后，由一发行者提供一初始身份验证阶段给一特定使用者，且发行者开始给予特定顾客一智能卡装置的第一登录流程。该方法及系统更包含在该初始身份验证阶段后，由该发行者提供该智能卡装置的另一身份验证阶段。因此，当该智能卡装置与该发行者两者互相验证身份后，该特定使用者及该发行者可完成登录流程。

[0031] 另一方面，本发明揭露了一种发行者利用智能卡装置数据传输的流程及系统。该流程及系统提供使用者登录一智能卡装置，且执行该智能卡装置与该发行者的互相身份验证。该流程与系统进一步包含在该互相身份验证后，建立一金钥，该金钥系作为加密和解密该发行者和该智能卡装置间的数据传输。

【附图说明】

- [0032] 图1为一现有IC卡的封闭散布模式的流程图 (先前技术)；
- [0033] 图2为一智能卡装置的开放散布模式的流程图；
- [0034] 图2A为一完整初始化以及个人化智能卡装置的流程图；

- [0035] 图2B为一流程图,绘示智能卡装置的数据传输;
- [0036] 图3为一流程图,绘示制造商提供的初始阶段;
- [0037] 图4为一流程图,显示制造商提供的智能卡装置的身份验证;
- [0038] 图5为一流程图,显示发行者提供给智能卡装置的第一次身份验证;
- [0039] 图6为一流程图,显示在该第一次身份验证阶段后,由该发行者提供智能卡装置的身份验证;
- [0040] 图7为一第一登录阶段的流程图;
- [0041] 图8为一流程图,显示由智能卡装置提供发行者的身份验证阶段;
- [0042] 图9为一第二登录阶段的流程图;
- [0043] 图10为一登入阶段的流程图;
- [0044] 图11为一互相身份验证的流程图;
- [0045] 图12为一数据传输阶段的流程图;以及
- [0046] 图13为一更改密码阶段的流程图。
- [0047] 【主要组件符号说明】
- [0048] 本案皆为步骤流程图,因此并无组件符号可列出。

【具体实施方式】

[0049] 本发明涉及一种银行卡系统,特别涉及一种可以提供一IC银行卡做商业用途的方法以及系统。以下的说明可使本领域的一般技艺人士可通过本专利案的内容,制作以及使用本发明以及其要求。下述的较佳实施例的不同的变化、基本原则以及特性的说明将可使本领域的一般技艺人士可轻易的了解。但本发明将不为以下实施例所限,其专利范围将以本文所述的原则和特征来做较宽广的解释。

- [0050] 本发明的系统与方法提供一种机构,该机构提供了以下的优点:
- [0051] 1.适用于所有现今的智能卡的商业模式、市场以及应用。
- [0052] 2.为了创造尚未成形的市场及应用,引介空白智能卡装置的商业模式。
- [0053] 3.提供了一可解决日益浮现的信息内容维安问题的工具。
- [0054] 虽然以上使用『智能卡装置』的名称,但其实泛指为应用在IC卡或应用于任何界面的智能卡,诸如保全数字卡(SD)或埋设于一智能卡之中的微型保全数字卡(micro SD)。
- [0055] 为了能够详述现今使用的系统以及方法,请参照以下的叙述以及搭配相对应的图式。
- [0056] 现有IC卡运作的生命周期包含了数个流程:
- [0057] 1.制造:设计组装IC智能卡和主机(hosting) IC卡。
- [0058] 2.预备卡片:加载智能卡操作系统。
- [0059] 3.初始化/个人化:程序初始化和个人化顾客信息。
- [0060] 4.开始运作:启用应用以及卡片。
- [0061] 5.终止:停用应用以及卡片。
- [0062] 一般而言,在IC卡的生命周期期间,涉及了数个不同的团体,团体包含IC卡供货商、卡片制造商、操作系统开发商、卡片发行者、存取终端机以及顾客。
- [0063] 如图1所示的现有IC卡的封闭散布模式的流程图,其依循着以下步骤:

[0064] (A1) IC卡供货商设计组装IC智能卡,该供货商可同时开发可被植入IC卡的智能卡操作系统(步骤11)。

[0065] (A2) 卡片制造商组装主机(hosting) IC卡并且将操作系统登录于其上,其操作系统可由IC供货商或卡片发行者所提供(步骤12)。

[0066] (A3) 顾客有一账户,此账户已由卡片发行者建立,卡片可为银行卡或是信用卡(步骤13)。

[0067] (A4) 卡片发行者得到的空白IC卡中已登录智能卡操作系统(步骤14)。

[0068] (A5) 根据特定使用者的账户信息,卡片发行者利用自身的机器设备将IC卡初始化及个人化(步骤15)。

[0069] (A6) 此IC卡视为『已发行』,并实质上送达顾客手上(步骤16)。

[0070] (A7) 顾客利用存取终端机、电话或个人计算机启用IC卡(步骤17)。

[0071] (A8) 卡片被发行服务器启用并可开始使用(步骤18)。

[0072] 需特别注意的是,在上述步骤15(A5)中,卡片发行者通过内部安全通道(in-house secure channel)执行IC卡初始化以及个人化。IC卡会搭载发行者的安全认证(security certificate),此安全认证可为稍后的身份验证阶段操作时使用。

[0073] 融合读取器功能以及智能卡于一单一的智能卡装置之中,根据本发明实施例的系统与方法在生命周期以及发行步骤上,可当一IC卡使用。进一步而言,一种经由机构提供的开放商业模式将被详述于下。

[0074] 请参见图2的实施例,其绘示一智能卡装置的开放散布模式,此散布模式包含了以下步骤:

[0075] (B1) IC卡供货商设计组装IC智能卡,该供货商可同时开发可被植入智能卡装置的操作系统(步骤21)。

[0076] (B2) 卡片制造商组装主机(hosting) 智能卡装置,并且将由IC供货商所提供的操作系统登录于其上(步骤22)。

[0077] (B3) 顾客有一由特定发行者建立的账户,此特定的发行者为一提供实质上的内容或是虚拟的服务的服务供货商(步骤23)。

[0078] (B4) 顾客可由任何相关业者铺设的零售通路购置或是索取智能卡装置(步骤24)。

[0079] (B5) 通过一存取终端机,最有可能是个人计算机,顾客可连接服务供货商/发行者的服务器,并执行智能卡装置的初始化和个人化(步骤25)。

[0080] (B6) 接着,服务供货商/发行者根据特定顾客的账户信息,通过存取终端机将智能卡装置初始化以及个人化(步骤26)。

[0081] (B7) 智能卡装置视为已被服务供货商/发行者『发行』(步骤27)。

[0082] (B8) 顾客通过相同的存取终端机启用智能卡装置(步骤28)。

[0083] (B9) 服务供货商/发行者启动智能卡装置并且可开始使用(步骤29)。

[0084] 比较图1的封闭散布系统与图2的开放散布系统,虽然两者有部分相似,但却有显著的相异点。于封闭模式中发行IC卡包含了步骤14(A4)以及步骤15(A5),而于开放模式中发行智能卡装置则需步骤24(B4)至步骤26(B6)。

[0085] 如图1所示,于一IC卡的现有封闭散布模式中,卡片发行者经由步骤14取得IC卡,因此此步骤与发行者有关。接着,通过专属的以及安全通道辅以特定顾客的账户信息,卡片

发行者利用自身的机器设备将IC卡初始化以及个人化。这过程通常代价高昂、毫无弹性、而且旷日废时。因此,较有益地可提供一种空白智能卡发行系统,因而本领域的使用者可将IC卡通过远程、安全的方式加以初始化以及个人化。且让使用者初始化智能卡的地点可为接通网络的个人计算机或可联机的公共场所的自动贩卖机。异于现有模式的是,此智能卡装置并不需要经过一发行者授权的『零售商』来完成个人化过程。尽管,两造之间的通信频道(communication channel)并不尽完善安全,但远程的个人化服务仍可利用一安全手段达成安全传送智能卡以及发行者之间的专属及机密数据。若上述的远程个人化过程广泛的应用,则可使得智能卡发行系统更具有成本效益及竞争性。

[0086] 在一智能卡装置的开放散布模式中,顾客会于初始化以及个人化之前就取得智能卡装置。因而,并不会隐含任何先备知识可将服务供货商/发行者与智能卡装置相关联。也因并无任何与供货商相关的先备知识,进而在初始化以及处理数据上产生了些许考验。第一,如下述问题所言,如何在一不安全的公共网络频道上验证服务供货商/发行者的身份,因智能卡装置制造时并无登录任何适切的认证。第二,在存在着众多可能的服务供货商/发行者情况下,如何在一不安全的公共网络频道上验证服务供货商/发行者的身份。第三,若顾客操作的初始化以及个人化皆通过存取终端机(可能是个人计算机)通过不安全的公众网络频道完成,要如何使智能卡装置维持安全。

[0087] 现今开放模式发明皆伴随着上述已知问题。本发明为可实行内容保障以及安全的内容散布的一种智能卡装置的零售散布模式。

[0088] 在开放散布模式中发行智能卡装置必然伴随着一些问题需要克服。第一,当在其领域中存在着众多可能的服务供货商/发行者,若要与其一服务供货商/发行者相关联,智能卡装置必须先确认要如何在不安全的公众网络频道中,验证智能卡装置身份。第二,当智能卡装置制造的初并无登录任何适切的认证,则必须确认要如何通过一个不安全的公众网络频道,验证服务供货商/发行者身份。第三,若顾客使用存取终端机(可能是计算机)通过一个不安全的公众网络信道执行初始化以及个人化,则需要确认如何使得智能卡装置维持安全。

[0089] 在上述问题解决之前,尚有三个工作需要在使用者拿到智能卡装置前完成:(1)智能卡是否被初始化了?(2)智能卡装置是否已经第一次登录过了?及(3)智能卡装置是否在本领域中已被登录以及身份验证?

