



(12)发明专利

(10)授权公告号 CN 104486323 B

(45)授权公告日 2017. 10. 31

(21)申请号 201410755617.4

(22)申请日 2014.12.10

(65)同一申请的已公布的文献号
申请公布号 CN 104486323 A

(43)申请公布日 2015.04.01

(73)专利权人 福建联迪商用设备有限公司
地址 350003 福建省福州市软件大道89号
福州软件园一区23号楼

(72)发明人 洪逸轩 苏文龙 孟陆强 林建群

(74)专利代理机构 福州市博深专利事务所(普通合伙) 35214

代理人 林志峥

(51) Int. Cl.
H04L 29/06(2006.01)

(56)对比文件

CN 104410641 A, 2015.03.13,
US 2007283151 A1, 2007.12.06,
CN 1041559289 A, 2014.11.19,
CN 103595718 A, 2014.02.19,
CN 103716167 A, 2014.04.09,

审查员 马旗超

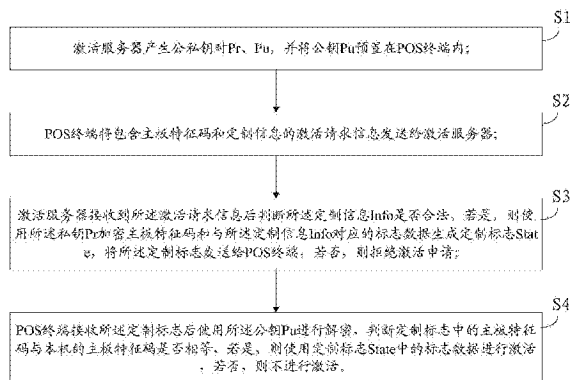
权利要求书1页 说明书5页 附图4页

(54)发明名称

一种POS终端安全受控的联网激活方法及装置

(57)摘要

本发明公开一种POS终端安全受控的联网激活方法,包括:激活服务器产生公私钥对Pr、Pu,将公钥Pu预置在POS内;POS将包含主板特征码和定制信息的激活请求信息发送给激活服务器;激活服务器接收到所述激活请求信息后判断所述定制信息是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息对应的标志数据生成定制标志,将所述定制标志发送给POS,若否,则拒绝激活申请;POS接收所述定制标志后使用所述公钥Pu进行解密,判断所述主板特征码与本机的主板特征码是否相等,若是,则使用所述标志数据进行激活,若否,则不进行激活。本发明实现根据客户化定制需求对POS进行激活。本发明还提供一种POS终端安全受控的联网激活装置。



1. 一种POS终端安全受控的联网激活方法,其特征在于,包括以下步骤:

激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

POS终端将包含主板特征码和定制信息的激活请求信息发送给激活服务器;

激活服务器接收到所述激活请求信息后判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息Info对应的标志数据生成定制标志State,将所述定制标志发送给POS终端,若否,则拒绝激活申请;

POS终端接收所述定制标志后使用所述公钥Pu进行解密,判断定制标志中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志State中的标志数据进行激活,若否,则不进行激活。

2. 根据权利要求1所述的POS终端安全受控的联网激活方法,其特征在于,若POS终端使用公钥Pu解密时发生错误,则不进行激活。

3. 根据权利要求2所述的POS终端安全受控的联网激活方法,其特征在于,在POS终端出厂前激活服务器获取POS终端SN码,所述SN为序列号,将所述POS终端SN码和该POS终端的标志数据关联存储于激活服务器内。

4. 根据权利要求3所述的POS终端安全受控的联网激活方法,其特征在于,所述激活请求信息还包括POS终端SN码;

激活服务器根据所述POS终端SN码寻找本地数据库中与所述定制信息对应的标志数据。

5. 一种POS终端安全受控的联网激活装置,其特征在于,包括预置模块、请求模块、第一判断模块和第二判断模块;

所述预置模块用于激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

所述请求模块用于POS终端将包含主板特征码和定制信息的激活请求信息发送给激活服务器;

所述第一判断模块用于激活服务器接收到所述激活请求信息后判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息Info对应的标志数据生成定制标志State,将所述定制标志发送给POS终端,若否,则拒绝激活申请;

