(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 102647274 B
(45)授权公告日 2014.10.08

(21)申请号 201210106378.0

(22)申请日 2012.04.12

(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 陈瑞兵 高明鑫

(74)专利代理机构 福州市鼓楼区博深专利代理事务所(普通合伙) 35214
代理人 林志峥

(51)Int.Cl.
H04L 9/08(2006.01)
G07G 1/14(2006.01)

(56)对比文件
CN 101593389 A,2009.12.02,
CN 102013982 A,2011.04.13,
WO 2008/021581 A3,2008.04.03,
WO 2009/070041 A3,2009.06.04,
CN 101656007 A,2010.02.24,

审查员 程梦莉

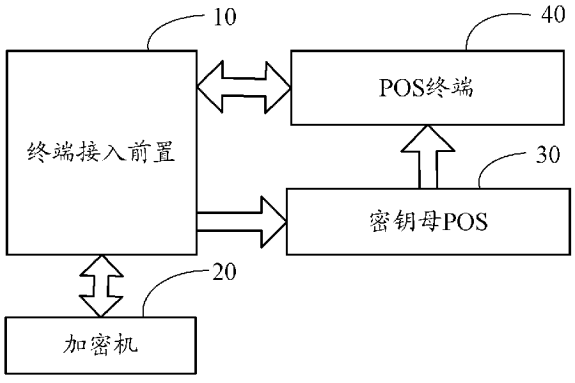
权利要求书2页 说明书5页 附图3页

(54)发明名称

POS终端、终端接入前置、主密钥管理系统及其方法

(57)摘要

本发明公开了一种主密钥管理方法,包括:生成主密钥及主密钥密文并将所述主密钥密文写入密钥库表;将所述密钥库表转换成密钥文件并加载到密钥母POS;所述密钥母POS接收一POS终端发送的密钥分发请求,检索所述密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至所述POS终端,同时将所述主密钥标记为已用;所述POS终端根据接收到的密钥索引号及所述POS终端的硬件序列号生成安全模块号并将所述安全模块号发送至终端接入前置;所述终端接入前置接收所述安全模块号并将所述接收到的安全模块号写入一终端表以登记所述安全模块号。本发明还公开一种POS终端、终端接入前置、主密钥管理系统。



CN 102647274 B

1. 一种主密钥管理方法，其特征在于，包括：

(1) 生成主密钥及与所述主密钥对应的主密钥密文并将所述主密钥密文写入密钥库表；

(2) 将所述密钥库表转换成与密钥母 POS 约定格式的密钥文件并将所述密钥文件加载到所述密钥母 POS；

(3) 所述密钥母 POS 接收一 POS 终端发送的密钥分发请求，根据所述密钥分发请求检索所述密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至所述 POS 终端，同时将所述主密钥标记为已用；

(4) 所述 POS 终端接收所述主密钥及密钥索引号，根据接收到的密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将所述安全模块号发送至终端接入前置；以及

(5) 所述终端接入前置接收所述安全模块号并将所述接收到的安全模块号写入一终端表以登记所述安全模块号。

2. 根据权利要求 1 所述的主密钥管理方法，其特征在于，还包括：

(6) 一 POS 终端发送交易请求及一安全模块号至所述终端接入前置；

(7) 所述终端接入前置接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的已登记的安全模块号，并当检索到匹配的安全模块号时处理所述交易请求，当未检索到匹配的安全模块号时拒绝所述交易请求。

3. 根据权利要求 2 所述的主密钥管理方法，其特征在于：

当检索到匹配的安全模块号时，所述终端接入前置发送认证成功提示至所述 POS 终端。

4. 根据权利要求 2 所述的主密钥管理方法，其特征在于：

当未检索到匹配的安全模块号时，所述终端接入前置发送认证失败提示至所述 POS 终端。

5. 一种主密钥管理系统，包括加密机、终端接入前置、密钥母 POS 以及 POS 终端，所述加密机用于生成主密钥并采用指定密钥对所述主密钥进行加密以生成主密钥密文，所述终端接入前置包括交易单元，其特征在于，