[0090] 图2A为一完整初始化以及个人化一智能卡装置的流程图,其中流程始于由制造商(MN)提供的智能卡装置(SC)初始阶段(authentication phase)(步骤200)。紧接于其后的是,制造商提供智能卡装置身份验证阶段(步骤201)。在智能卡装置被发放之后,发行者(IS)提供智能卡装置第一次身份验证阶段(authentication phase)(步骤202)。发行者开始智能卡装置第一登录阶段(步骤203)。紧接着,发行者对智能卡装置施行身份验证阶段(步骤204)。智能卡装置因应此而开始对发行者进行一身份验证阶段(步骤205)。当智能卡装置以及发行者两者互相验证身份后,发行者开始第二次阶段登录(步骤206)。

[0091] 图2B为一智能卡装置的数据传输的流程图,在这流程中,使用者先经由存取终端机去执行一登入阶段(Login Phase)后(步骤207),智能卡装置以及发行者两者进行互相验证身份的阶段(步骤208)。在相互验证身份后,会建立一组金钥(session key),此金钥的用处为在数据传输阶段,提供发行者以及智能卡装置之间传输数据的加密以及解密用(步骤

209)。

[0092] 更多不同阶段的智能卡装置初始化以及个人化将详述如下。

[0093] 1.由制造商提供初始阶段

[0094] 根据图3所示,在制作的过程中,步骤31,制造商起初建立了一个特定的识别码(ID)UID_SC、一对钥匙,分别是一个人钥匙KS_SC和一公用钥匙KV_SC。在步骤33中,特定的识别码和一对钥匙皆被传送至智能卡装置。经由步骤34,制造商进一步传送一UID的认证,此认证上签署了一人钥匙KS_MN。伴随着此认证传送至智能卡装置的亦有制造商的公用钥匙KV_MN(步骤36)。智能卡装置于步骤39时储存UID_SC、KS_SC、KV_SC、KKV_MN以及CERT_UID_SC_by_MN。接着,步骤37,制造商将智能卡装置的公用钥匙KV_SC传送至一凭证机构(certificate authority;CA)。凭证机构签署及产生一认证CERT_KV_SC_by_CA(步骤300),认证接着在步骤302会被传回智能卡装置,并在步骤306中存储于智能卡装置中。制造商亦同时将它的公用钥匙KV_MN传送给凭证机构,以产生一签署认证。若凭证机构第一次收到此认证请求,则会使用它个人钥匙KS_CA签署并存储认证CERT_KV_MN_CA,做为以后参考用(步骤304)。

[0095] 2.由制造商提供智能卡装置的身份验证阶段

[0096] 如图4所示,步骤42中,制造商请求从智能卡装置中取得UID_SC及CERT_UID_SC_by_MN。并于步骤43中从智能卡装置接收UID_SC及CERT_UID_SC_by_MN。紧接着,制造商传送它的公用钥匙KV_MN至凭证机构(步骤44),并请求凭证机构回传KV_CA、CERT_MN_by_CA(步骤45)。步骤46,凭证机构回传它自身的公用钥匙KV_CA以及先前储存的相对应制造商的公用钥匙KV_MN的认证CERT_MN_by_CA。制造商接着从接受到的数据中解密出公用钥匙KV_MN1(步骤47)。取出的公用钥匙KV_MN1可进一步用以解密认证CERT_UID_SC_by_MN和索取特定识别码UID_SC1(步骤48)。若索取的特定识别码UID_SC1等于原始智能卡装置储存的UID_SC,则智能卡装置验证完成(步骤49)。若否,则验证失败(步骤401)。经过此阶段,智能卡装置可被发放(deploy)至该领域。

[0097] 3.发行者给予智能卡装置第一次身份验证阶段

[0098] 智能卡装置通过发布者发放至该领域和成为终端使用者的财产后,智能卡装置已可和发行者产生第一次相关联。但先于任何个人化或登录流程之前,智能卡装置需与发行者身份验证。如图5所示,步骤52,发行者要求从智能卡装置中取得UID_SC、CERT_UID_SC_by_MN、KV_MN。接收智能卡装置中的UID_SC、CERT_UID_SC_by_MN、KV_MN后(步骤53),发行者将接收的制造商公用钥匙KV_MN传送给凭证机构(步骤54),并向凭证机构索取KV_CA、CERT_MN_by_CA(步骤55)。接着,凭证机构返还它的公用钥匙KV_CA并搜寻先前相对应制造商的公用钥匙KV_MN的认证CERT_MN_by_CA(步骤56)。发行者即可自接收的信息解密公用钥匙KV_MN1(步骤57)。进一步而言,公用钥匙KV_MN1旨在用于解密认证CERT_UID_SC_by_MN并索取一特定辨识码UID_SC1(步骤58)。若索取的UID_SC1与原本储存于智能卡装置中的辨识码UID_SC相同,则智能卡装置身份验证完成(步骤59)。若否,则身份验证失败(步骤501)。

[0099] 4.第一登录阶段

[0100] 智能卡装置被发行者第一次验证后,智能卡装置可开始第一登录阶段。如图6所示,发行者传送它的公用钥匙KV_IS给凭证机构并要求一认证(步骤61)。凭证机构使用一个人钥匙KS_CA签署并产生一认证CERT_KV_IS_by_CA(步骤62)。此认证接着返回发行者(步骤

63)。在步骤64中,发行者向智能卡装置索取公用钥匙KV_SC。在发行者接收到KV_SC后,发行者会在其上签署他个人钥匙KS_IS,并产生一认证CERT_KV_IS_by_CA(步骤66)。接着,步骤67,发行者发送二认证CERT_KV_IS_by_CA和CERT_KV_SC_by_IS给予智能卡装置。智能卡装置则会储存这两个认证并做稍后使用(步骤68)。此时,智能卡装置已可开始进一步的个人化。

[0101] 5.第一次身份验证后,发行者对智能卡装置施行身份验证阶段

[0102] 请参考图7,步骤71中,发行者先产生了一组随机数字RNUM1。接着在步骤73中,作为一个讯问信号(challenge),此随机数字RNUM1被送至智能卡装置。为了产生一认证CERT_R_by_SC,此随机数字RNUM1由智能卡装置的个人钥匙KS_SC所签署(步骤74)。并在步骤76中,将此认证传回发行者。在步骤78中,发行者紧接着向智能卡装置索取先前储存的认证CERT_KV_SC_by_CA。此返还的认证,在步骤700中,再被索取并归还给发行者。在步骤701中,发行者向凭证机构索取凭证机构的公用钥匙KV_CA。在702步骤中接收KV_CA后,步骤703中,发行者使用向凭证索取机构的公用钥匙来修复(recover)相对应的智能卡装置公用钥匙KV_SC1。被修复的智能卡装置公用钥匙KV_SC1,可被用以修复相对应认证CERT_R_by_SC中随机数字,并与原始作为讯问信号的随机数字RNUM1相比对(步骤704)。若比对相同,则智能卡装置身份验证完成。若否,则身份验证失败(步骤705)。

[0103] 6.智能卡装置对发行者进行一身份验证阶段

[0104] 智能卡装置被发行者身份验证后,换成智能卡装置对发行者进行身份验证。如图8所示,步骤81中智能卡装置产生一随机数字RNUM2。步骤83,作为一个讯问信号,此第二随机数字被送至发行者。并在步骤84中,发行者签署了他的个人钥匙KS_IS,并将认证CERT_R_by_IS回传给智能卡装置(步骤86)。此时,智能卡装置向凭证机构索取一公用钥匙KV_CA(步骤800)。并在步骤803,凭证机构传回一公用钥匙KV_CA给智能卡装置。经由步骤804,智能卡装置向其内存索取一认证CERT_KV_IS_by_CA,并以凭证机构的公用钥匙KV_CA进行解密。解密后得到一发行者公用钥匙KV_IS1,此发行者公用钥匙可进一步使用于认证CERT_R_by_IS的解密。将解密后的结果与先前的随机数字RNUM2比对(步骤805)。若比对相同,则发行者身份验证成功。若否,则失败(步骤806)。

[0105] 7.第二登录阶段

[0106] 当发行者与智能卡装置完成相互验证身份后。发行者已可开始执行登录第二登录阶段。如图9所示,发行者向智能卡装置索取一特定的识别码(ID)UID_SC(步骤92)。在步骤94,智能卡装置回传发行者欲索取的信息。步骤95,发行者开始个人化/登录流程,起先必须创建一对相对应的账号名称以及密码ACCT及PSWD。步骤96,同时产生一组随机数字ACCT_key_on_IS及ACCT_key_on_SC。并在步骤97,账户名称ACCT会与随机数字ACCT_key_on_IS相异(exclusive-or),并产生一杂凑值(hash value)HASH_ACCT。相对应的密码PSWD则与随机数字ACCT_key_on_SC相异,并产生一杂凑值HASH_PSWD(步骤98)。HASH_ACCT及HASH_PSWD产生了一相异的HASH_ACCT_PSWD。HASH_PSWD可进一步的与HASH_ACCT杂凑后建立一签章SIG_HASH_ACCT_PSWD(步骤99)。在步骤901中,HASH_ACCT_PSWD、SIG_HASH_ACCT_PSWD、ACCT_key_on_SC等数据被传送至智能卡装置,并储存于智能卡装置之中(步骤902)。发行者亦储存了ACCT、ACCT_key_by_IS于其数据库作为稍后使用(步骤903)。此时,发行者即完成特定智能卡装置的登录或个人化,此智能卡已可被使用。

[0107] 登入阶段

[0108] 图10为一流程图,绘示使用者通过存取终端机的登入阶段。步骤101,使用者在存取终端机上键入账户名称ACCT1及密码PSWD1,以便登入。步骤102,账户名称ACCT1及密码PSWD1皆被传送至智能卡装置。在步骤103中,智能卡装置产生一HASH_PSWD1。步骤104, HASH_ACCT2产生于HASH_ACCT_PSWD及HASH_PSWD1中。签章SIG_HASH_ACCT_PSWD1即由杂凑的HASH_ACCT2和HASH_PSWD1所产生(步骤105)。若签章SIG_HASH_ACCT_PSWD1与先前储存的SIG_HASH_ACCT_PSWD相同(步骤106),则登入成功且可继续执行互相身份验证阶段(步骤108)。反的,则登入失败(步骤107)。