所述第二判断模块用于POS终端接收所述定制标志后使用所述公钥Pu进行解密,判断定制标志中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志State中的标志数据进行激活,若否,则不进行激活。

6. 根据权利要求5所述的POS终端安全受控的联网激活装置,其特征在于,所述第二判断模块还用于若POS终端使用公钥Pu解密时发生错误,则不进行激活。

7. 根据权利要求6所述的POS终端安全受控的联网激活装置,其特征在于,所述预置模块还用于在POS终端出厂前激活服务器获取POS终端SN码,所述SN为序列号,将所述POS终端SN码和该POS终端的标志数据关联存储于激活服务器内。

8. 根据权利要求7所述的POS终端安全受控的联网激活装置,其特征在于,所述激活请求信息还包括POS终端SN码;

激活服务器根据所述POS终端SN码寻找本地数据库中与所述定制信息对应的标志数据。

一种POS终端安全受控的联网激活方法及装置

技术领域

[0001] 本发明涉及电子支付领域,特别是涉及一种POS终端安全受控的联网激活方法及装置。

背景技术

[0002] 当POS终端出厂时或者受到攻击维修后,POS终端处于非使用状态,此时需要激活才能进入正常的使用状态。由于POS终端客户对POS终端的个性化需求越来越多,随之而来的POS终端客户化定制也越来越多,为了确保在POS终端出厂前和出厂后其状态能够满足客户化定制的需求,需要在POS终端激活时,校验POS信息与客户化定制的需求相同再进行激活操作,因此大大增加了激活的工作量。

发明内容

[0003] 本发明所要解决的技术问题是:提供一种POS终端安全受控的联网激活方法及装置,用于满足根据客户化定制对POS终端进行激活。

[0004] 为了解决上述技术问题,本发明采用的技术方案为:

[0005] 一种POS终端安全受控的联网激活方法,包括以下步骤:

[0006] 激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

[0007] POS终端将包含主板特征码和定制信息Info的激活请求信息发送给激活服务器;

[0008] 激活服务器接收到所述激活请求信息后,判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息Info对应的标志数据生成定制标志State,将所述定制标志State发送给POS终端,若否,则拒绝激活申请;

[0009] POS终端接收所述定制标志State后使用所述公钥Pu进行解密,判断定制标志中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志State中的标志数据进行激活,若否,则不进行激活。

[0010] 为解决上述技术问题,本发明提供的另一技术方案为:

[0011] 一种POS终端安全受控的联网激活装置,包括预置模块、请求模块、第一判断模块和第二判断模块;

[0012] 所述预置模块用于激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

[0013] 所述请求模块用于POS终端将包含主板特征码和定制信息Info的激活请求信息发送给激活服务器;

[0014] 所述第一判断模块用于激活服务器接收到所述激活请求信息后判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息Info对应的标志数据生成定制标志State,将所述定制标志State发送给POS终端,若否,则拒绝激活申请;

[0015] 所述第二判断模块用于POS终端接收所述定制标志State后使用所述公钥Pu进行

解密,判断定制标志State中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志中的标志数据进行激活,若否,则不进行激活。

[0016] 本发明的有益效果在于:区别于现有POS终端无法实现根据客户化定制需求进行联网激活,本发明通过POS终端上传定制信息Info,激活服务端下传对应的标志数据,POS终端根据所述标志数据进行激活,从而实现根据客户化定制需求进行联网激活,并且激活服务器通过验证定制信息Info的合法性和对定制信息Info进行加密处理,POS终端通过验证定制标志中的主板特征码和定制信息Info,确保每个POS终端的定制标志State都不相同,POS终端只能通过激活服务器激活,并且整个激活过程的安全受控性。

附图说明

- [0017] 图1为本发明一实施方式POS终端安全受控的联网激活方法的方法流程图;
- [0018] 图2为本发明一实施方式POS终端安全受控的联网激活装置的功能模块框图;
- [0019] 图3为本发明一实施方式中激活服务器与POS终端的连接关系图;
- [0020] 图4为本发明一实施方式POS终端安全受控的联网激活方法的具体步骤流程图;
- [0021] 图5为本发明一实施方式中状态标志State的数据格式示意图;
- [0022] 图6为本发明一实施方式中POS终端的内部激活流程图;
- [0023] 标号说明:
- [0024] 10、预置模块;20、请求模块;30、第一判断模块;40、第二判断模块。