所述终端接入前置包括：

密钥写入单元，用于获取所述主密钥密文并将所述主密钥密文写入密钥库表，其中，所述密钥库表包括密钥索引号、主密钥密文、以及工作密钥密文；

数据库单元，用于存储所述密钥库表；

WEB 管理单元，用于将所述密钥库表转换成与所述密钥母 POS 约定格式的密钥文件；

密钥加载单元，用于将所述密钥文件加载到所述密钥母 POS；

所述密钥母 POS 用于检索所述密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至所述 POS 终端，同时将所述主密钥标记为已用；

所述 POS 终端包括：

存储单元；

密钥获取单元，用于向所述密钥母 POS 发送密钥分发请求，以及接收并关联地存储所述主密钥和密钥索引号至所述存储单元；

安全模块号生成单元，用于根据所述密钥索引号及所述 POS 终端的硬件序列号生成安

全模块号并将所述安全模块号发送至所述终端接入前置；以及

所述终端接入前置还包括：

登记单元，用于接收所述安全模块号并将所述接收到的安全模块号写入一终端表以登记所述接收到的安全模块号，所述数据库单元还用于存储所述终端表。

6. 根据权利要求 5 所述的主密钥管理系统，其特征在于：

所述 POS 终端还用于当发送交易请求时一并发送所述安全模块号至所述终端接入前置；

所述终端接入前置还包括：

认证单元，用于当接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的安全模块号，并当检索到匹配的安全模块号时发送一交易指令至所述交易单元以处理所述交易请求；所述认证单元还用于当未检索到匹配的安全模块号时发送一拒绝交易指令至所述交易单元以拒绝所述交易请求。

7. 根据权利要求 5 所述的主密钥管理系统，其特征在于：

所述密钥文件的格式是 TXT 格式。

8. 一种终端接入前置，包括交易单元，其特征在于，所述终端接入前置还包括：

密钥写入单元，用于从加密机处获取主密钥密文并将所述主密钥密文写入密钥库表，其中，所述密钥库表包括密钥索引号、主密钥密文、以及工作密钥密文；

数据库单元，用于存储所述密钥库表；

WEB 管理单元，用于将所述密钥库表转换成与所述密钥母 POS 约定格式的密钥文件；

密钥加载单元，用于将所述密钥文件加载到所述密钥母 POS；以及

登记单元，用于接收 POS 终端发送的安全模块号并将所述接收到的安全模块号写入一终端表以登记所述接收到的安全模块号，所述数据库单元还用于存储所述终端表。

9. 根据权利要求 8 所述的终端接入前置，其特征在于：

所述终端接入前置还包括：

认证单元，用于当接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的安全模块号，并当检索到匹配的安全模块号时发送一交易指令至所述交易单元以处理所述交易请求；所述认证单元还用于当未检索到匹配的安全模块号时发送一拒绝交易指令至所述交易单元以拒绝所述交易请求。

10. 一种 POS 终端，其特征在于，所述 POS 终端包括：

存储单元；

密钥获取单元，用于向密钥母 POS 发送密钥分发请求，以及接收并关联地将所述密钥母 POS 分发的主密钥和密钥索引号存储至所述存储单元；以及

安全模块号生成单元，用于根据所述密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将所述安全模块号发送至终端接入前置。

POS 终端、终端接入前置、主密钥管理系统及其方法

技术领域

[0001] 本发明涉及信息安全领域，特别涉及一种 POS 终端、终端接入前置、主密钥管理系统及方法。

背景技术

[0002] 使用银行卡通过 POS 终端进行刷卡消费已成为目前主流的消费结算方式，目前 POS 终端在交易时，涉及主密钥及工作密钥，该主密钥存储于 POS 终端中，用于加密该工作密钥以对该工作密钥进行保护。其中，该工作密钥包括 PIN 密钥以及校验 MAC 密钥，该 PIN 密钥用于加密持卡人的客户银行密码，该 MAC 密钥用于对报文进行 MAC 校验。

[0003] 当 POS 终端初始化时，需下载主密钥，传统的 POS 终端主密钥下载方案为，在下载主密钥前，先将 POS 终端与使用该 POS 终端的商户账号相关联，即将 POS 终端带至银行，将 POS 终端的设备号与商户账号相关联，然后下载主密钥至该 POS 终端，该种做法较繁琐，增加了下载主密钥的工作量。