[0109] 为了达成发放智能卡装置于其领域之中,在本实施例中,假设无论是个人计算机与智能卡装置之间、个人计算机与发行者之间,以及发行者与凭证机构之间的通信频道皆为不安全频道。

[0110] 为了进一步的改善通信安全,在不同团体间的双向沟通中加入了一个讯问信号以及反馈机制。

[0111] 为了进一步的改善通信安全,一个讯问信号以及反馈机制被加入,以为不同团体间的双向沟通提供一金钥。

[0112] 现今证实有效机制包含金钥交换键一致的算法(Diffie-Hellman; D-H),利用此算法产生一必要的共享金钥SK,此共享金钥可在不安全的频道下为两团体所用。

[0113] 但金钥交换键一致的算法需要比其它金钥交换机制更长的作用时间。本发明的其中一目的即为以其它的金钥交换机制来补充传统的交换键一致的算法的交换机制。

[0114] 1.互相身份验证阶段

[0115] 图11为一流程图,其绘示发行者及智能卡装置的互相身份验证。登入成功后,步骤111中,智能卡装置产生了一随机数字RNUM3。步骤112中,RNUM3及ACCT_key_on_SC产生一HASH_RNUM3。HASH_ACCT2_RUM3也一样地被产生出来。在步骤112中,智能卡装置依据最近时标(time stamp)T1产生一签章SIG_HASH_ACCT2_RNUM3_T1。步骤113中,账户名称ACCT1、杂凑值HASH_ACCT2_RNUM3、一时标T1以及签章SIG_HASH_ACCT1_RNUM3_T1皆被传送至发行者。发行者接着核实ACCT1和时标T1的有效性。若核实确实,发行者则可查阅账户数据库跟索取账户相关的秘密金钥(secret key)ACCT_key_on_IS,此为步骤114。步骤115中, HASH_ACCT1、HASH_RNUM3及一签章SIG_HASH_ACCT1_RNUM3_T1被产生出来。步骤116中,比对两个签章。若两者相异,则智能卡装置的身份验证失败(步骤117)。反的,发行者可查阅此智能卡装置的最近时标,以及依据杂凑时标T3产生一新的签章SIG_HASH_ACCT1_RNUM3_HASH_T3(步骤118)。产生杂凑时标HASH(T3)的目的是为了避免可能的回放攻击(replay attack),时标T3及新签章SIG_HASH_ACCT1_RNUM3_HASH_T3会被在步骤1100时传送至智能卡装置。智能卡装置会核实此时标T3是否为正确(Valid)。同样地,在步骤1101中,产生一新签章SIG_HASH_ACCT2_RNUM3_HASH_T3。此新产生的签章会与刚接收的签章SIG_HASH_ACCT2_RNUM3_HASH_T3相比对(步骤1102)。若比对失败,则发行者的身份验证失败(步骤1103)。反的,发行者的身份验证和互相身份验证完成。此时,一金钥SK已建立。智能卡装置的金钥为HASH_RNUM3,此金钥与刚产生的随机数字RNUM3和秘密金钥ACCT_key_on_SC相关联。而发行者的金钥为HASH_RNUM3(步骤1105),产生的逻辑基本上与HASH_RNUM3相同。

[0116] 2.数据传输阶段

[0117] 图12为一流程图,其绘示互相身份验证完成后的数据传输阶段。在两个团体之间,建立一被用以加密/解密的金钥。在步骤121和122中,一金钥SK已被建立。此钥匙可被当作一双向认可的秘密钥匙,并用以传输发行者以及智能卡装置之间的数据。若智能卡装置欲传送SC_DATA给发行者,则SC_DATA会优先被金钥SK加密,并因此产生一加密过的信息E_SC_DATA(步骤123)。此加密的信息接着通过公用不安全的通信频道被传送给发行者(步骤124)。此加密过的信息,接着被先前所述的认可的秘密钥匙SK解密,并于发行者的接收端产生一SC_DATA(步骤125)。

[0118] 相似地,若发行者试图传送IS_DATA给智能卡装置,则IS_DATA会优先被金钥SK加密,并因此产生一加密过的信息E_IS_DATA(步骤126)。此加密的信息接着通过公用不安全的通信频道被传送给智能卡装置(步骤127)。此加密过的信息,接着被先前所述的认可的秘密钥匙SK解密,并于智能卡装置接收端产生一IS_DATA(步骤128)。

[0119] 3. 更改密码阶段

[0120] 图13为一流程图,其绘示一更改密码过程,此过程并不需要涉及发行者服务器。在某些情况的下,使用者需要更改密码。理想情形的下,更改密码亦需要发行者的些许关注。但于本实施例中,更改密码的过程中,发行者的参与为非必要的,并可保持智能卡装置既安全且数据完整。

[0121] 一开始,使用者需于一存取终端机中键入旧密码PSWD1(步骤131),接着密码会被传送至智能卡装置(步骤132),并产生一相对应的杂凑密码HASH_PSWD1。一杂凑账户名称HASH_ACCT2,产生于HASH_PSWD1以及先前储存的HASH_ACCT_PSWD之中。同样的,签章SIG_HASH_ACCT_PSWD1亦可产生于HASH_ACCT2和HASH_PSWD1(步骤133)之中。此签章接着与之前储存的签章SIG_HASH_ACCT_PSWD相比对(步骤134)。若比对失败,则登入失败。反的,若比对成功,则登入成功。使用者被提醒键入一新密码PSWD2(步骤136),新密码PSWD2则被送入智能卡装置(步骤137)。智能卡装置中的新密码PSWD2与秘密钥匙ACCT_key_on_SC可产生一HASH_PSWD2,HASH_ACCT_PSWD以之前接收的HASH_ACCT2及新产生的HASH_PSWD2进行更新。签章SIG_HASH_ACCT_PSWD亦可以HASH_ACCT2和HASH_PSWD2进行更新(步骤138)。更新过的HASH_ACCT_PSWD及SIG_HASH_ACCT_PSWD皆被储存于智能卡装置里作为以后使用(步骤139)。

[0122] 另一例示实施例

[0123] 虽然本实施例特别指可施行于『智能卡装置』之中,但其亦可应用在IC卡或应用于任何界面的智能卡,诸如保全数字卡(SD)或埋设一智能卡的微型保全数字卡(micro SD)之中。

[0124] 上述的实施例仅用来例举本发明的实施态样,以及阐释本发明的技术特征,并非用来限制本发明的保护范畴。任何熟悉此技术者可轻易完成的改变或均等性的安排均属于本发明所主张的范围,本发明的权利保护范围应以申请专利范围为准。