具体实施方式

[0025] 为详细说明本发明的技术内容、所实现目的及效果,以下结合实施方式并配合附图予以说明。

[0026] 本发明最关键的构思在于:通过由激活服务器产生与POS终端客户化定制对应的定制标志State并下发给POS终端,POS终端使用该定制标志State进行激活,从而实现根据客户化定制需求进行激活。

[0027] 请参照图1,本发明一实施方式为:一种POS终端安全受控的联网激活方法,包括以下步骤:

[0028] 激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

[0029] POS终端将包含主板特征码和定制信息Info的激活请求信息发送给激活服务器;

[0030] 激活服务器接收到所述激活请求信息后判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息Info对应的标志数据生成定制标志State,将所述定制标志State发送给POS终端,若否,则拒绝激活申请;

[0031] POS终端接收所述定制标志State后使用所述公钥Pu进行解密,判断定制标志中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志State中的标志数据进行POS终端激活,若否,则不进行激活。

[0032] 其中,所述标志数据包含该POS终端客户化定制所要求具体的功能和应用程序列表等内容,标志数据存储于激活服务器里,定制信息Info用于表示本POS终端的客户化定制版本信息,所述定制信息Info在POS终端出厂前被注入到POS终端中。所述公私钥对Pr、Pu是在激活服务器中生成,并将公钥Pu注入到POS终端中。主板特征码,是每台POS终端都不相

同,可以唯一标识POS终端设备的标识,从而确保定制标志State每台终端设备都不相同。

[0033] 在POS终端在出厂前,生成与该POS终端客户化定制对应的标志数据,并将所述标志数据与POS终端的序列号SN和主板特征号关联存储于激活服务器内。

[0034] 由以上描述可得,本发明的有益效果为:本发明激活服务器下发与POS终端客户化定制内容相对应的标志数据(即与所述定制信息对应的标志数据),POS终端使用该标志数据进行激活,从而使POS终端激活后满足客户化定制的需要,并且,本发明整个激活过程在POS终端和激活服务器两端各需要进行验证,从而保证满足激活服务器和POS终端的激活条件后才允许激活,使激活整个过程都在安全受控范围内进行。

[0035] 进一步的,在上述实施方式中,若POS终端使用公钥Pu解密时发生错误,则不进行激活。

[0036] 由上述描述可知,当所述公钥Pu解密时发生错误,则说明POS终端所接收到的定制标志State可能不是对应的激活服务器所发送的,本实施方式及时的拒绝该定制标志State,以防止POS终端受到恶意攻击。

[0037] 进一步的,在一实施方式中,在POS终端出厂前激活服务器获取POS终端SN码,将所述POS终端SN码和该POS终端的标志数据关联存储于激活服务器内。

[0038] 进一步的,所述激活请求信息还包括POS终端SN码;

[0039] 激活服务器根据所述POS终端SN码寻找本地数据库中与所述定制信息对应的标志数据。

[0040] 由上述描述可知,本实施方式通过激活服务器根据POS终端SN码寻找对应的标志数据,另一方面通过查寻本地数据库中是否存在该SN码,可以验证该POS终端是否为本激活服务器所管理。

[0041] 请参阅图2,本发明提供的另一技术方案为:一种POS终端安全受控的联网激活装置,包括预置模块10、请求模块20、第一判断模块30和第二判断模块40;

[0042] 所述预置模块10用于激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置在POS终端内;

[0043] 所述请求模块20用于POS终端将包含主板特征码和定制信息Info的激活请求信息发送给激活服务器;

[0044] 所述第一判断模块30用于激活服务器接收到所述激活请求信息后判断所述定制信息Info是否合法,若是,则使用所述私钥Pr加密主板特征码和与所述定制信息对应的标志数据生成定制标志State,将所述定制标志State发送给POS终端,若否,则拒绝激活申请;

[0045] 所述第二判断模块40用于POS终端接收所述定制标志State后使用所述公钥Pu进行解密,判断定制标志中的主板特征码与本机的主板特征码是否相等,若是,则使用定制标志中的标志数据进行激活,若否,则不进行激活。