发明内容

[0004] 本发明主要解决的技术问题是提供一种简便的用于 POS 终端的主密钥管理方法以及使用该方法的主密钥管理系统、POS 终端以及终端接入前置。无需在下载主密钥前将 POS 终端与商户账号相关联，母 POS 可向需要主密钥的 POS 终端一次性分发主密钥及密钥索引号，POS 终端将该密钥索引号与该 POS 终端的硬件序列号相结合生成安全模块号，而后将该安全模块号在终端接入前置处登记。当发送交易请求报文时，POS 终端同时发送该安全模块号至终端接入前置以对该 POS 终端及其密钥索引号的合法性进行认证。

[0005] 为解决上述技术问题，本发明采用的一个技术方案是：

[0006] 提供一种主密钥管理方法，包括：(1) 生成主密钥及与所述主密钥对应的主密钥密文并将所述主密钥密文写入密钥库表；(2) 将所述密钥库表转换成与密钥母 POS 约定格式的密钥文件并将所述密钥文件加载到所述密钥母 POS；(3) 所述密钥母 POS 接收一 POS 终端发送的密钥分发请求，根据所述密钥分发请求检索所述密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至所述 POS 终端，同时将所述主密钥标记为已用；(4) 所述 POS 终端接收所述主密钥及密钥索引号，根据接收到的密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将所述安全模块号发送至终端接入前置；以及 (5) 所述终端接入前置接收所述安全模块号并将所述接收到的安全模块号写入一终端表以登记所述安全模块号。

[0007] 其中，所述的主密钥管理方法还包括：(6) 一 POS 终端发送交易请求及一安全模块号至所述终端接入前置；(7) 所述终端接入前置接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的已登记的安全模块号，并当检索到匹配的安全模块号时处理所述交易请求，当未检索到匹配的安全模块号时拒绝所述交易请求。

[0008] 其中，当检索到匹配的安全模块号时，所述终端接入前置发送认证成功提示至所

述 POS 终端。当未检索到匹配的安全模块号时，所述终端接入前置发送认证失败提示至所述 POS 终端。

[0009] 本发明采用的另一个技术方案是：

[0010] 提供一种主密钥管理系统，包括加密机、终端接入前置、密钥母 POS 以及 POS 终端，所述加密机用于生成主密钥并采用指定密钥对所述主密钥进行加密以生成主密钥密文，所述终端接入前置包括交易单元。所述终端接入前置包括：密钥写入单元，用于获取所述主密钥密文并将所述主密钥密文写入密钥库表，其中，所述密钥库表包括密钥索引号、主密钥密文、以及工作密钥；数据库单元，用于存储所述密钥库表；WEB 管理单元，用于将所述密钥库表转换成与所述密钥母 POS 约定格式的密钥文件；密钥加载单元，用于将所述密钥文件加载到所述密钥母 POS；所述密钥母 POS 用于检索所述密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至所述 POS 终端，同时将所述主密钥标记为已用。

[0011] 所述 POS 终端包括：存储单元；密钥获取单元，用于向所述密钥母 POS 发送密钥分发请求，以及接收并关联地存储所述主密钥和密钥索引号至所述存储单元；安全模块号生成单元，用于根据所述密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将所述安全模块号发送至所述终端接入前置；以及所述终端接入前置还包括：登记单元，用于接收所述安全模块号并将所述接收到的安全模块号写入一终端表以登记所述接收到的安全模块号，所述数据库单元还用于存储所述终端表。

[0012] 其中，所述 POS 终端还用于当发送交易请求时一并发送所述安全模块号至所述终端接入前置；所述终端接入前置还包括：认证单元，用于当接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的安全模块号，并当检索到匹配的安全模块号时发送一交易指令至所述交易单元以处理所述交易请求；所述认证单元还用于当未检索到匹配的安全模块号时发送一拒绝交易指令至所述交易单元以拒绝所述交易请求。

[0013] 其中，所述密钥文件的格式是 TXT 格式。

[0014] 本发明采用的另一个技术方案是：

[0015] 提供一种终端接入前置，包括交易单元，所述终端接入前置还包括：密钥写入单元，用于从加密机处获取主密钥密文并将所述主密钥密文写入密钥库表，其中，所述密钥库表包括密钥索引号、主密钥密文、以及工作密钥；数据库单元，用于存储所述密钥库表；WEB 管理单元，用于将所述密钥库表转换成与所述密钥母 POS 约定格式的密钥文件；密钥加载单元，用于将所述密钥文件加载到所述密钥母 POS；以及登记单元，用于接收 POS 终端发送的安全模块号并将所述接收到的安全模块号写入一终端表以登记所述接收到的安全模块号，所述数据库单元还用于存储所述终端表。

