(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102640176 B
(45)授权公告日 2016.03.02

(21)申请号 201080018079.0
(22)申请日 2010.04.23
(30)优先权数据
PP50024-2009 2009.04.24 SK
(85)PCT国际申请进入国家阶段日
2011.10.24
(86)PCT国际申请的申请数据
PCT/IB2010/051779 2010.04.23
(87)PCT国际申请的公布数据
WO2010/122520 EN 2010.10.28
(73)专利权人 SMK公司
地址 日本东京
(72)发明人 米罗斯拉夫·弗洛赖克
米夏尔·马萨里克
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 武晨燕 迟姗
(51)Int.Cl.
*G06Q 20/20*(2012.01)
*G06Q 20/32*(2012.01)
(56)对比文件
CN 1484803 A,2004.03.24,
CN 101313329 A,2008.11.26,
US 2007145123 A1,2007.06.28,
审查员 张旭光

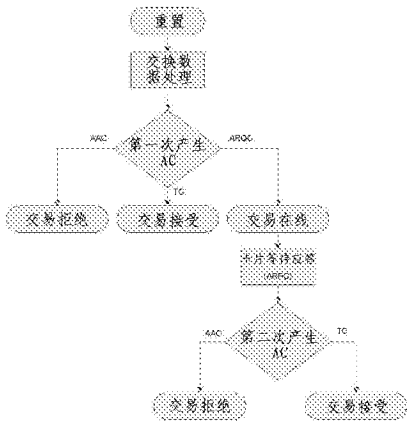
权利要求书2页 说明书7页 附图5页

(54)发明名称

尤其是利用非接触式支付装置的电子支付交易的方法和系统

(57)摘要

一种电子支付交易的方法，其特征在于下述事实，即在一次支付交易处理期间，中断卡片(1)和终端(2)之间的通信链路(3)，并在中断原始通信链路(5)之后，由卡片(1)接收ARPC应答文件。通过卡片(1)的重置将两个阶段分开，其中在第二阶段中使用初始支付数据(ARQC)。在卡片(1)的存储器中存储电子签名的ARQC支付文件，至少持续到接收和处理ARPC应答文件的相应时间。该解决方案能够将具有支付卡(1)的移动电话放置在终端(2)的读卡器附近两次。在第一次，产生在线授权的请求，在第二次接触时，将支付处理器(5)的信息记录在支付应用中。




CN 102640176 B

1. 一种使用了非接触式支付装置的电子支付交易方法，包括一个过程，在该过程中，由支付卡片 (1) 产生 ARQC 形式的支付文件并利用 CDOL 形式的支付数据在支付卡片 (1) 上进行电子签名，在支付卡片 (1) 重置之后从支付终端 (2) 接收支付数据，所述支付文件在支付卡片 (1) 和支付终端 (2) 的通信链路 (3) 上传送至支付处理器 (5)，随后所述支付卡片 (1) 从所述支付处理器 (5) 接收回应答文件，其是 ARPC 型，其编码形式包含有关支付文件的数据，所述支付卡片 (1) 处理应答文件，接下来限定和向支付终端 (2) 发送 TC 或 AAC 形式的支付接受或拒绝声明，其特征在于下述事实，即在一次支付交易处理期间，所述支付卡片 (1) 和支付终端 (2) 之间的通信链路 (3) 中断，所述支付卡片 (1) 和支付终端 (2) 之间的通信链路 (3) 中断之后，在支付卡片 (1) 上从支付处理器 (5) 接收应答文件；其中支付卡片的重置将支付交易处理的两个阶段分隔，以至于在第二阶段使用在通信链路 (3) 中断之前在支付卡片 (1) 上产生的数据，由此支付卡片 (1) 将来自第一阶段的原始产生并存储的支付文件与第二阶段中包括在应答文件中的支付文件进行比较。

2. 如权利要求 1 所述的电子支付交易方法，其特征在于下述事实，即 ARQC 形式的电子签名支付文件存储在支付卡片 (1) 的存储器中，至少持续到从支付处理器 (5) 接收相应的 ARPC 形式的应答文件，所述支付卡片 (1) 解码接收的应答文件，并获得有关支付文件的信息，所述信息用于产生应答文件，并且随后所述支付卡片 (1) 产生支付的接受或拒绝声明。

3. 如权利要求 2 所述的电子支付交易方法，其特征在于下述事实，所述支付卡片 (1) 将存储在支付卡片 (1) 上原始产生的支付文件和包含在应答文件中的支付文件进行比较。

4. 如权利要求 1 至 3 中任一项所述的电子支付交易方法，其特征在于下述事实，即原始产生并在支付卡片 (1) 上存储的支付文件与应答文件内的支付文件相同的情况下，在支付卡片 (1) 上产生支付的同意声明。

5. 如权利要求 1 至 3 中任一项所述的电子支付交易方法，其特征在于下述事实，即在接收应答文件之后，所述支付终端 (2) 需要恢复所述支付卡片 (1) 和支付终端 (2) 之间的通信链路 (3)，其中在恢复所述支付卡片 (1) 和支付终端 (2) 之间的通信链路 (3) 之后，所述支付卡片 (1) 请求支付终端 (2) 再次发送由支付处理器 (5) 的应答作为补充的支付数据。

6. 如权利要求 1 至 3 中任一项所述的电子支付交易方法，其特征在于下述事实，即所述支付卡片 (1) 包含在移动通信设备 (4) 的可移动存储卡中。

7. 如权利要求 1 所述的电子支付交易方法，其特征在于下述事实，即用于传送应答文件的通信路径 (6) 与用于在支付卡片 (1) 和支付终端 (2) 之间传送支付文件的通信链路 (3) 不同。

8. 如权利要求 1 至 3 中任一项所述的电子支付交易方法，其特征在于下述事实，即从所述支付处理器 (5) 接收应答文件之后，所述支付终端 (2) 在第二阶段与支付卡片 (1) 接触，作为一个支付终端 (2)，该支付终端具有的标识与支付终端 (2) 在向支付处理器 (5) 发送支付文件阶段中的标识不同。

9. 如权利要求 8 所述的电子支付交易方法，其特征在于下述事实，即所述支付终端 (2) 存储应答文件，准备用于恢复和所述支付卡片 (1) 的通信链路 (3)。

10. 如权利要求 1 至 3 中任一项所述的电子支付交易方法，其特征在于下述事实，即移动通信网络用于发送所述应答文件，所述支付卡片 (1) 在移动通信设备 (4) 上接收应答文件，其中所述移动通信设备接收 SMS 形式的消息。