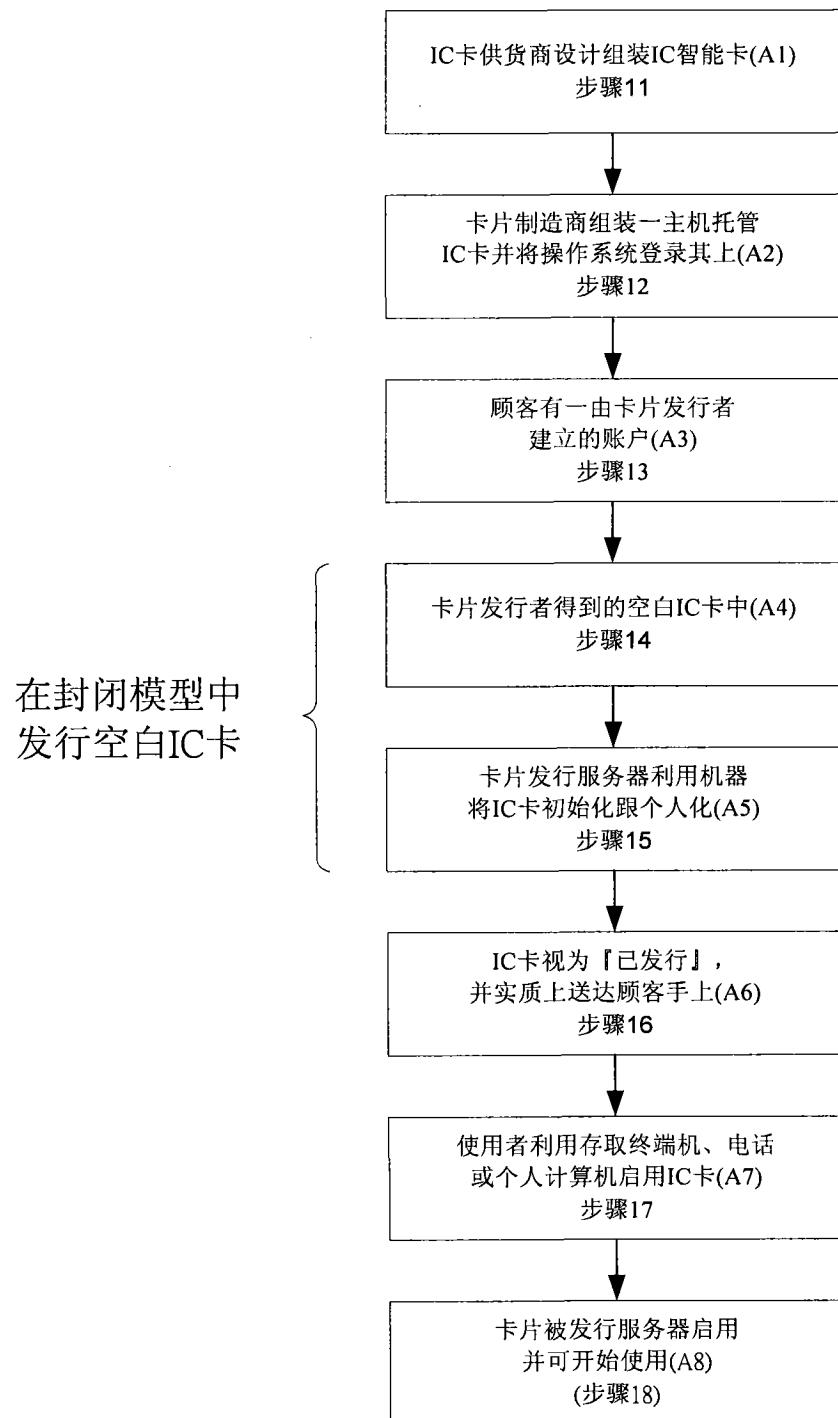


图1

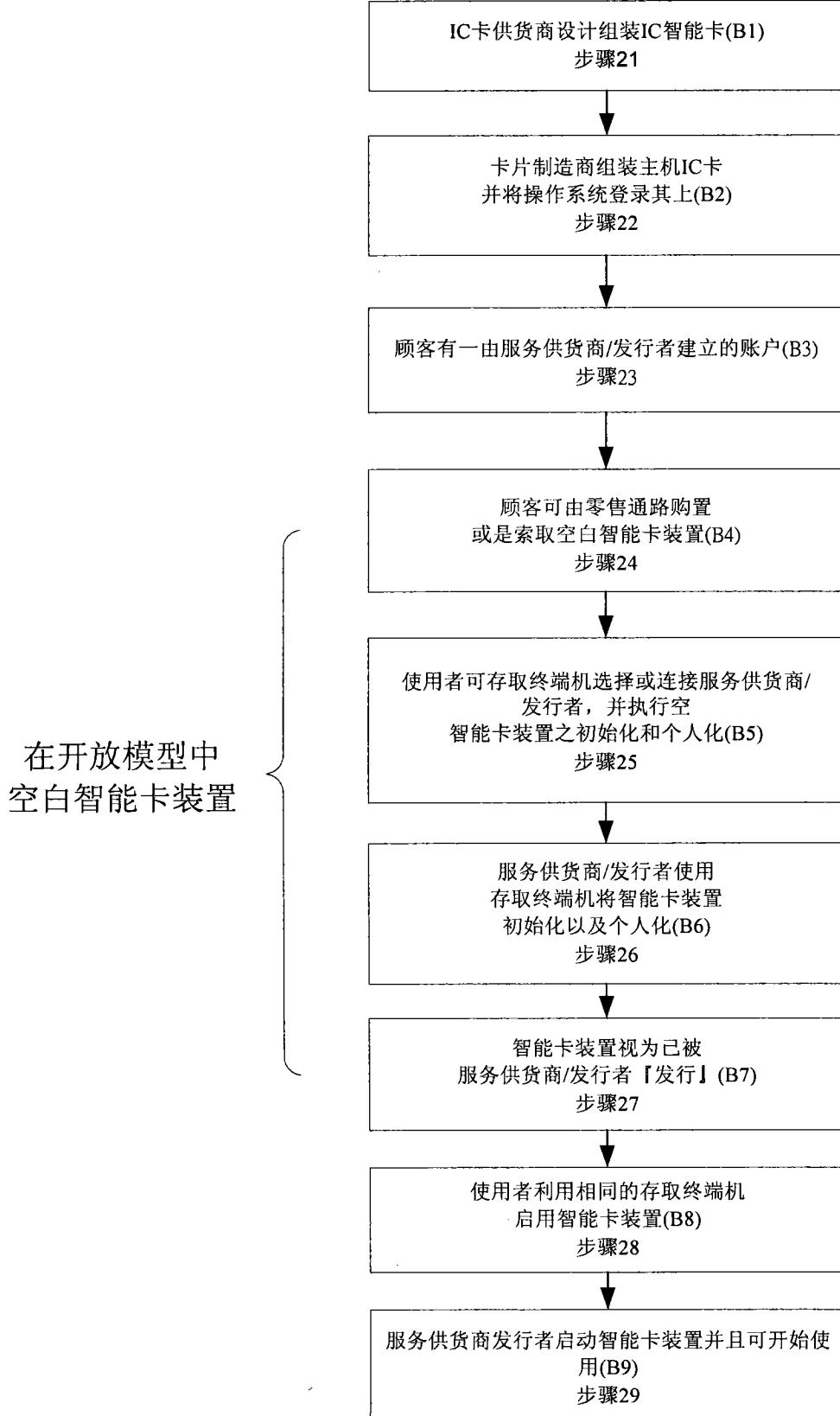


图2

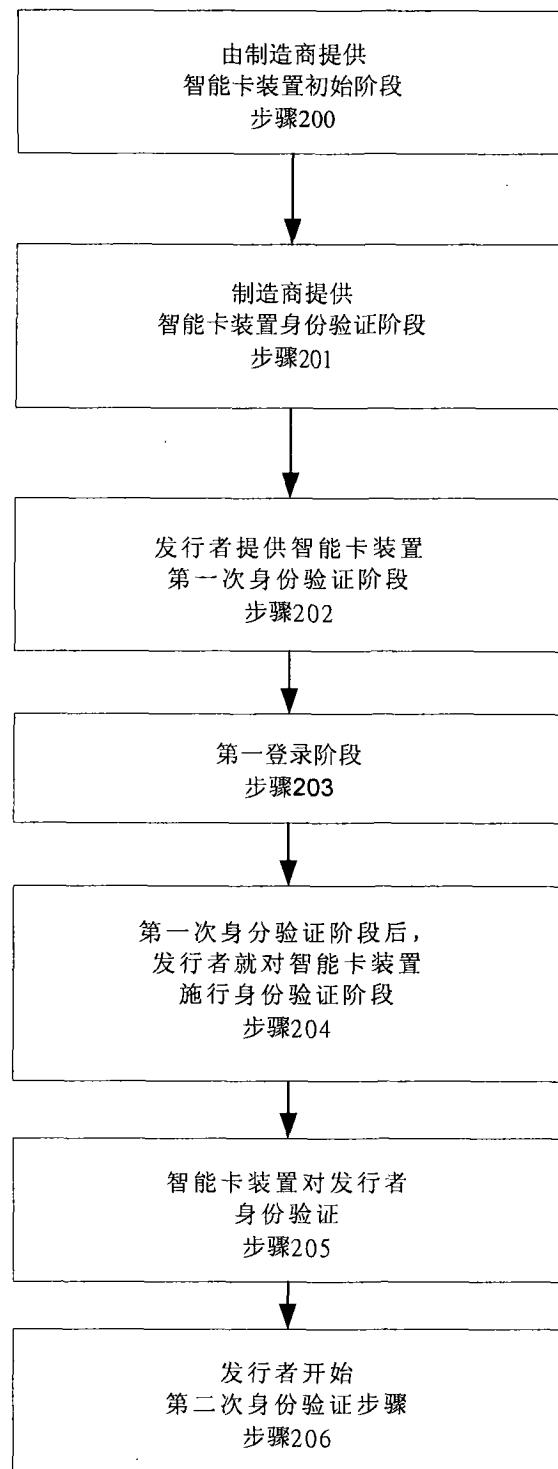


图2A