[0016] 其中，所述终端接入前置还包括：认证单元，用于当接收所述安全模块号并检索所述终端表，判断是否检索到与所述接收到的安全模块号匹配的安全模块号，并当检索到匹配的安全模块号时发送一交易指令至所述交易单元以处理所述交易请求；所述认证单元还用于当未检索到匹配的安全模块号时发送一拒绝交易指令至所述交易单元以拒绝所述交易请求。

[0017] 本发明采用的另一个技术方案是：

[0018] 提供一种 POS 终端，包括：存储单元；密钥获取单元，用于向密钥母 POS 发送密钥

分发请求，以及接收并关联地将所述密钥母 POS 分发的主密钥和密钥索引号存储至所述存储单元；以及安全模块号生成单元，用于根据所述密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将所述安全模块号发送至终端接入前置。

附图说明

[0019] 图 1 为本发明一实施方式中主密钥管理系统的系统架构图；

[0020] 图 2 为本发明一实施方式中终端接入前置的功能模块图；

[0021] 图 3 为本发明一实施方式中 POS 终端的功能模块图；

[0022] 图 4 为本发明一实施方式中在主密钥生成与分发时，主密钥管理方法在图 1 的系统中执行的流程图；

[0023] 图 5 为本发明一实施方式中在 POS 终端交易时，主密钥管理方法在图 1 中的系统中执行的流程图。

[0024] 主要元件符号说明

[0025] 10、终端接入前置；20、加密机；30、密钥母 POS；40、POS 终端；

[0026] 11、数据库单元；12、WEB 管理单元；13、密钥加载单元；14、登记单元；

[0027] 15、认证单元；16、交易单元；17、密钥写入单元；41、密钥获取单元；

[0028] 42、存储单元；43、安全模块号生成单元。

具体实施方式

[0029] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0030] 请参阅图 1，为本发明一实施方式中主密钥管理系统的系统架构图。该主密钥管理系统包括终端接入前置 10 以及分别与该终端接入前置 10 通信连接的加密机 20、密钥母 POS 30 以及 POS 终端 40，该密钥母 POS 30 与 POS 终端 40 通信连接。

[0031] 加密机 20 用于随机生成终端主密钥，采用指定密钥对该主密钥进行加密以生成主密钥密文，并将该主密钥密文发送至所述终端接入前置 10。

[0032] 请参阅图 2，为本发明一实施方式中终端接入前置 10 的功能模块图。该终端接入前置 10 包括数据库单元 11、WEB 管理单元 12、密钥加载单元 13、登记单元 14、认证单元 15、交易单元 16 以及密钥写入单元 17。

[0033] 该密钥写入单元 17 接收该主密钥密文并将该接收到的主密钥密文写入数据库单元 11 中存储的密钥库表中。该密钥库表包括密钥索引号、主密钥密文以及工作密钥密文，该工作密钥密文包括校验值、PIN 密钥以及 MAC 密钥等。

[0034] 该 WEB 管理单元 12 用于从数据库单元 11 中获取密钥库表并将该获取的密钥库表转换成与密钥母 POS 30 约定格式的密钥文件，其中，该密钥文件包括密钥索引号、主密钥密文以及校验值等。在本实施方式中，该密钥文件的格式为 TXT 格式。该密钥加载单元 13 用于将密钥文件通过通信接口加载到密钥母 POS30 中。

[0035] 该密钥母 POS 30 用于将加载的密钥文件分发到 POS 终端 40，具体地，该密钥母 POS 30 当接收到 POS 终端 40 发送的密钥分发请求时，检索密钥文件中当前可用的主密钥，标记该主密钥已用并将该主密钥及与该主密钥对应的密钥索引号发送至进行密钥分发请

求的 POS 终端 40。

[0036] 请参阅图 3，为本发明一实施方式中 POS 终端的功能模块图。该 POS 终端 40 包括密钥获取单元 41、存储单元 42 以及安全模块号生成单元 43。