11. 如权利要求 6 所述的电子支付交易方法，其特征在于下述事实，所述可移动存储卡是微 SD 或迷你 SD 或 SD 型的。

12. 如权利要求 6 所述的电子支付交易方法，其特征在于下述事实，即用于传送应答文件的通信路径 (6) 与用于在支付卡片 (1) 和支付终端 (2) 之间传送支付文件的通信链路 (3) 不同。

13. 一种使用了非接触式支付装置的电子支付交易系统，包括移动通信设备 (4) 中的支付卡片 (1)、支付终端 (2) 以及所述支付终端 (2) 和支付处理器 (5) 之间的连接，其特征在于下述事实，所述支付卡片 (1) 包括具有存储支付文件的存储器，其中在中断所述支付卡片 (1) 和所述支付终端 (2) 之间的通信链路 (3) 后支付卡片 (1) 重置，之后，所述支付文件也存储在存储器中，其中所述支付终端 (2) 包括用于暂时存储 ARPC 形式的应答文件的存储器，在接收应答文件后，调整所述支付终端 (2) 用于改变其登记标识数据，由此当支付终端 (2) 带有与第一阶段的支付终端 (2) 的标识不同的标识时，支付终端 (2) 在第二阶段登录支付卡片 (1)。

14. 如权利要求 13 所述的电子支付交易系统，其特征在于下述事实，即用于存储支付文件的支付卡片 (1) 的存储器是安全元件。

15. 如权利要求 13 或 14 所述的电子支付交易系统，其特征在于下述事实，即所述支付卡片 (1) 包含在移动通信设备 (4) 的可移动存储卡中。

16. 如权利要求 13 或 14 所述的电子支付交易系统，其特征在于下述事实，即所述支付卡片 (1) 包括用于和所述支付终端 (2) 通信的非接触式通信元件 (7)。

17. 如权利要求 15 所述的电子支付交易系统，其特征在于下述事实，所述可移动存储卡是微 SD 或迷你 SD 或 SD 型的。

# 尤其是利用非接触式支付装置的电子支付交易的方法和系统

## 技术领域

[0001] 本发明涉及一种电子支付应用的过程和系统，其中该电子支付应用使用支付卡形式的支付装置。它涉及一种利用非接触式支付装置的直接借记支付交易的方法，其中调整该非接触式支付装置从而其可以插入移动通信设备中。

## 背景技术

[0002] 销售点 (POS) 终端通常用于利用不同的芯片支付卡处理电子支付交易。这些终端连接至远程支付处理器，其中该处理器是属于支付卡发行商或银行的结算中心的形式。在支付过程开始时，支付卡的芯片重置到其初始位置中。重置后，在卡片和终端之间交换有关卡片和终端类型的信息。这些基本识别将卡片和终端之间的连接带入允许相互通信和与支付处理服务器通信的位置。

[0003] POS 终端将所需支付的数据发送至卡片内，数据结构例如包括数量，现金，日期和类似信息。该终端也请求卡片给出声明。卡片根据其设置产生应答，并签署其电子签名。“TC”（交易证书）形式的卡片响应表示接受离线支付，不需要支付处理器的授权。“AAC”（应用授权密文）形式的响应表示在任何情况下，卡片都不接受支付。本发明的主题是在产生 ARQC（授权请求密文）形式的响应期间，支付过程的方法和过程。该应答表示卡片需要授权以及和支付处理服务器的合作。

[0004] 在产生主要是 ARQC 型支付文件的形式的应答后，卡片将该加密的支付文件发送至处理器并等待至接收处理器的应答。在等待时，支付卡必须和终端保持接触以产生卡片和支付处理器之间连续的通信通道。该通道的中断将引起支付过程的终止。如果支付处理器向卡片返回 ARPC 响应文件（授权响应密文），那么该文件通过终端发送至支付卡中，支付卡将来自响应文件的指令解码用于进一步过程（尤其用作 ARPC），并将结果以 TC 最终是 AAC 的形式向终端汇报。

[0005] 支付卡和迄今为止公知的终端 / 支付处理器之间的通信方法的实质特征是恒定的连接，在双向通信期间给定的非现金式支付硬件元件的连续的不中断通道。该通信大约持续几秒，最后是十分之几秒。卡片和终端之间的连接的中断引起卡片应用的新启动，这将例如经由其计算器的增加而记录。计算器数据的改变将引出新产生的支付文件 ARQC 的变化，并且在中断之后，它不可能利用在连接中断之前原始产生的数据成功完成支付过程。当利用通过接触连接的标准支付卡时，由于仅在卡片提早从恰当的读卡器槽中取出的情况下该连接中断，因此保持可靠的通信链路没有问题。

[0006] 随着非接触式支付装置的使用的增加，在通信通道的稳定性上出现了问题。要求付款人一直拿着他的非接触式支付装置，并在整个支付过程中将该装置置于非接触式读卡器可到达的范围内是不合适的。为了防止其他设备的任何干扰，非接触式读卡器通常具有有限的到达范围，以降低产生非接触场所需的能量，并降低安全风险。需要一种将支付通信过程划分为几个中断的阶段的解决方案。但是，直到现在，还没有满足该需求的过程和方

法。

[0007] 使用一种解决方案，在该方案中，非接触式支付卡也适用于和终端的接触连接。在该结构中，大多数支付通过支付卡和终端之间的非接触式链路实现，在此期间，支付卡不用等待支付处理器的响应。为了实现卡片和支付处理服务器之间的双向通信，卡片有必要和终端有规律的，例如每隔十次支付，接触连接。然后，卡片从支付处理器接收指令并执行指令。该结构降低了用户的舒适度，并且最重要的是它需要支付卡的接触面，它不适合使用移动通信设备内支付卡的支付。不可能要求不同的移动通信设备，例如移动电话以接触的方式连接至 POS 终端。