[0046] 从上述描述可知,本发明的有益效果在于:本发明可以实现根据客户化定制需求以POS终端进行激活,同时保证整个激活过程安全受控。

[0047] 进一步的,在一实施方式中,所述第二判断模块40还用于若POS终端使用公钥Pu解密时发生错误,则不进行激活。

[0048] 由上述描述可知,当所述公钥Pu解密时发生错误,则说明POS终端所接收到的定制标志State可能不是对应的激活服务所发送的,本实施方式及时的拒绝该定制标志,以防止

POS终端受到恶意攻击。

[0049] 进一步的,所述预置模块10还用于在POS终端出厂前激活服务器获取POS终端SN码,将所述POS终端SN码和该POS终端的标志数据关联存储于激活服务器内。

[0050] 由上述描述可知,将所述POS终端SN码和该POS终端的标志数据关联存储于可以便于激活服务器管理标志数据,防止标志数据被误下载。

[0051] 进一步的,所述激活请求信息还包括POS终端SN码;

[0052] 激活服务器根据所述POS终端SN码寻找本地数据库中与所述定制信息对应的标志数据。

[0053] 请参照图3至图6,本发明的具体实施例一为:一种POS终端安全受控的联网激活方法,如图3所示,激活服务器与中间转发设备网络连接,中间转发设备与POS终端通过串、并口或USB线连接。

[0054] 其中,激活服务器用于鉴别POS终端信息,以及生成特殊定制标志State;

[0055] 中间转发设备用于服务器和POS终端数据沟通;

[0056] POS终端:被激活的终端设备。

[0057] 请参阅图4,该POS终端安全受控的联网激活方法的具体步骤为:

[0058] 1、激活服务器产生公私钥对Pr、Pu,并将公钥Pu预置于POS终端内;

[0059] 2、POS终端将POS终端SN码、主板特征码、POS客户化定制信息Info以及包含的软件等信息发送至激活服务器进行激活申请;其中,主板特征码,是每台POS终端都不相同,可以唯一标识POS终端设备的标识,从而确保定制标志State每台终端设备都不相同;

[0060] 3、激活服务器接收到所述激活申请后判断POS终端的客户化定制信息Info是否满足条件;

[0061] 4、当客户化定制信息满足条件时,激活服务器使用私钥Pr加密SN、主板特征码和客户定制信息Info,生成定制标志State,并下发给对应的POS终端;

[0062] 请参阅图5,为所述定制标志State的数据格式示意图,POS终端的状态标志State数据由激活服务器加密状态标志需要的数据构成,状态标志State待加密数据包含:POS的序列号SN、主板特征码和客户化定制信息Info;

[0063] 5、POS终端接收并存储所述定制标志State;

[0064] 请参阅图6,POS终端在接收到所述定制标志State执行以下激活步骤:

[0065] 5.1、读取定制标志State数据;

[0066] 5.2、使用所述预置的公钥Pu解密定制标志State;

[0067] 5.3判断公钥解密是否正确;若否,则结束激活,若是,则转至步骤5.4;

[0068] 5.4、读取定制标志State中的主板特征码MC和定制信息Info;

[0069] 5.5、读取POS终端的主板特征码MC' 和定制信息Info' ;

[0070] 5.6、判断主板特征码MC与MC' 是否相等和定制信息Info和定制信息Info' 是否相同,若否,则不激活,若是,则进行激活,POS进入正常使用状态。

[0071] 当POS终端出厂时或者受攻击维修后,POS处于非正常状态,需要通过激活才能进入正常的使用状态。在本具体实施例中,POS终端激活是在联网状态下激活时,在POS终端中下发一个根据客户化定制需求的特殊的标志State,POS判别到该特殊的标志State合法时,POS才允许正常运行,时满足客户化定制的需求而不被篡改。特殊标志的生成需要后台服务

参与,在激活过程中,通过读取POS中的信息,发送给后台服务判别,满足后台服务认为的激活条件后,才允许激活成功。确保只有后台服务才能生成该标志State,达到有效管控POS的联网激活。

[0072] 综上所述,本发明提供的POS终端安全受制的联网激活方法及装置不仅可以实现通过网络根据客户化定制需求进行激活,使POS终端的激活后客户化定制的需求而不被篡改,并且在整个激活过程都在激活服务器安全受制的范围内进行。