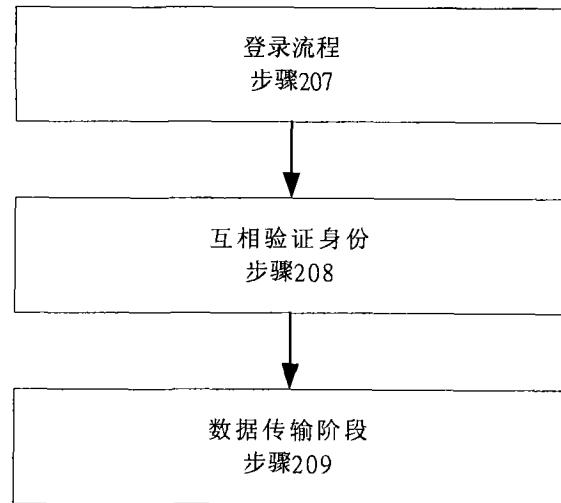


图2B

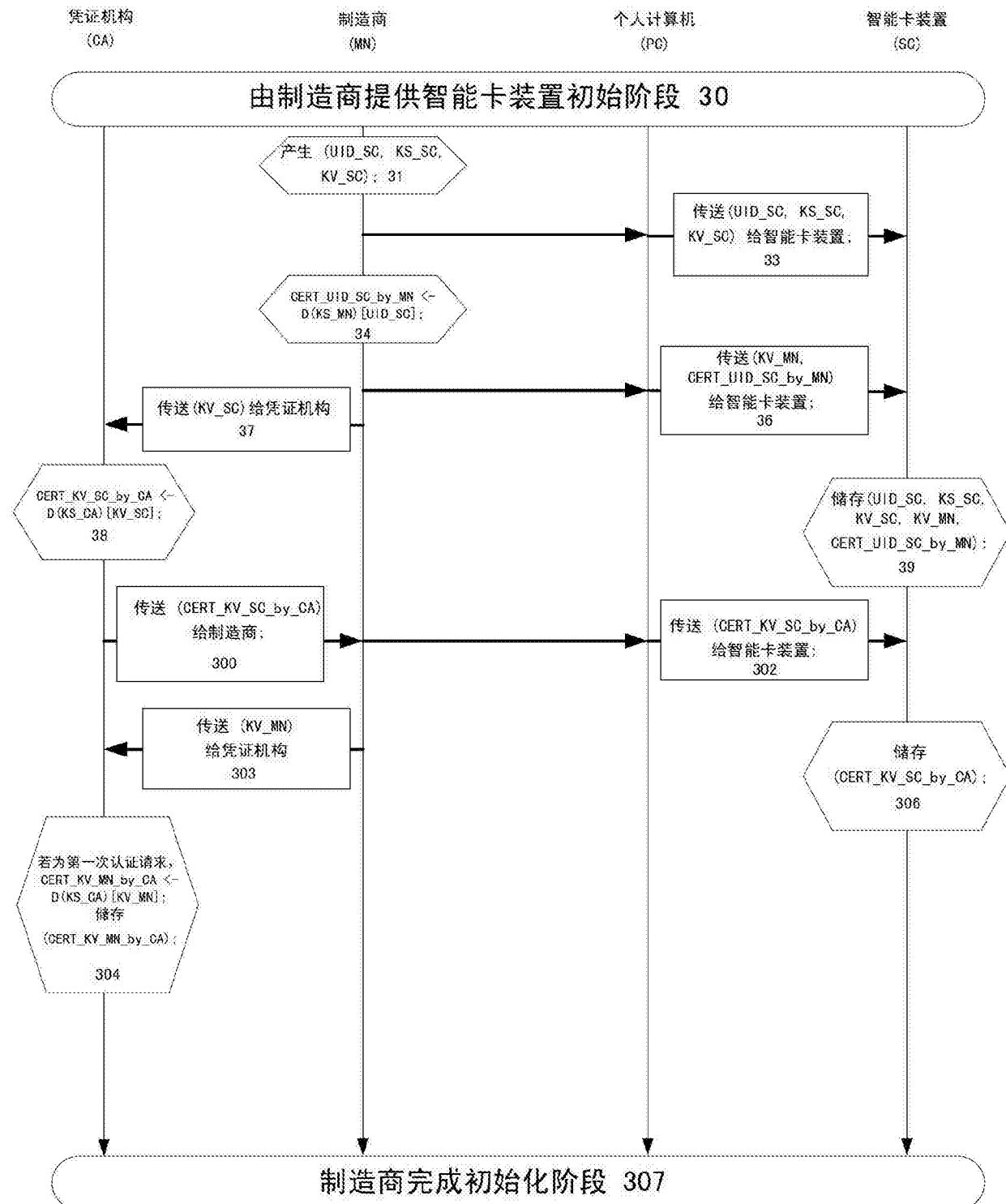


图3

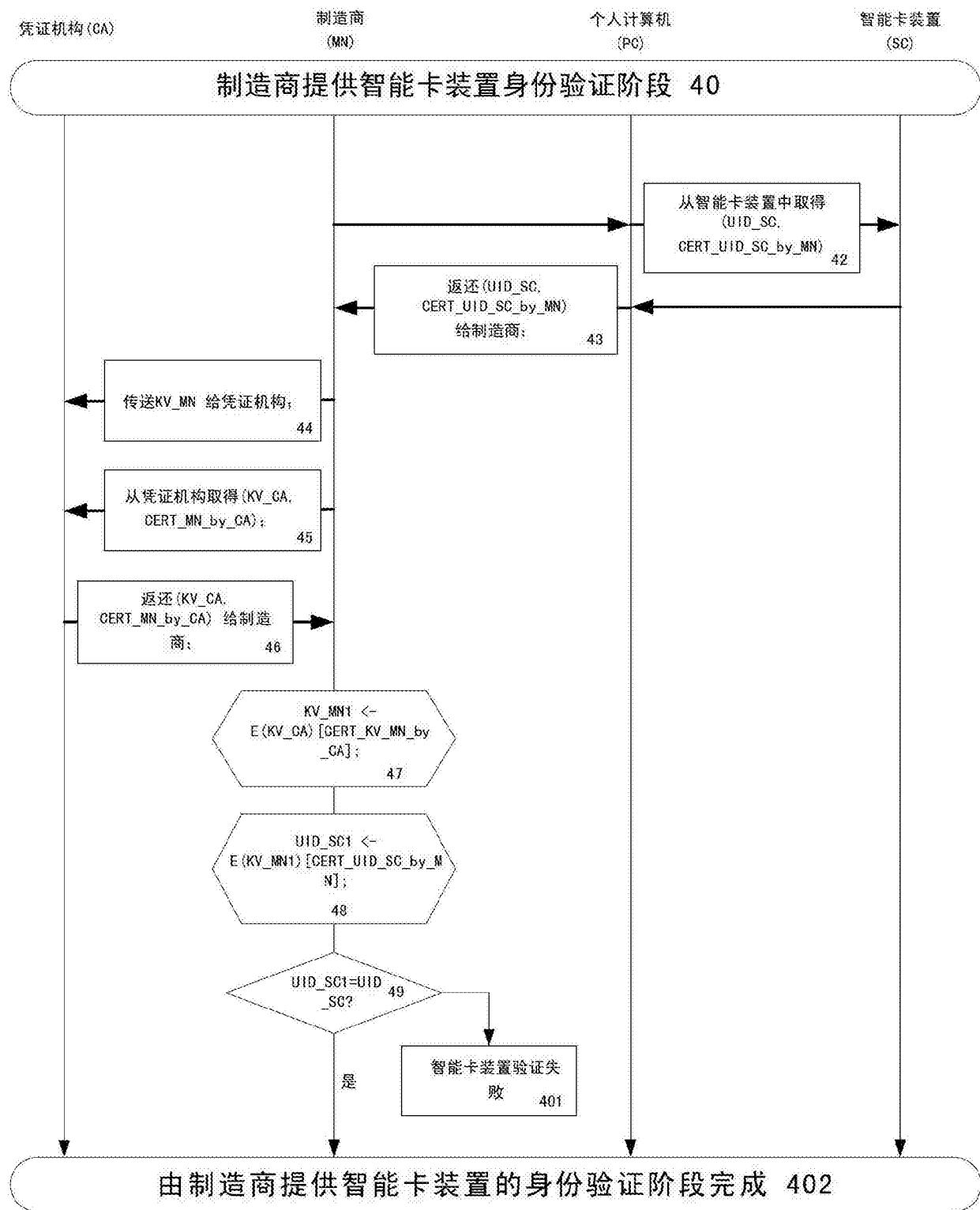


图4