## 发明内容

[0008] 通过一种非接触式支付交易的方法，尤其是利用了非接触式支付装置，可以显著消除上述缺点。其包括一种方法，通过该方法，在卡片重置后，卡片从支付终端接收支付数据。基于这些数据，产生主要是 ARQC 形式的支付文件并进行电子签名。该支付文件经由卡片和支付终端之间的链路发送至支付处理器，随后卡片接收回来自处理器的响应文件，主要是 ARPC 形式，其包括有关编码形式的原始支付文件的连贯数据。该卡片将处理和解码响应文件，并随后决定，限定并根据本发明主要以 TC 或 AAC 形式向终端回送支付的肯定性或否定性声明。本发明的主题在于下述事实 :在处理一个支付交易期间，中断卡片和终端之间的通信链路。在从卡片向终端发送支付文件后，基本上立即产生该中断。从终端初始接收数据，产生 ARQC 形式的支付文件，并发送至终端大约持续几毫秒，这在将卡片轻松的放置在终端读卡器附近期间是可实现的。在卡片和终端之间的原始通信链路中断之后，由卡片接收支付处理器的响应文件。上述的支付交易处理和通信的两个阶段由卡片重置划分，而在第二阶段，使用在卡片和终端之间的通信链路中断之前在卡片上产生的数据。在一次支付交易期间，由通信链路的再建立来引起卡片新的重置。

[0009] 上述通信机制可以以安全的方式实现，同时对于公共 EMV(Europay，MasterCard，VISA) 的过程很少有干涉，使得电子签名的支付文件，尤其是 ARQC 形式的存储在卡片的存储器中，而支付文件存储在存储器中至少直到从支付处理器接收和进行特殊的应答文件的时间，主要作为ARPC的时间。尤其作为ARQC存储支付文件，是提交的解决方案的实质特征，这是由于其允许以这样的方式将支付交易的过程分为几个阶段，即引起第二阶段的中断和过程不会导致进行中的支付交易的消除和关闭。

[0010] 卡片解码接收的应答文件，获得有关支付文件的信息，其中在应答文件产生期间支付处理器使用该信息。在应答文件中编码 ARQC 支付文件，并且在该应答文件中可以存储用于卡片的其他指令和脚本。该卡片将原始产生和存储的支付文件与包含在应答文件中的支付文件做比较，随后该卡片产生支付的拒绝或接受声明。在原始产生并在卡片上存储的支付文件和从解码的应答文件中产生的支付文件相同的情况下，支付的接受声明位于卡片上。这意味着在第二处理阶段，除了其他操作，卡片也将存储的 ARQC 文件和 ARQC 文件做比较，这用作支付处理器产生 ARPC 的基础。

[0011] 接收应答文件之后，终端需要卡片和终端之间的通信链路再连接。在重新建立卡片和终端之间的通信链路后，卡片需要从终端再发送 CDOL( 卡片风险管理数据对象表 ) 形式的支付数据，其与由支付处理器应答作为补充的原始的 CDOL 比较。

[0012] 如果支付卡片包含在移动通信设备，例如移动电话中，它是有利的。从该支付装置可扩展的角度来看，如果支付卡位于微 SD 或迷你 SD 或 SD 型的存储卡中，由于移动电话通常具有加入扩展存储卡的槽，因此，它比较恰当。

[0013] 在现有单阶段通信系统中，在支付交易期间，从支付处理器向卡片的反向通信总是通过和支付文件发送至支付处理器时使用的相同的通信通道实现。具有两个阶段的新方法可以将这些阶段不仅从时间的角度划分，而且从硬件角度划分。可以使用不同于传送支付文件所使用的通信路径，来传送应答文件。其可以是经由移动通信网络的连接，包含卡片的移动通信设备登陆该网络。移动通信网络用于发送应答文件，应答文件通过移动电话进入卡片中，其中该移动电话接收 SMS 形式的应答文件。但是这在终端接收应答文件之后、在终端和卡片之间的通信链路没有在预定的时间期限内重新建立时发生。那么终端在该状态向支付处理器发送信息，并且组织将应答文件以不同形式发送至卡片中。

[0014] 在使用经由 POS 终端相同的通信路径的情况下，它是恰当的，即该终端在从支付处理器接收应答文件之后登陆卡片，该终端作为具有与支付文件发送至支付处理器时的阶段中支付终端标识不同的标识的终端。基本上，它意味着具有不同标识前缀的终端给卡片一个信号，即它试图作为后处理终端连接，用以完成已经启动的支付交易。在这种结构中，终端保持应答文件，用于准备和卡片再次建立通信链路。

[0015] 通过一种非接触式支付交易方法，尤其使用了非接触式支付设备，也可以显著消除本技术现状的缺陷，其中该非接触式支付设备包括根据本发明的支付卡，终端，终端和支付处理器之间的连接。本发明的主题也在于下述事实：支付卡配有用于存储支付文件，优选是 ARQC 形式的支付文件的存储器，其中当卡片和终端之间的通信链路终止时，即使在卡片重置之后，支付文件也存储在存储器中。该终端配有存储器，用于暂时存储主要是 ARPC 形式的应答文件，并调整该存储器以在接收应答文件之后改变其标识数据。从达到所需的安全性角度来说，用于存储支付文件的卡片的存储器是安全元件的形式是很有必要的。

[0016] 在有利的结构中，设置该系统使得支付卡在移动通信设备内，优选在微 SD 或迷你 SD 或 SD 形式的存储卡中，其中该存储器卡包括用于和终端连接的通信元件。借此，实现移动电话的更新，不仅用于支付卡载体或者各种支付卡载体的功能，而且用于在移动电话和终端之间产生通信通道。该通信将主要根据 NFC 标准运行。

## 附图说明

[0017] 图 1 至 5 更详细的描述了本发明，其中图 1 示出了电子支付交易的现有方法和连接的算法。图 2 示出了具有两个单独的处理电子支付应用的阶段的算法。

[0018] 图 3 代表一种用于移动电话上非接触式，直接借记交易的系统连接方案，其中该移动电话配有插入存储器卡上的支付卡，并且该存储器卡在第一阶段具有天线，所以处于预处理。以从上至下的顺序示出了命令过程和文件流。

[0019] 在图 4 中，具有与根据图 3 的方案相关的连接方案，其中示出了经由终端，在卡片上传送的第二阶段后处理。以从上至下的顺序示出了命令过程和文件流。

[0020] 在图 5 中，具有与图 3 中的方案相关的连接方案，但是这里示出了第二阶段，在 SMS 消息上 APRC 传送形式的后处理。以从上至下的顺序示出了命令过程和文件流。