[0073] 以上所述仅为本发明的实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等同变换,或直接或间接运用在相关的技术领域,均同理包括在本发明的专利保护范围内。

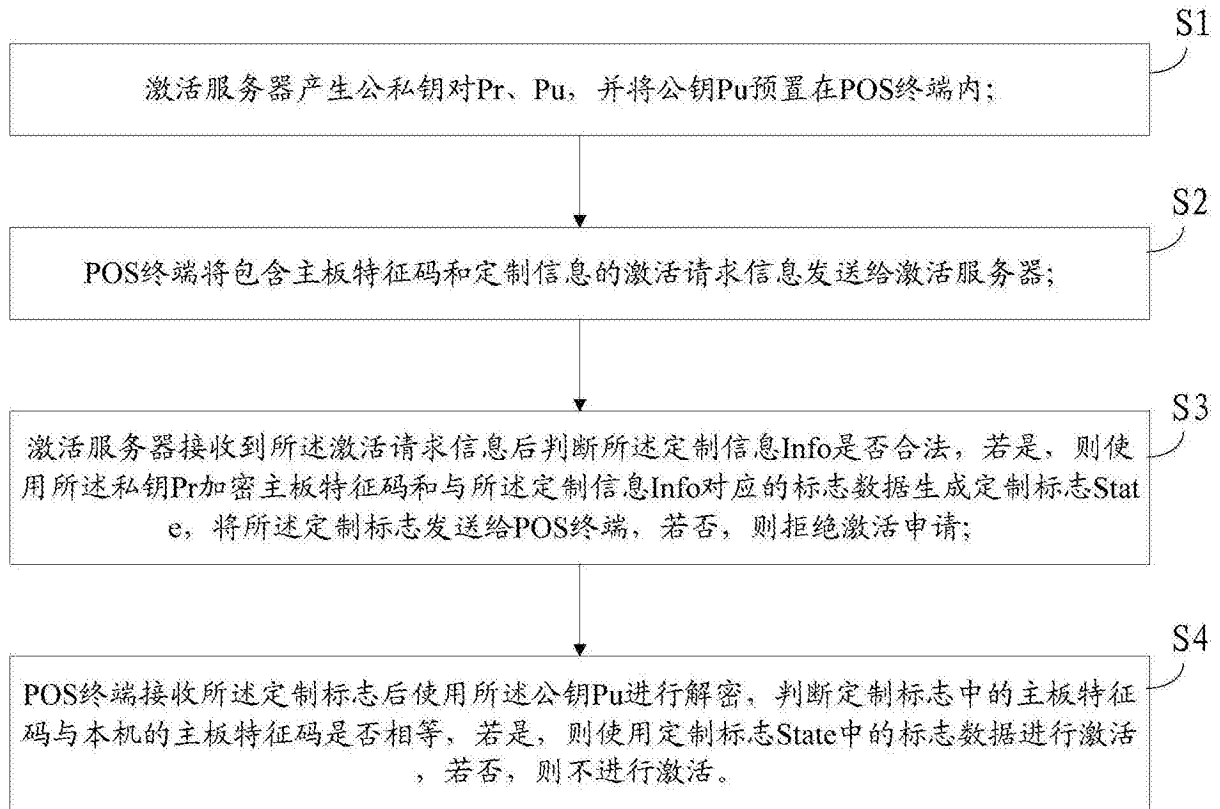


图1

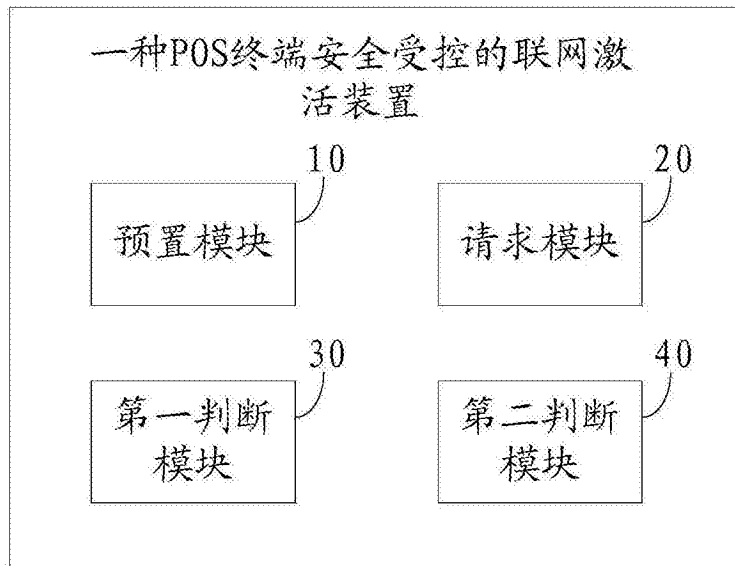


图2

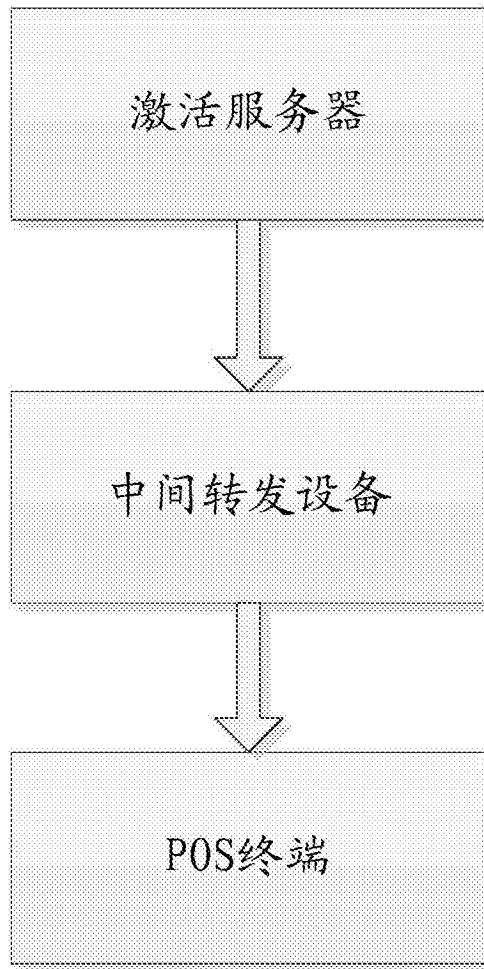