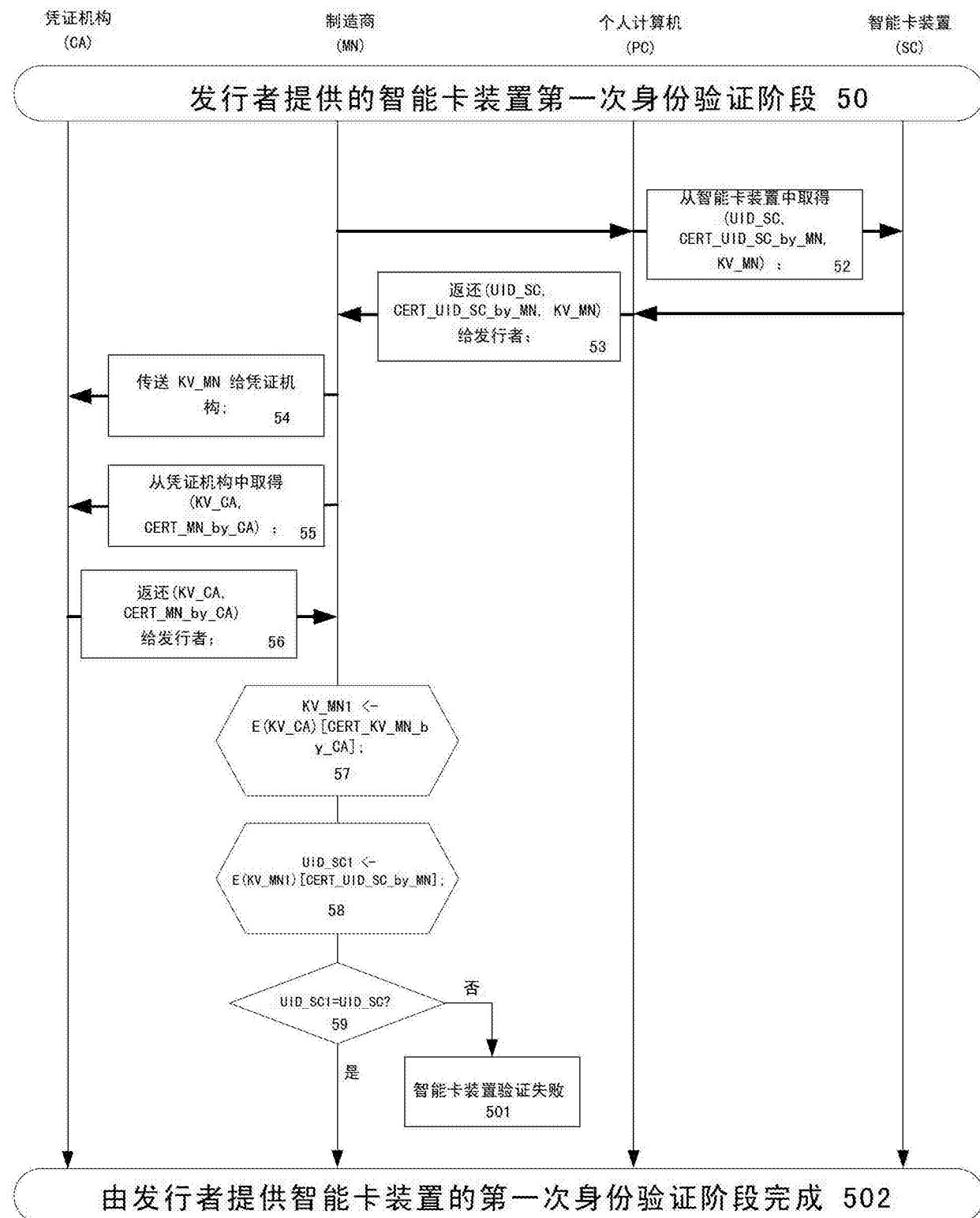


图5

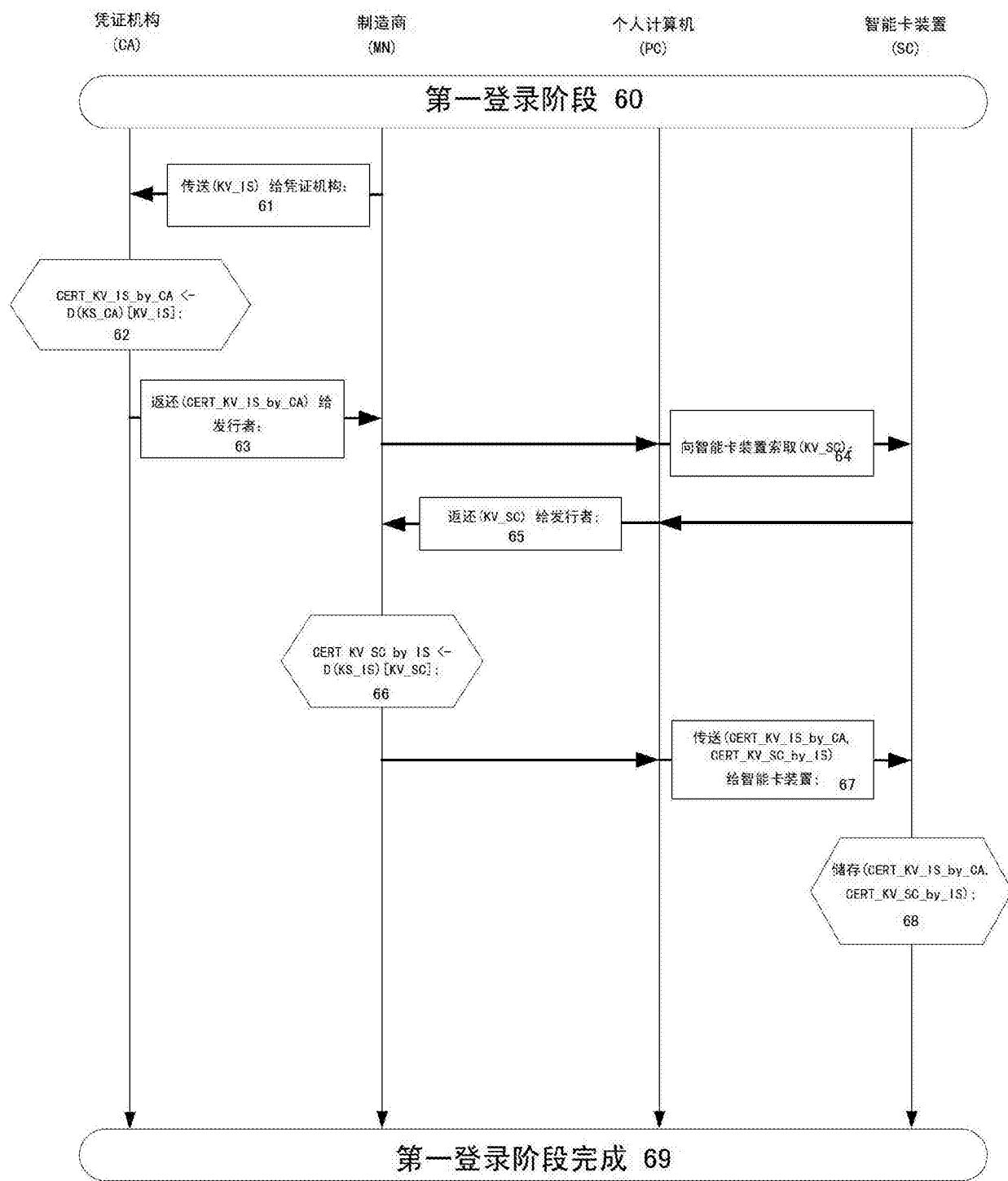


图6

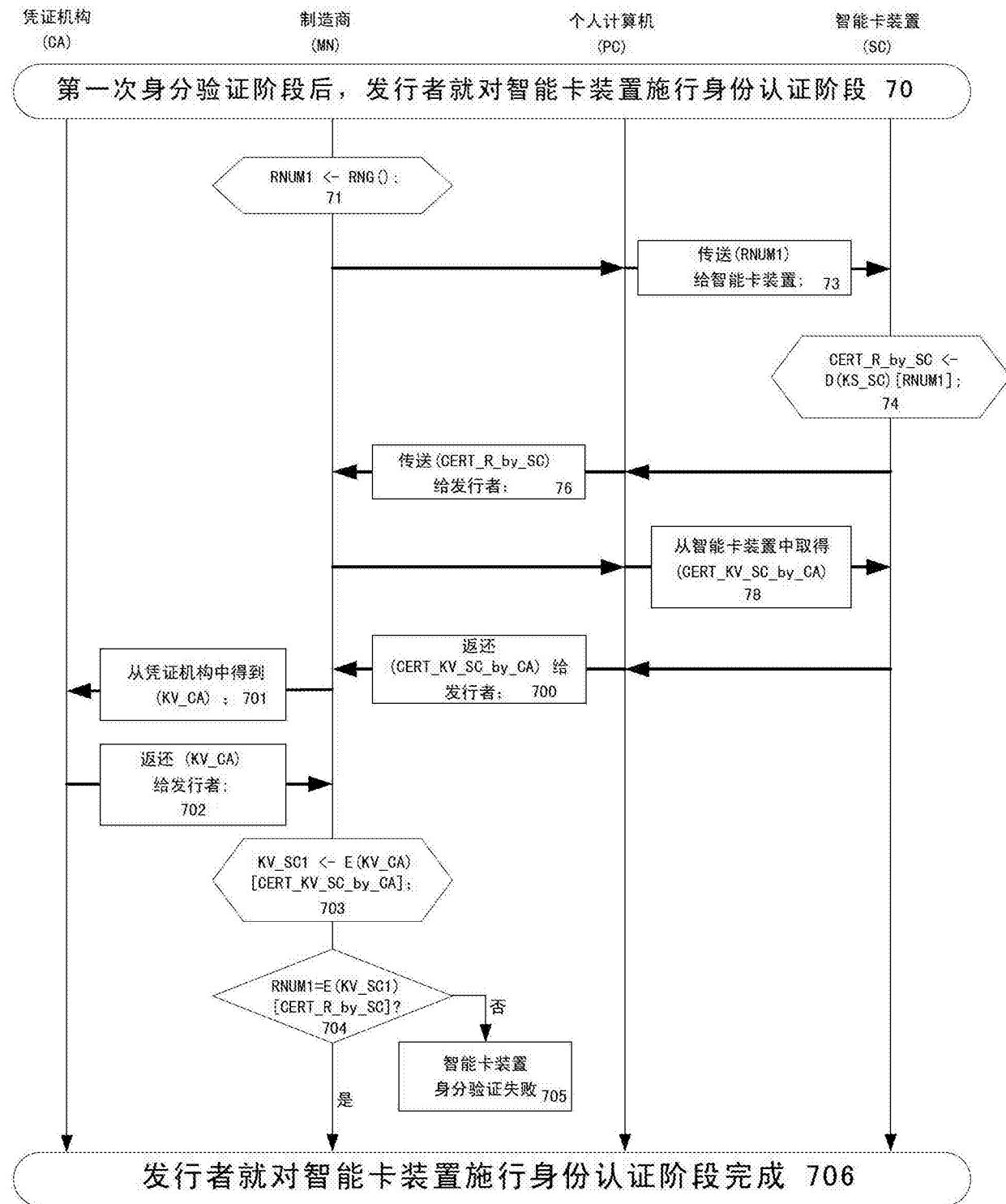


图7