[0021] 相关符号列表

[0022] 1- 卡片

[0023] 2- 支付终端

[0024] 3- 通信链路

[0025] 4- 移动通信设备

[0026] 5- 支付处理器

[0027] 6- 通信路径

[0028] 7- 通信元件

[0029] POS- 销售点

[0030] AAC- 应用授权密文

[0031] ARQC- 授权请求密文

[0032] ARPC- 授权响应密文

[0033] CDOL- 卡片风险管理数据对象列表

[0034] TC- 交易证书

[0035] POS 12- 由销售商管理的销售点

[0036] POS 12tc2- 由销售商在后处理中管理的销售点 - 具有不同的终端容量

[0037] EMV-Europay，MasterCard，VISA

## 具体实施方式

[0038] 示例 1

[0039] 在该示例中，该系统包括移动通信设备 4，具有 NFC 读卡器的终端 2，支付处理服务器 5，终端 2 和支付处理服务器 5 之间的连接。该移动通信设备 4 例如由 NOKIA 6131 移动电话表示。具有微 SD 格式存储器的可移动卡片 1 插入移动通信设备 4 的槽中。支付卡 1 和 NFC 通信元件 7 位于可移动卡片 1 上，其中该可移动卡片具有通用标准尺寸的存储器。卡片 1 配有用于存储支付文件的存储器，安全元件的形式的存储器，分别具有安全元件的实际范围的形状。即使在卡片 1 重置后 ARQC 支付文件也存储于其中。在交易第一阶段中，中断卡片 1 和终端 2 之间的通信链路 3 之后，通过将卡片 1 再连接至终端 2，引起卡片 1 重置。终端 2 配有用于暂时存储，尤其是 ARPC 形式的应答文件的存储器。终端 2 具有可变标识前缀；在接收应答文件之后，调整终端 2 以改变其识别数据。在第一阶段，终端 2 记录为 12 型终端 2（由销售员管理 POS 终端 2），在第二阶段，终端 2 记录为 12tc2 型或者可能是 27 型（后处理终端 (Post_Process_Terminal)）终端 2。终端类型的改变用于校正通信消息的匹配，原则上它可是新型号的终端，例如 27。在其他情况下，当在现有处理系统中引入终端的新型号出现问题时，可以使用型号相同的 12 和不同的终端容量，这里表示为 12tc2 ＝具有不同 tc- 终端容量的 12。终端 2 具有存储器用于存储应答文件 APRC，准备用于实现通信链路 3 和卡片 1 再连接。

[0040] 在终端 2 中准备有关所需支付的数据，包括数量，货币和日期。这些包含在 CDOL1 数据（卡片风险管理数据对象列表）中。用户将其移动电话置于终端 2 的读卡器。在产生通信链路 3 之后，终端 2 向卡片 1 请求声明。基于接收的数据，卡片 1 产生 ARQC 密文形式的支付文件。该文件由卡片 1 的电子签名编码。在原始产生通信链路 3 期间，将支付文件 ARQC 传送至终端 2。在其产生后，ARQC 支付文件存储在卡片 1 的安全元件中。将 ARQC 支

付文件传送至终端 2 之后，无论移动电话从终端 2 的读卡器移除或不移除，基本上都没有什么关系。假设在整个支付交易期间，由于用户手拿移动电话，电话会移除。移动电话在终端 2 的请求下，或者实际上在监视支付交易整个过程的服务员的请求下，放置在终端 2 的读卡器附近。在第一次放置后，用户等待另一次放置的请求。当一个支付交易在进行中时，卡片 1 和终端 2 之间的通信链路 3 断开。

[0041] 同时，ARQC 支付文件从终端 2 发送至支付处理器 5。支付处理器处理并评估它，并和其他可能的指令一起将 ARQC 支付文件解码为 ARPC 密文形式的应答文件。该文件包括有关 ARQC 支付文件的解码数据。在卡片 1 和终端 2 之间的原始通信链路 3 中断之后，卡片 1 从支付处理器 5 接收 ARPC 应答文件。该中断包括暂时的时间元素，其分隔支付交易处理的第一和第二阶段。从卡片 1 的观点来看，这两个阶段由被卡片 1 被重置分隔，而第二阶段使用第一阶段在卡片上产生的数据。

[0042] ARQC 支付文件存储在卡片 1 的存储器中至少持续到接收和处理来自支付处理器 5 的特殊的 ARPC 应答文件的时刻。卡片 1 解码接收的 ARPC 应答文件，获得有关 ARQC 支付文件的信息，其中在产生 ARPC 应答文件时，支付处理器 5 使用该有关 ARQC 支付文件的信息。接下来，卡片 1 将原始产生和存储的 ARQC 支付文件和包含在 ARPC 应答文件中的 ARQC 支付文件做比较。在该比较后，卡片 1 对其声明做出决定，其中该声明有关正在进行的支付。随后，卡片 1 产生 TC 或 AAC 形式的支付的接受或拒绝声明。当原始产生并存储在卡片 1 上的 ARQC 支付文件与包含在 ARPC 应答文件中的 ARQC 支付文件相同时，在必要的情况下，在卡片 1 上产生接受声明。

[0043] 在该示例中所述的连接也提供如何将 ARPC 应答文件传送至卡片 1 更多可能的方式。如果终端 2 向支付处理器 5 汇报用户没有第二次将其移动电话放置在终端 2 的读卡器的附近，那么支付处理器 5 会试着将 ARPC 作为 SMS 数据发送至分配给该特殊支付卡 1 的电话号码上。在移动电话中，作为与插入的微 SD 卡相关的数据，分析接收的 SMS，并将其自己的通用的，基本上虚拟的 POS 终端 2 的启动初始化。SMS 消息包含有关终端 2 的信息，其中该终端 2 属于具有前缀 17 的支付处理器 5（属于支付处理器 5 的后处理终端 2）。

[0044] 示例 2

[0045] 分两个步骤实现在线支付交易的过程 - 预处理和后处理。可以将完成例如 PAYPASS 和 PAYWAVE 规范的非接触式应用用作支付应用。在卡片 1 上具有两个单独的应用 -PAYPASS/PAYWAVE 和 PAYPASS/PAYWAVE_POSTPROCESS。这些应用位于一个安全域中，并且是 EMV 兼容的，虽然它们至少共用三个公共变量（数据元素）：离线计数器，应用交易计数器 (ATC)，最后一次在线应用交易计数器 (LATC)。应用 PAYPASS/PAYWAVE 临时存储 ARQC 值，其后来在 POSTPROCESS 中提供至 PAYPASS/PAYWAVE_POSTPROCESS，因此，这个不必再重数一次，从而节约了时间。根据本发明，引入了新型终端 2 :Terminal_Type = 27(POST PROCESS TERMINAL 2)。