[0037] 该密钥获取单元 41 用于向密钥母 POS 30 发送密钥分发请求，并将密钥母 POS 30 分发的主密钥和密钥索引号关联地存储至该存储单元 42，该安全模块号生成单元 43 用于根据该密钥索引号以及 POS 终端的硬件序列号生成安全模块号，并将该安全模块号存储至存储单元 42。该安全模块号包括硬件序列号以及密钥索引号，例如，若硬件序列号为“123L013K”，密钥索引号为“278”，则安全模块号为“123L013K00000278”。该安全模块号生成单元还用于将生成的安全模块号发送至终端输入前置的登记单元 14 进行登记。

[0038] 该登记单元 14 用于将接收到的安全模块号写入一终端表中以对该安全模块号进行登记，该终端表存储在该数据库单元 11 中，该终端表用于记录已完成登记的安全模块号。

[0039] 当 POS 终端 40 发送交易请求至终端输入前置的交易单元 16 进行交易时，POS 终端一并发送安全模块号至认证单元 15，该认证单元 15 用于检索终端表并确认是否检索到与所接收到的安全模块号匹配的已完成登记的安全模块号。

[0040] 该认证单元 15 还用于当检索到的匹配的安全模块号时，发送认证成功提示至 POS 终端 40 并发送交易指令至交易单元 16，交易单元 16 根据该交易指令处理 POS 终端 40 发送的交易请求。该认证单元 15 还用于当未在终端表中检索到匹配的安全模块号时，发送认证失败提示至 POS 终端 40 并发送拒绝交易指令至交易单元 16，交易单元 16 拒绝处理交易请求。

[0041] 请参阅图 4，为本发明的一实施方式中在主密钥生成与分发时，主密钥管理方法在图 1 的系统中执行的流程图。

[0042] 步骤 S40，加密机 20 随机生成主密钥，采用指定密钥对该主密钥进行加密以生成主密钥密文，该密钥写入单元 17 接收该主密钥密文并将该接收到的主密钥密文写入数据库单元 11 中存储的密钥库表。

[0043] 其中，该该密钥库表包括密钥索引号、主密钥密文以及工作密钥密文，该工作密钥密文包括校验值、PIN 密钥以及 MAC 密钥等。

[0044] 步骤 S41，该 WEB 管理单元 12 将该密钥库表转换成与密钥母 POS 30 约定格式的密钥文件，该密钥加载单元 13 将该密钥文件加载到该密钥母 POS 30。

[0045] 在本实施方式中，该密钥文件的格式是 TXT 格式。该密钥加载单元 13 用于将密钥文件通过通信接口加载到密钥母 POS 30 中。

[0046] 步骤 S42，该密钥母 POS 30 接收 POS 终端 40 的密钥获取单元 41 发送的密钥分发请求，根据该密钥分发请求检索该密钥文件中可用的主密钥并将所述主密钥及对应的密钥索引号分发至该 POS 终端 40，同时将所述主密钥标记为已用；

[0047] 步骤 S43，该 POS 终端 40 的密钥获取单元 41 接收该密钥母 POS30 分发的主密钥及密钥索引号，该安全模块号生成单元 43 根据该接收到的密钥索引号及所述 POS 终端的硬件序列号生成安全模块号并将该安全模块号发送至终端接入前置 10。

[0048] 步骤 S44，所述终端接入前置 10 的登记单元 14 接收该安全模块号并将该接收到的安全模块号写入一终端表以登记该安全模块号。

[0049] 其中，该终端表存储在该数据库单元 11 中，该终端表用于记录已完成登记的安全模块号。

[0050] 请参阅图 5，为本发明一实施方式中在 POS 终端交易时，主密钥管理方法在图 1 中的系统中执行的流程图。

[0051] 步骤 S50，POS 终端 40 发送交易请求至交易单元 16，发送安全模块号至认证单元 15。

[0052] 步骤 S51，该认证单元 15 检索终端表并判断是否检索到与所接收到的安全模块号匹配的已完成登记的安全模块号。当检索到匹配的安全模块号时，执行步骤 S52，否则，执行步骤 S53。