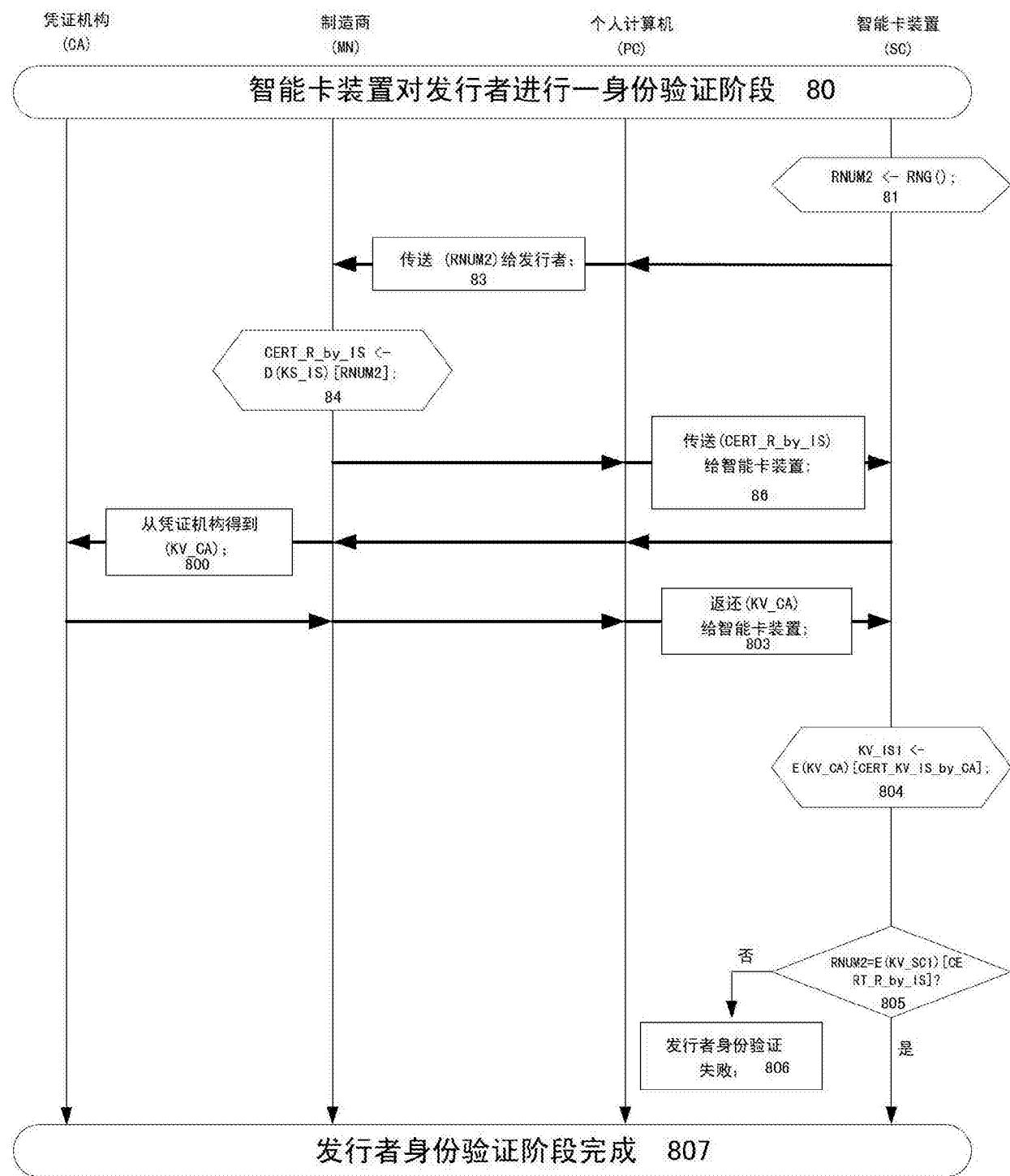


图8

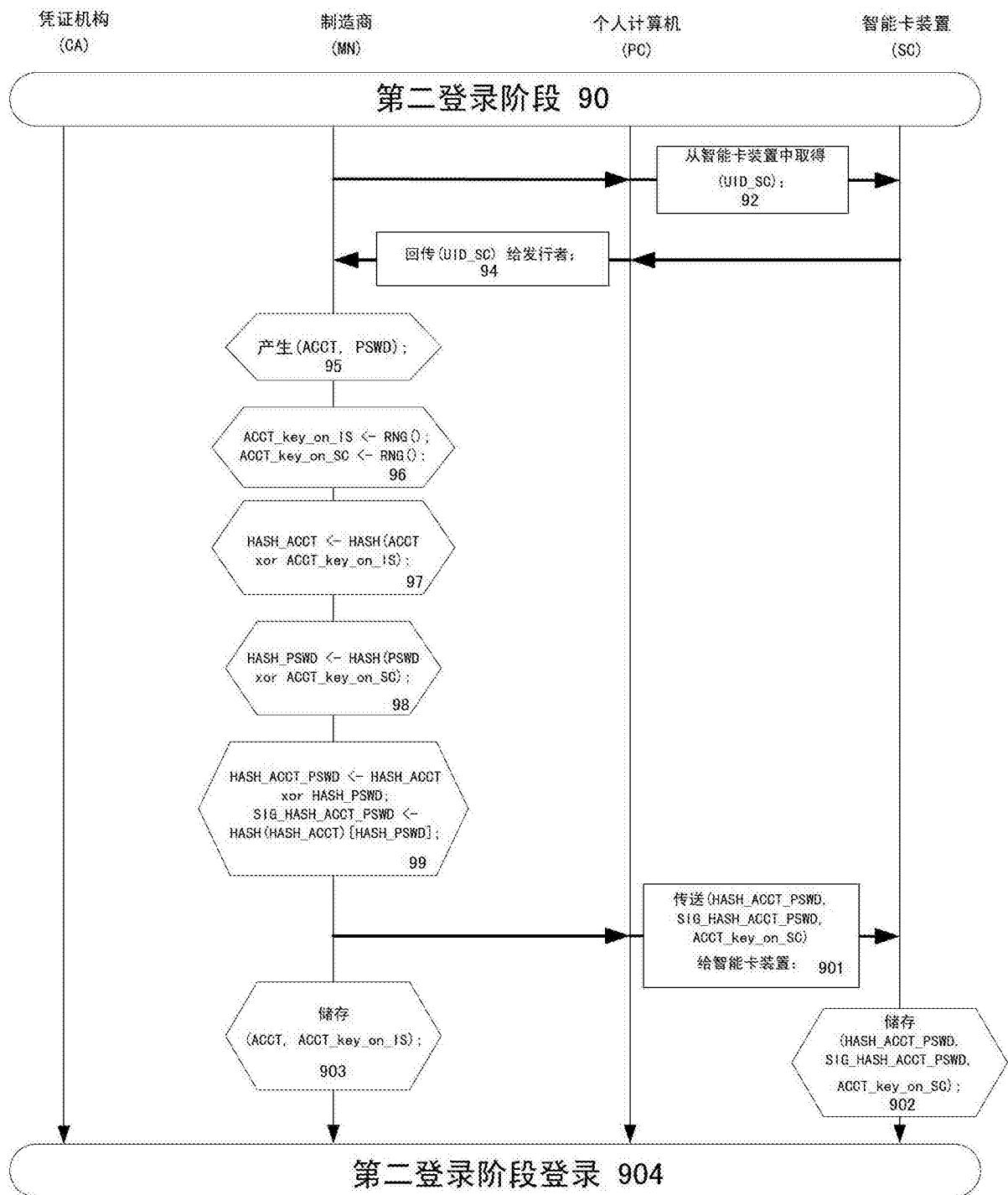


图9

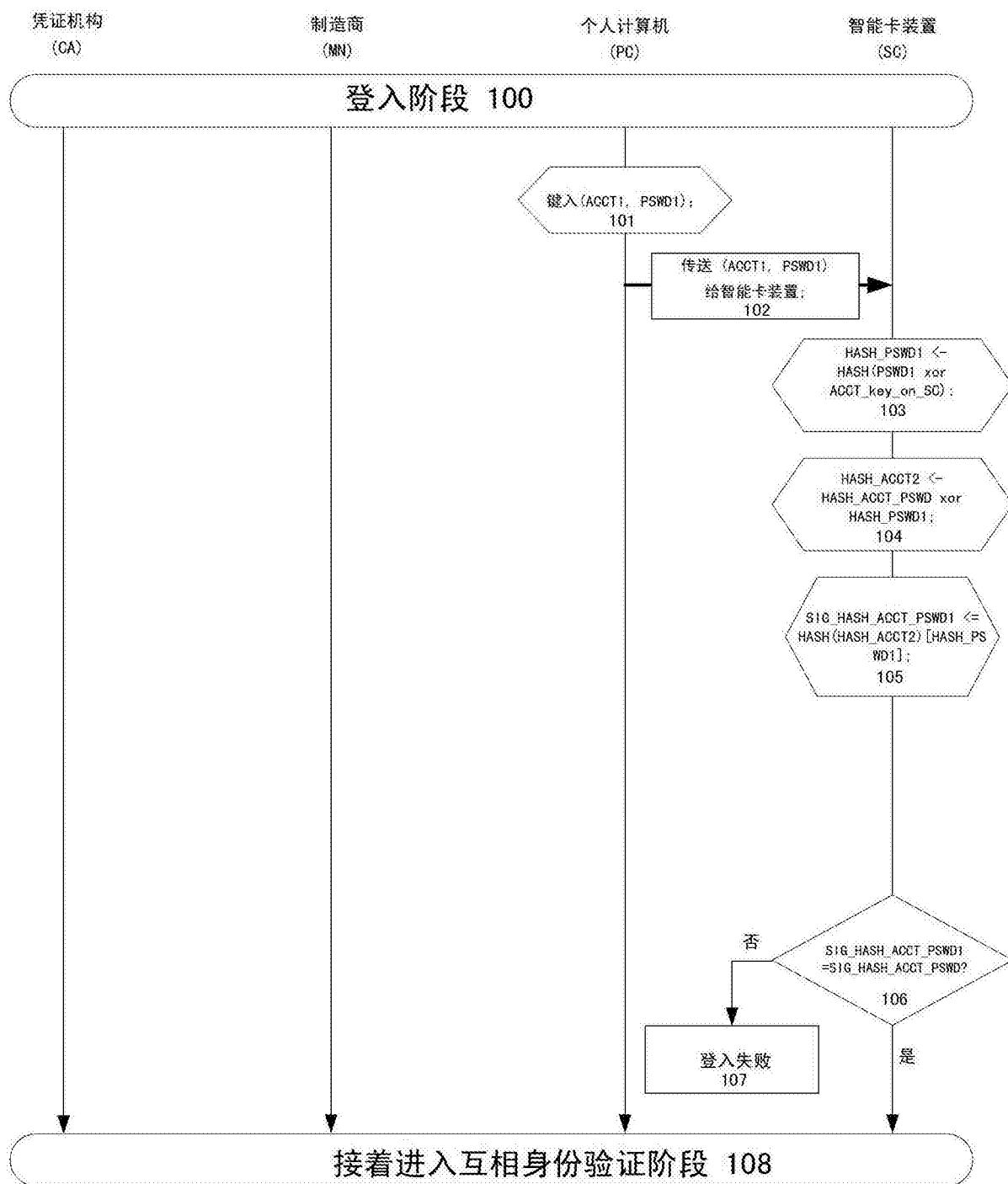


图10