[0046] 提供的解决方案能够将移动电话放置在终端 2 附近两次。在第一次，产生在线授权的请求，在第二次接触之后，来自支付处理器 5 的信息进入支付应用。如果用户没有第二次放置他的移动电话，但是相关的数据或脚本在应答内，那么终端 2 向支付处理器 5 报告没有传送应答，支付处理器 5 将试着再经由 SMS 向移动电话传送一次 - 在 SMS 响应 (SMS RESPONSE) 服务激活的情况下。在用户拥有该服务时，他可以欣然地并且规律地仅将其移动

电话放置在终端 2 的读卡器一次。当 GUI 经由 SMS 向支付处理器 5 报告 SMS REPORT 使能时，在第一次安装 GUI 期间，激活该服务。

[0047] 在支付处理器 5 发送 SMS RESPONSE 之后，没有接收到其接收了三个连续的在线支付的确认时，那么该服务自动失效。顾客连续在线支付 3 次和 / 或 GUI 没有激活，或者顾客的移动电话变为不支持该服务的类型。在失去激活之后，顾客接收 SMS，说明他必须在 GUI 上再次激活该服务或者利用支付交易过程的双接触方法。

[0048] 在该示例中，预处理代表在卡片 1 第一次放置，即将移动电话放置在终端 2 的读卡器时实现的公共的在线非接触式操作。在预处理期间，终端 2 将其自身表示为例如 Terminal_type ＝ 12（由销售商管理的 POS 终端 2）。终端 2 将在线授权的请求发送至支付处理器 5（用于发放支付卡片 1 的银行的授权服务器）。除此之外，预处理的结果是来自支付处理器的答复代码 (Response_code) 和脚本 (Script)。

[0049] 用户在移动电话中启动 GUI 支付应用。该应用需要密码。如果应用了密码，那么 EMBEDDED POS TERMINAL 使用密码进入 PIN 码。该 PIN 码存储在安全元件的单独应用中。EMBEDDED POS TERMINAL 校验 PAYPASS/PAYWAVE 应用中的 PIN，如果其有效，其构造支付应用使得在交易期间，不需要在外部 POS 终端 2 的 PIN 输入设备 (PED) 上的 PIN 的额外校验。由该结构限定了 PIN OVER PASSWORD 平台技术。如果用户启动了支付应用，但是没有输入密码，并且终端 2 需要 PIN 校验，则需要在 PED 上输入 PIN 或者将 FOB（外部数据载体）放置在读卡器附近，并将其发送至支付处理器 5 用于校验。如果电话不配有 GUI 支付应用，并且终端 2 需要 PIN 校验，那么校验在支付处理器 5 上在线完成。

[0050] 终端 2 向卡片 1 发送卡片风险管理数据对象列表 (CDOL1) 和第一次产生 AC(GENERATE AC) 命令。卡片 1 计算 ARQC。如果终端 2 的风险管理需要 PIN，并且在 GUI 上没有输入密码，那么终端 2 需要在 PIN 输入设备 (PED) 上输入 PIN。在该步骤，它在线校验 PIN。终端 2 将计算的 ARQC 密文作为在线授权的请求发送至支付处理器 5。支付处理器 5 回送用于补充 Response_code 和 Script 的应答 (ARPC 密文）。

[0051] 当终端 2 按照下述向卡片 1 发送用于接下来的处理的 Response_code 和 Script 时，在将卡片第二次放置在终端 2 附近期间运行后处理：

[0052] 1、在终端 2 从支付处理器（预处理的结束）接收 ARPC 密文后，终端要求用户再次将卡片 1，移动电话放置在终端的非接触式读卡器附近。

[0053] 2、在放置卡片 1 之后，终端 2 激活 PAYPASS/PAYWAVE_POSTPROCESS，并且其自身不表示为 Terminal_type ＝ 12，而是表示为 Terminal_type ＝ 27（由销售商管理的后处理终端），单独表示为 Terminal_type ＝ 12tc2

[0054] 3、卡片识别该类型终端（它在双接触交易处理中），并向终端 2 询问 CDOL2 数据以计算第二次 GENERATE AC。

[0055] 4、除了其他数据之外，来自终端 2 的 CDOL2 必须包含来自支付处理器的 Response_code。

[0056] 5、终端 2 向卡片 1 发送 Script。

[0057] 6、在计算 ARQC 期间使用，其在预处理期间暂时被存储。

[0058] 7、卡片向终端 2 发送计算的 TC/AAC。

[0059] 如果用户没有第二次将他的移动电话，移动通信设备 4 放置在读卡器上，那么终

端将向支付处理器 5 报告消息发送未成功。支付处理器将试着将 ARPC 作为 SMS 数据发送至 SD 卡 1 插入的电话号码中（在从激活 GUI 的 SMS 激活 SMS Response 期间，处理器 5 获得并记住该电话号码）。下发 SMS 技术记录接收的 SMS，在发现其包含 SD 卡的相关数据后，它运行 GENERIC POS TERMINAL。除了其他信息之外，SMS 数据必须包括有关 Ternimal_type ＝ 17（属于金融机构的后处理终端 2）的信息。GENERIC POS TERMINAL 在安全元件上读取默认终端的结构数据（终端 2 属于支付处理器 5 或者属于和支付处理器 5 合作的支付处理器）。随后，EMBEDDED POS TERMINAL 启动 PAYPASS/PAYWAVE_POSTPROCESS 并将自身表示为 Ternimal_type ＝ 17。卡片 1 识别该终端的类型（它在双接触交易处理平台上），并向终端 2 询问 CDOL2 数据（包含 ARPC），以计算第二个 GENERATE AC。终端 2 向卡片 1 发送 Script。在预处理期间临时存储的 ARQC 用于随后的计算。卡片 1 将计算的 TC/AAC 作为应答发送至终端 2。终端 2 解码应答，并将其存储在存储器中，在那由 GUI 接管并将其作为应答发送至支付的处理器 5 的 HOST，然而其从接收的 SMS RESPONSE 识别电话号码。

[0060] 当卡片 1 从支付处理器 5 接收 ARPC 时，其设置 LATC，使得其能够实现其他“n”个（未限制）的离线支付，无论其在 SMS Response 上还是在第二次接触上都没有关系。如果用户在双接触平台拒绝第二次接触和 / 或 SMS Response 没有激活，那么他不能实现离线支付。但是，他仍可以支付但只能在支付处理器 5 在线授权。在正确从支付处理器 5 接收 ARPC（响应）之后，允许离线交易。然后，通常在用户卡上具有足够的离线资金的情况下，允许该用户再次无限次支付。