[0053] 步骤 S52，交易单元 16 处理所述交易请求。

[0054] 步骤 S53，交易单元 16 拒绝所述交易请求。

[0055] 在本实施方式中，该步骤 S51 还包括当检索到匹配的安全模块号时认证单元 15 发送认证成功提示至该 POS 终端 40；当未检索到匹配的安全模块号时，认证单元 15 发送认证失败提示至该 POS 终端 40。

[0056] 本发明的 POS 终端、终端接入前置、主密钥管理系统及方法，无需在下载主密钥前将 POS 终端与商户账号相关联，本发明的母 POS 可向需要主密钥的 POS 终端一次性分发主密钥及密钥索引号，POS 终端将该密钥索引号与该 POS 终端的硬件序列号相结合生成安全模块号，而后将该安全模块号在终端接入前置处登记。当发送交易请求报文时，POS 终端同时发送该安全模块号至终端接入前置以对该 POS 终端及其密钥索引号的合法性进行认证。

[0057] 以上该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效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

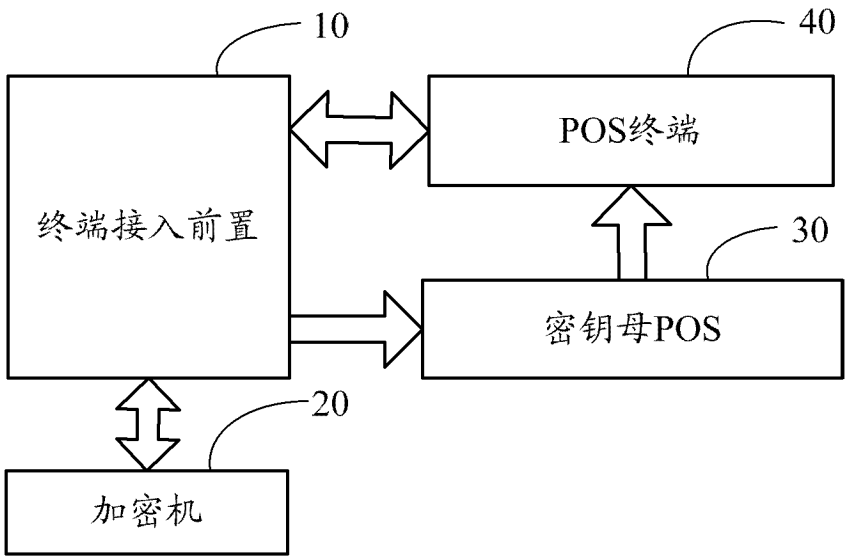

10
40
POS终端
终端接入前置
30
密钥母POS
20
加密机

图 1

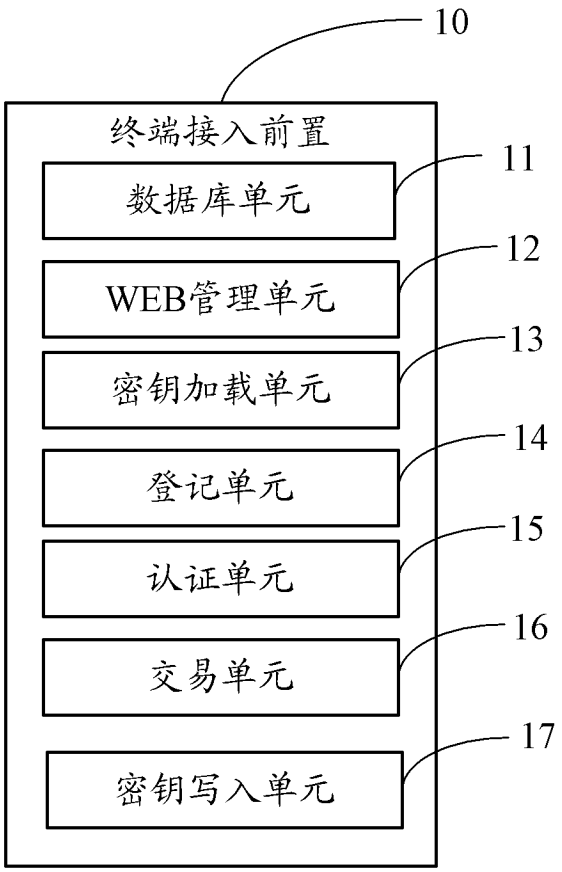

10
终端接入前置
11
数据库单元
12
WEB管理单元
13
密钥加载单元
14
登记单元
15
认证单元
16
交易单元
17
密钥写入单元

图 2

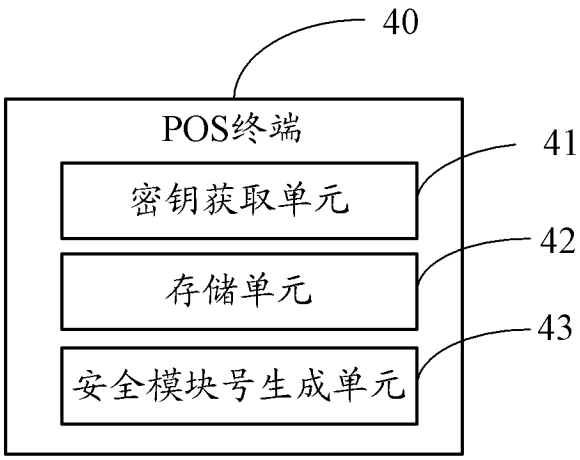

40
POS终端
41
密钥获取单元
42
存储单元
43
安全模块号生成单元

图 3

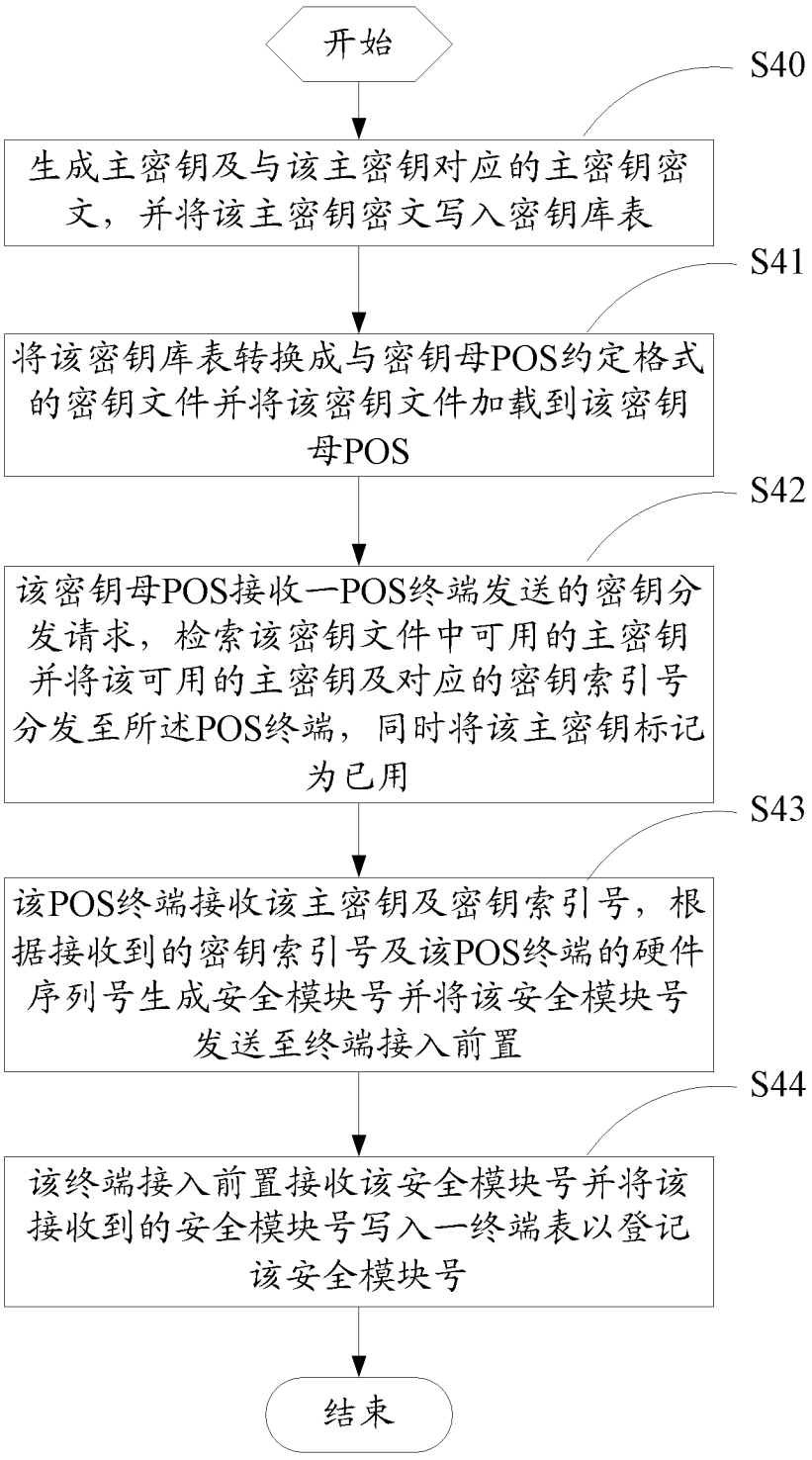

开始
S40