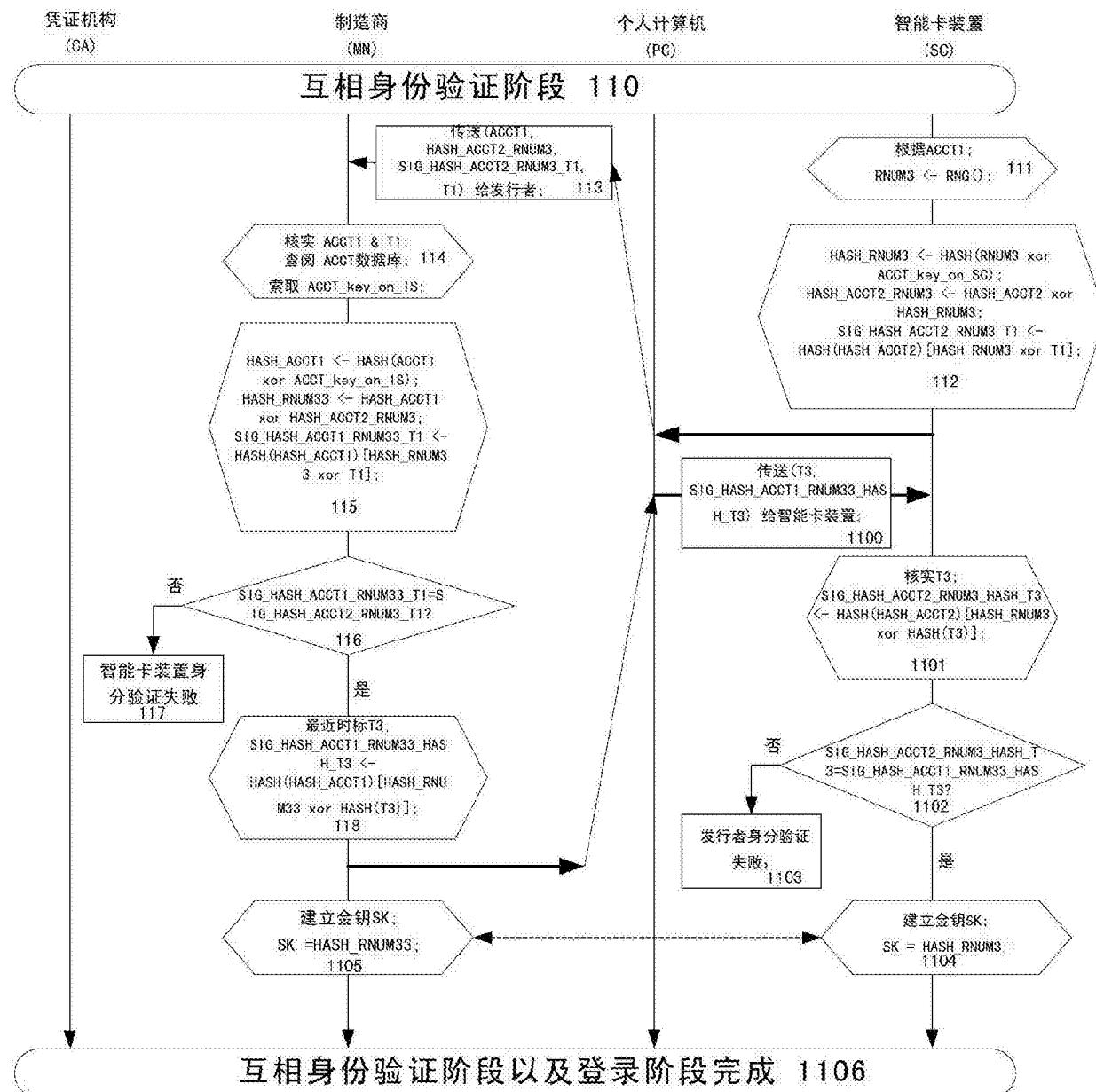


图11

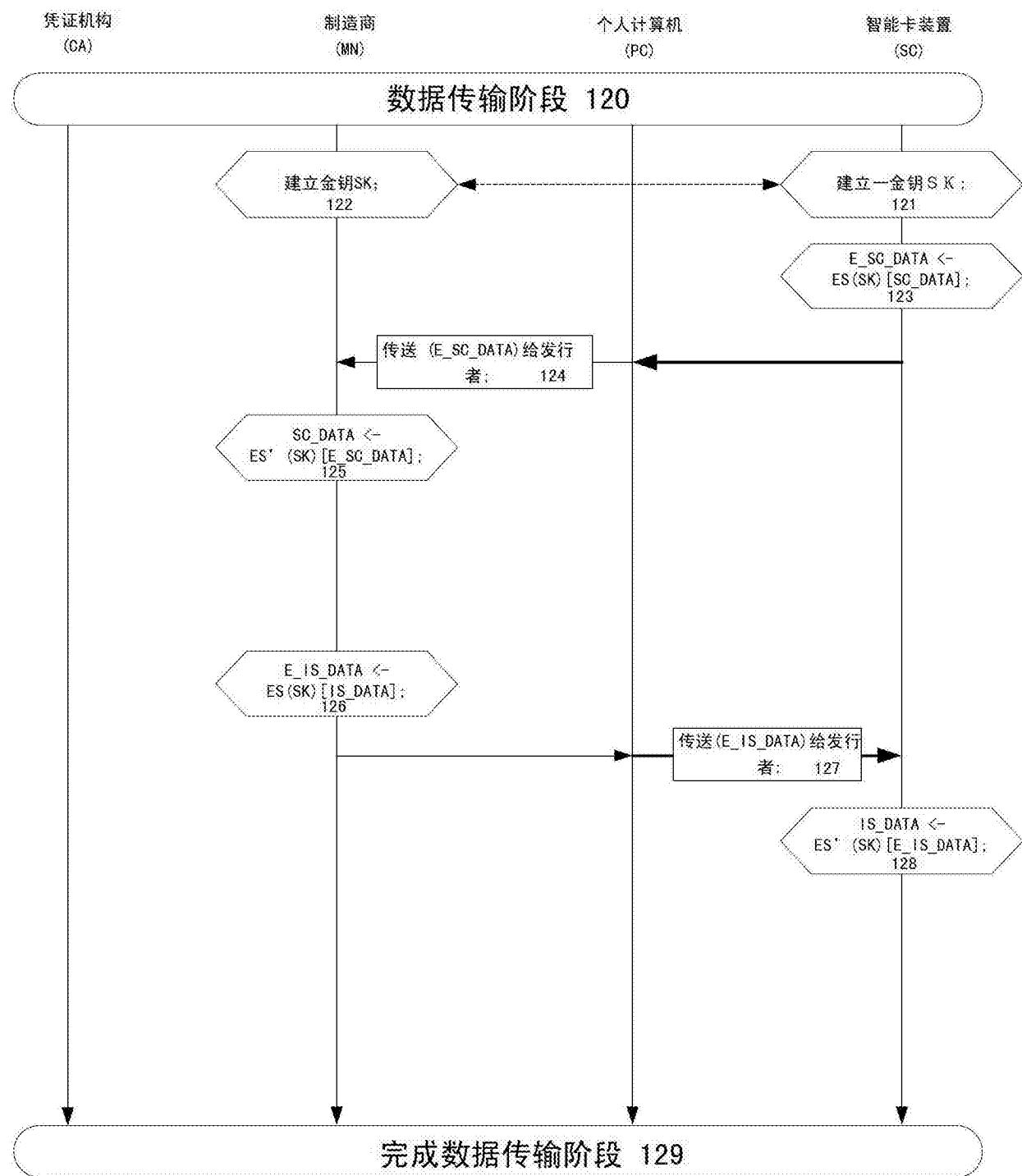


图12

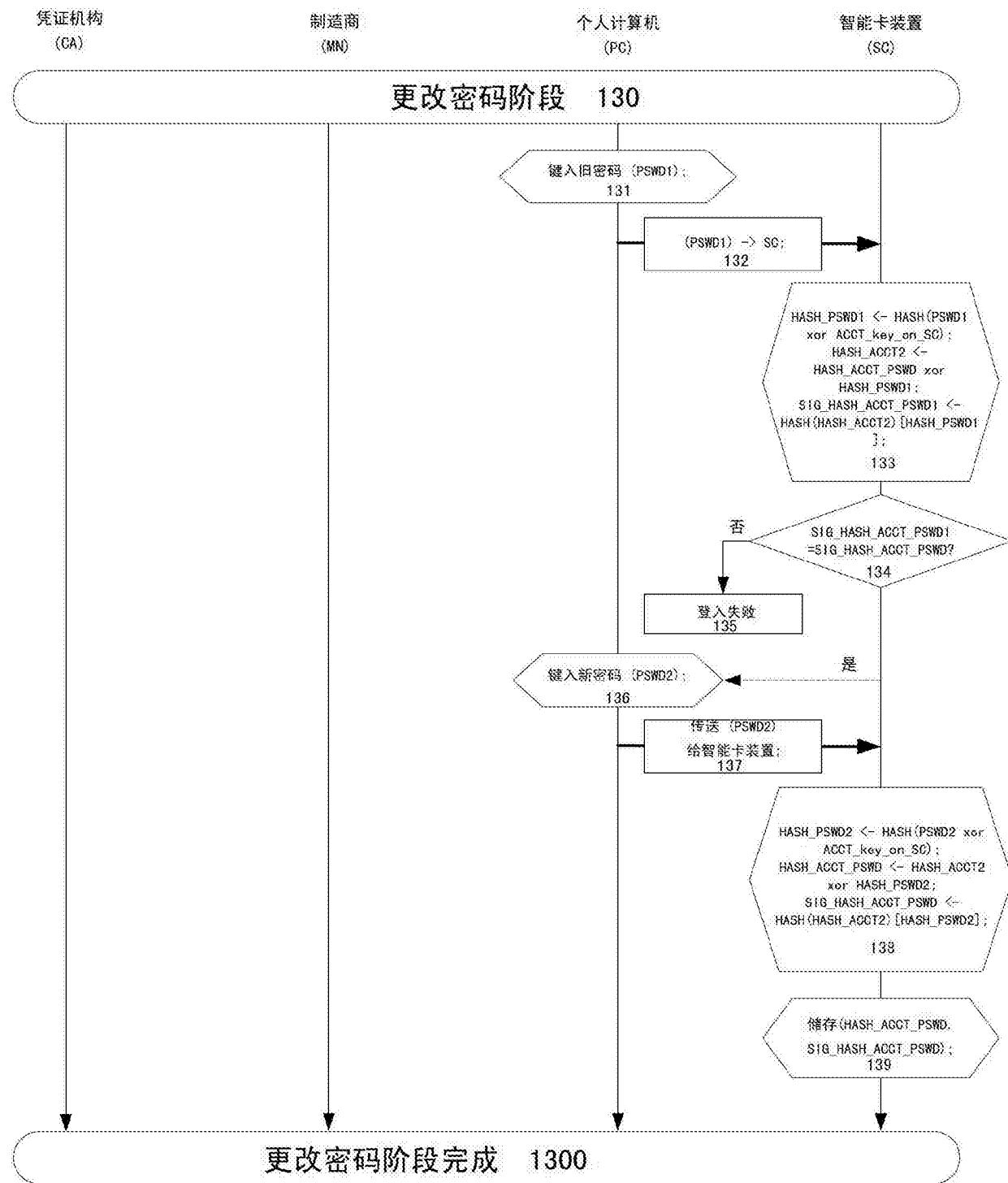


图13