[0061] 工业实用性

[0062] 工业实用性是显而易见的。根据该本发明，可以产生并使用电子支付应用的系统，在该系统，支付交易可以分为两个阶段，其可以在卡片和终端之间的通信链路产生中断。

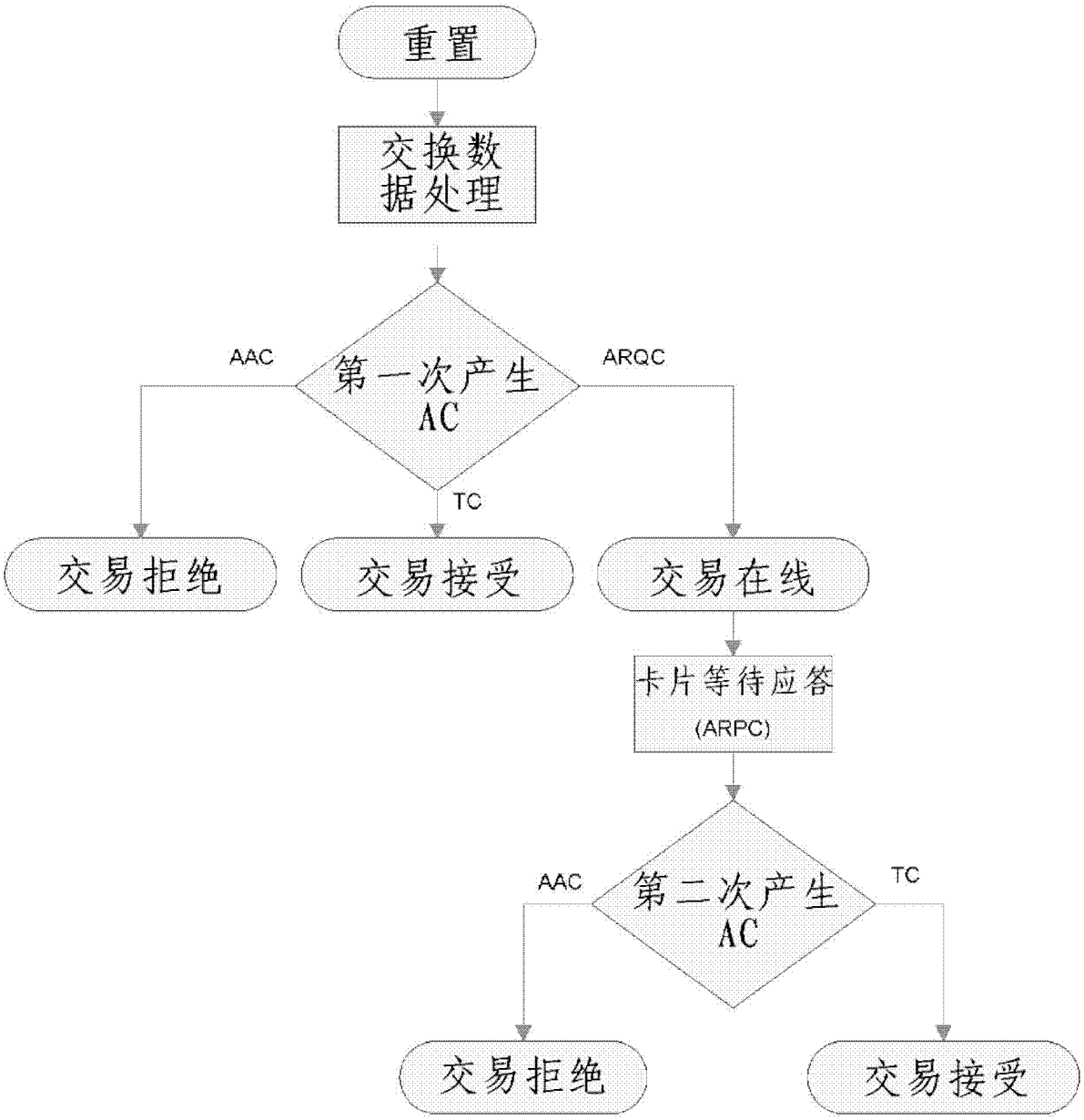

重置
交换数据处理
第一次产生AC
AAC
ARQC
TC
交易拒绝
交易接受
交易在线
卡片等待应答(ARPC)
第二次产生AC
AAC
TC
交易拒绝
交易接受