生成主密钥及与该主密钥对应的主密钥密文，并将该主密钥密文写入密钥库表
S41
将该密钥库表转换成与密钥母POS约定格式的密钥文件并将该密钥文件加载到该密钥母POS
S42
该密钥母POS接收一POS终端发送的密钥分发请求，检索该密钥文件中可用的主密钥并将该可用的主密钥及对应的密钥索引号分发至所述POS终端，同时将该主密钥标记为已用
S43
该POS终端接收该主密钥及密钥索引号，根据接收到的密钥索引号及该POS终端的硬件序列号生成安全模块号并将该安全模块号发送至终端接入前置
S44
该终端接入前置接收该安全模块号并将该接收到的安全模块号写入一终端表以登记该安全模块号
结束

图 4

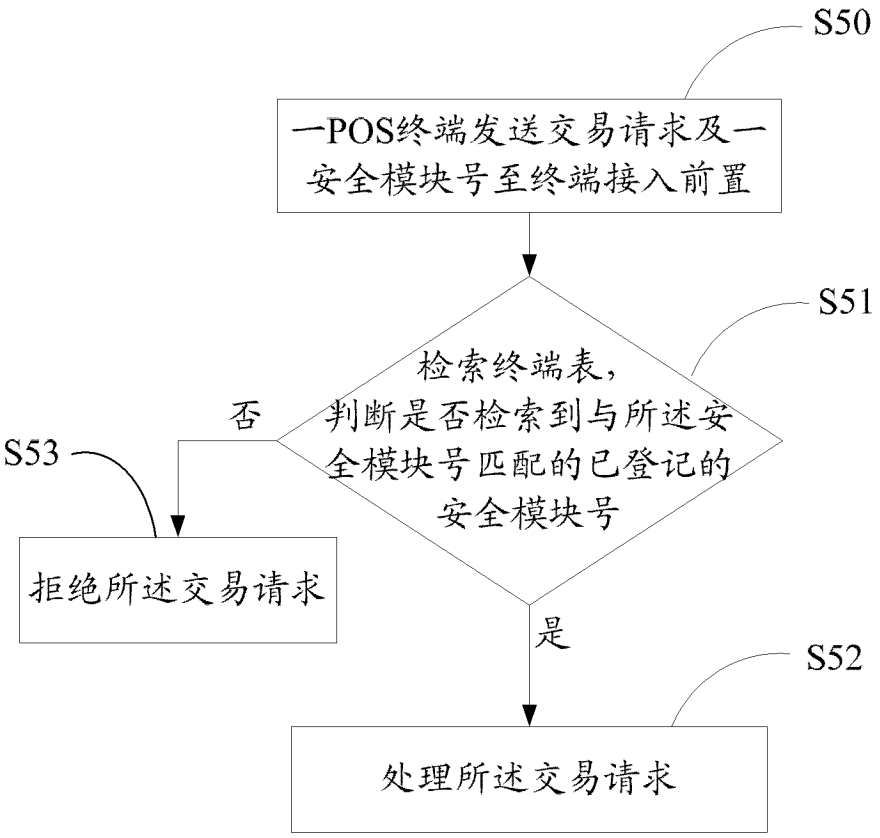

S50
一POS终端发送交易请求及一安全模块号至终端接入前置
S51
检索终端表，判断是否检索到与所述安全模块号匹配的已登记的安全模块号
否
S53
拒绝所述交易请求
是
S52
处理所述交易请求

图 5