图3

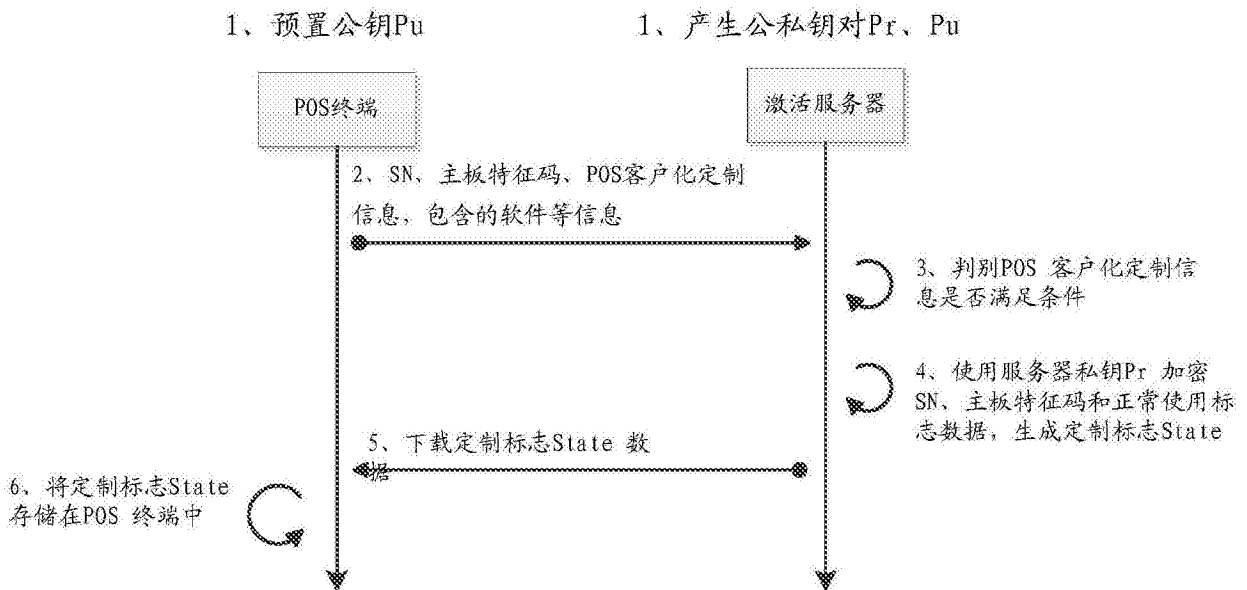


图4



图5

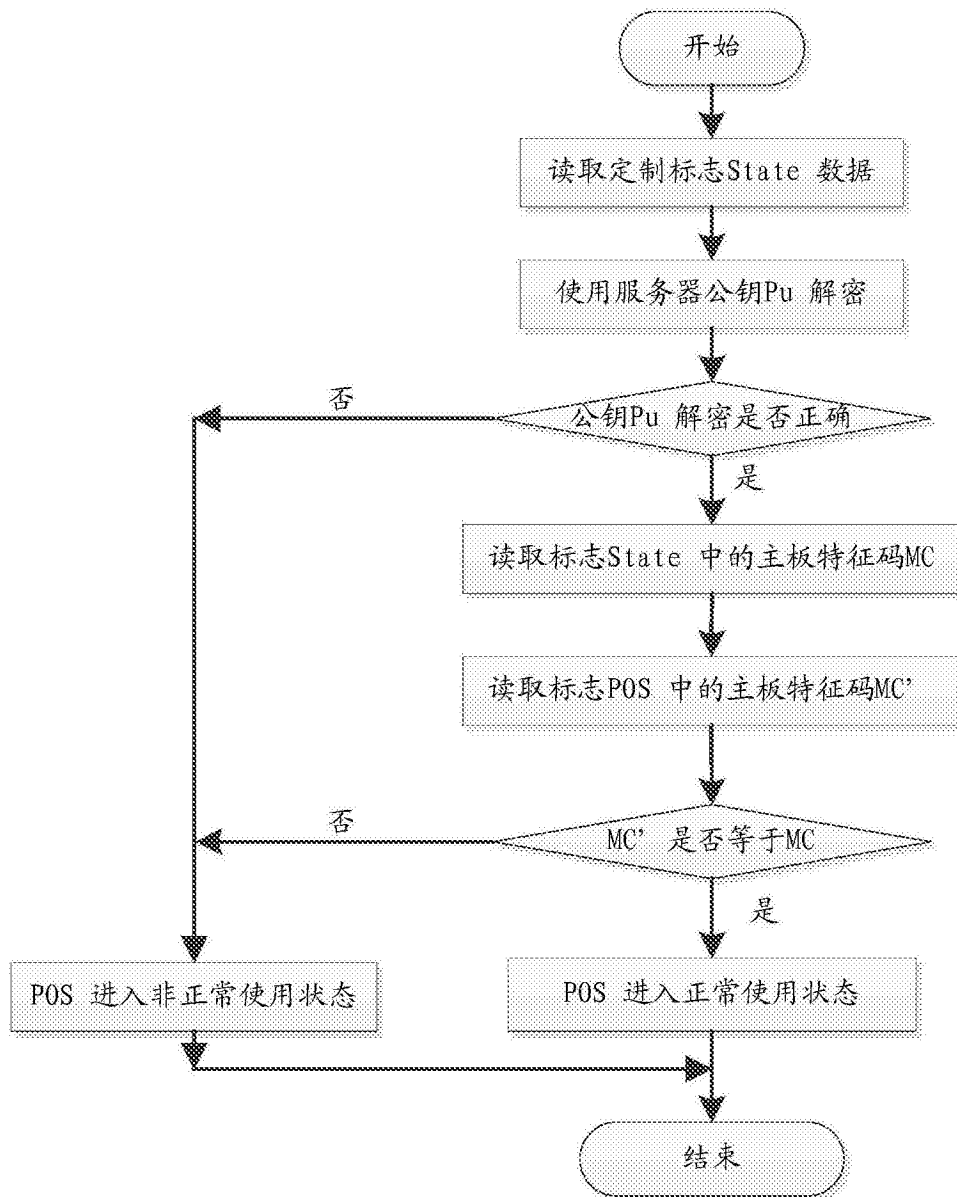


图6