图 1

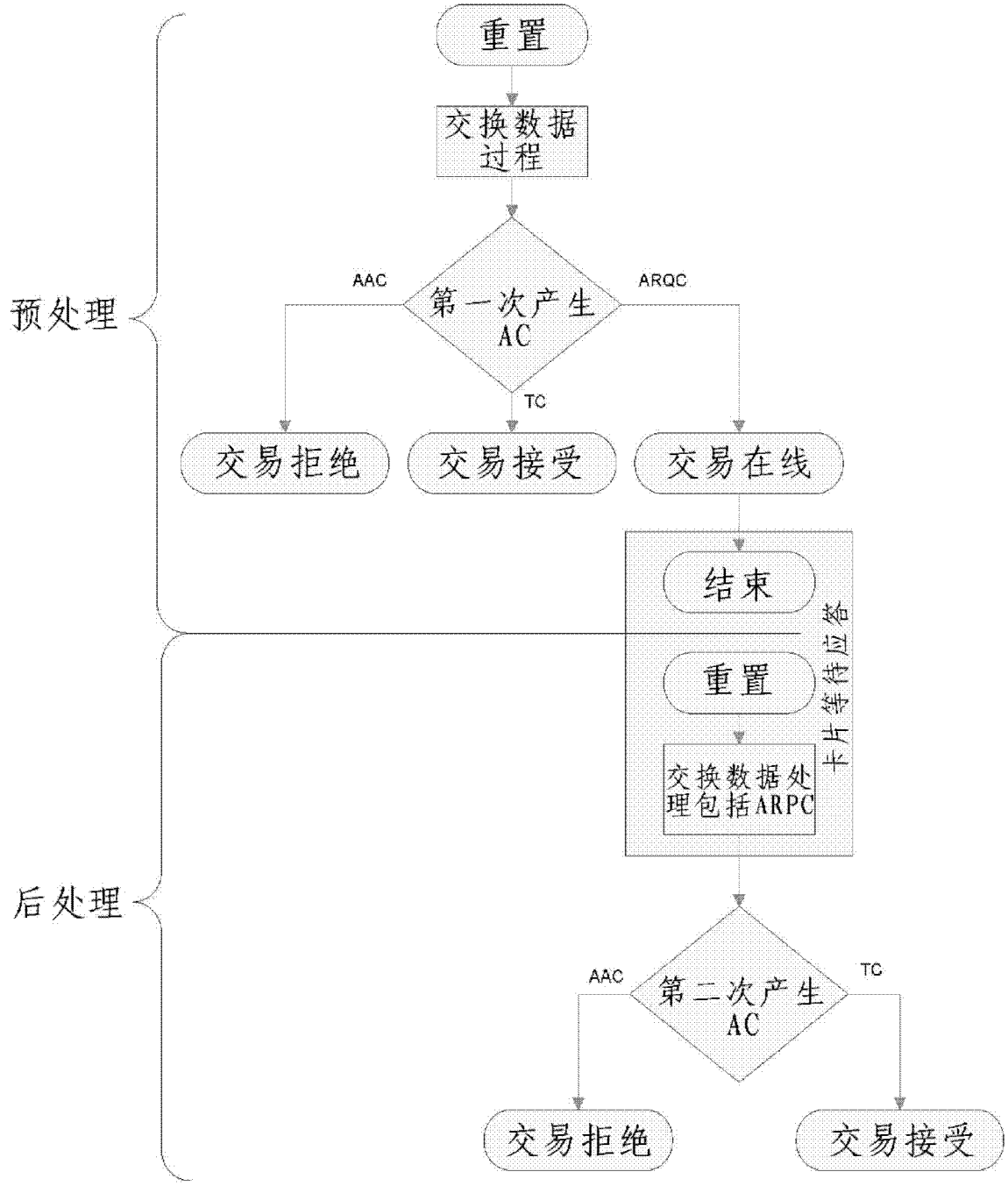

预处理
重置
交换数据过程
第一次产生AC
AAC
ARQC
TC
交易拒绝
交易接受
交易在线
卡片等待应答
结束
重置
交换数据处理包括ARPC
后处理
第二次产生AC
AAC
TC
交易拒绝
交易接受

图 2

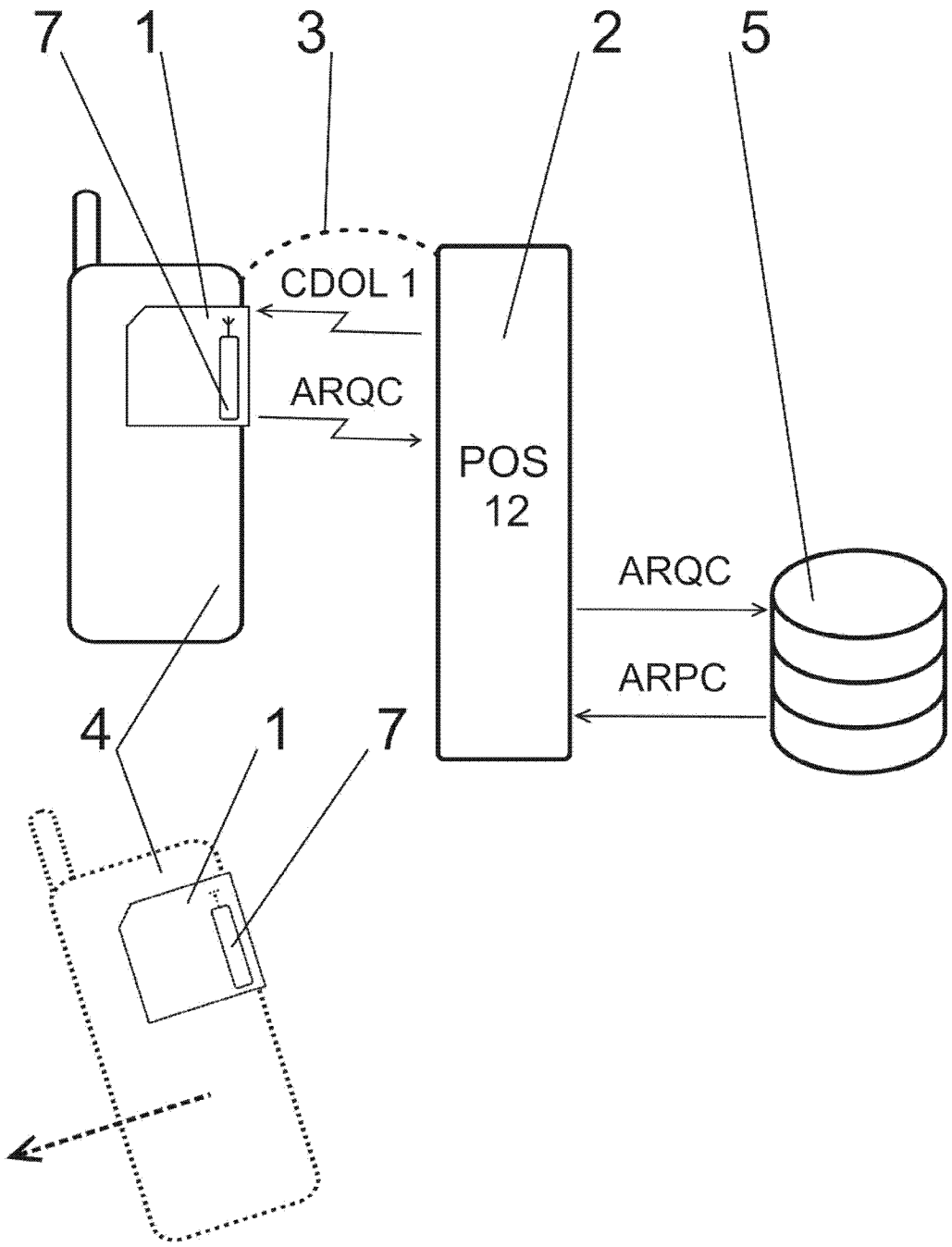



图 3

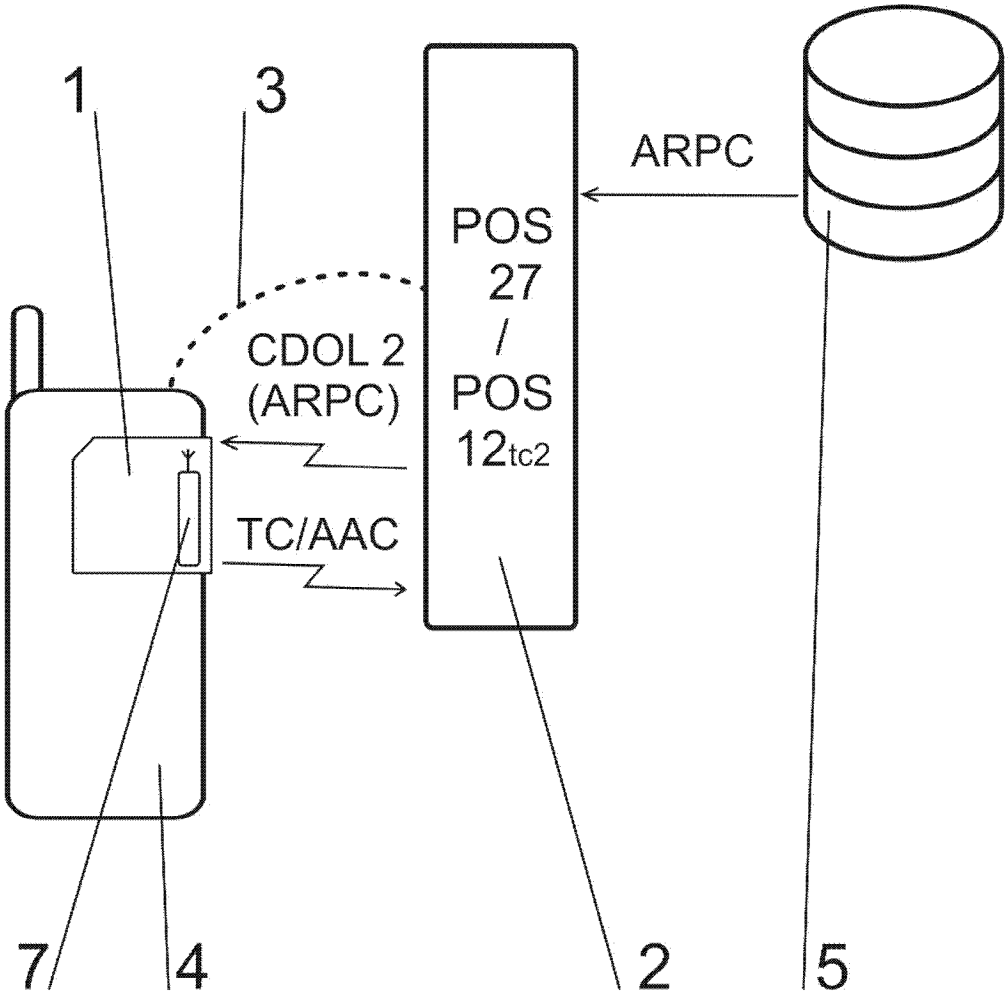



图 4

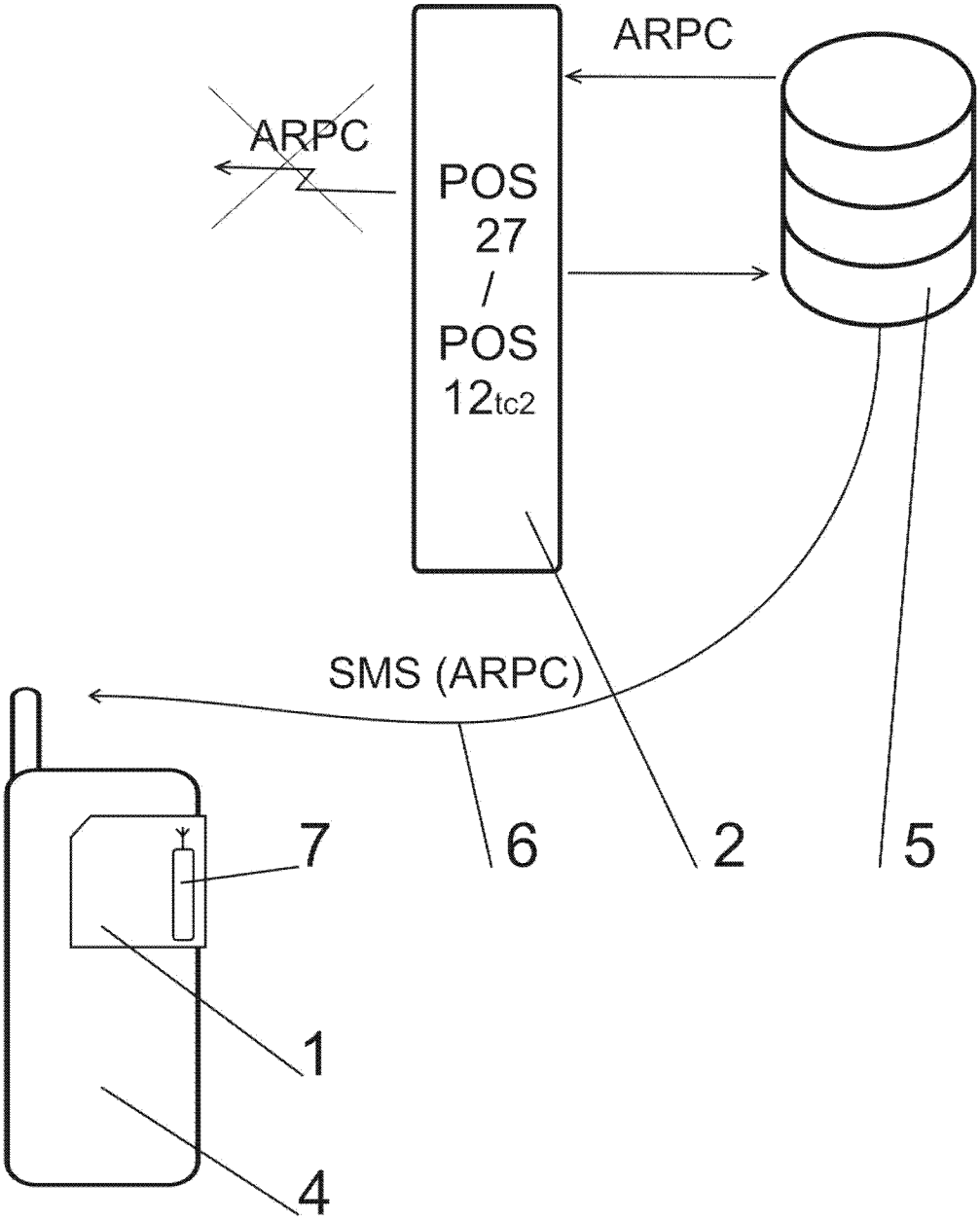



图 5