(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103903306 A
(43)申请公布日 2014.07.02

(21)申请号 201210585908.4

(22)申请日 2012.12.28

(71)申请人 北京握奇数据系统有限公司
地址 100102 北京市朝阳区望京利泽中园 101 号启明国际大厦 7 层

(72)发明人 张江涛 赵敏 计进波

(74)专利代理机构 北京天悦专利代理事务所（普通合伙） 11311
代理人 田明 任晓航

(51)Int.Cl.
G07B 11/00(2006.01)

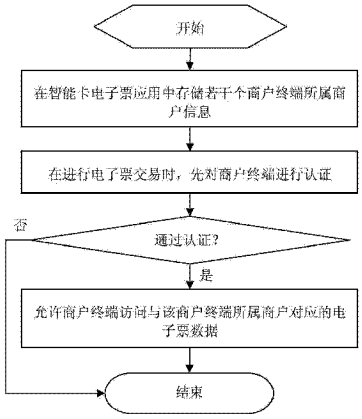
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种智能卡电子票应用实现方法及系统

(57)摘要

本发明公开了一种智能卡电子票应用实现方法及系统，属于电子票应用技术领域。本发明在智能卡电子票应用中存储若干个商户信息；在进行电子票交易时，先对商户身份进行认证；如果通过认证，则允许该商户的商户终端访问电子票应用中与该商户对应的电子票数据，否则不允许访问。本发明一方面通过对多商户的接入管理，保证了电子票的发行安全；另一方面，通过兼容多商户各自特定的电子票生成和验证方式，避免了商户终端的改造问题，节省了改造成本，对推动电子票业务的一卡通用、一卡多用起到了积极的作用。



CN 103903306 A

1. 一种智能卡电子票应用实现方法，包括以下步骤：

在智能卡电子票应用中存储若干个商户信息；

在进行电子票交易时，先对商户身份进行认证；如果通过认证，则允许该商户的商户终端访问电子票应用中与该商户对应的电子票数据，否则不允许访问。

2. 如权利要求 1 所述的智能卡电子票应用实现方法，其特征在于：所述商户信息包括商户认证秘钥和消息摘要秘钥、商户标识和商户电子票存储地址、商户授权信息、电子票和电子票交易记录。

3. 如权利要求 1 所述的智能卡电子票应用实现方法，其特征在于：所述方法还包括电子票应用发行端在智能卡电子票应用中增加、删除和修改商户信息的步骤，在增加、删除和修改商户信息之前，智能卡电子票应用与电子票应用发行端先进行相互认证。

4. 如权利要求 3 所述的智能卡电子票应用实现方法，其特征在于：所述智能卡电子票应用与电子票应用发行端进行相互认证的过程如下：

（1）电子票应用发行端向智能卡发起应用选择指令，选择电子票应用，智能卡返回相应的应用选择结果；

（2）电子票应用发行端生成应用认证随机数，向智能卡电子票应用发送应用合法性认证请求及所述应用认证随机数；

（3）智能卡电子票应用按照预先约定算法对认证随机数进行加密，生成认证密文数据，同时生成发行端认证随机数，将认证密文数据和发行端认证随机数返回给电子票应用发行端；

（4）电子票应用发行端按照预先约定算法对认证密文数据进行解密，将解密结果与所述应用认证随机数进行比较，如果解密结果与所述应用认证随机数相同，则校验通过，否则校验失败，结束认证过程；如果校验通过，则按照预先约定算法对发行端认证随机数进行加密，生成发行端认证密文数据，并将发行端认证密文数据发送给智能卡电子票应用，进行电子票应用发行端认证；

（5）智能卡电子票应用使用预先约定算法对所述发行端认证密文数据进行解密，将解密结果与所述发行端认证随机数进行比较，如果解密结果与所述发行端认证随机数相同，则校验通过，否则校验失败，结束认证过程。

5. 如权利要求 4 所述的智能卡电子票应用实现方法，其特征在于：在所述认证过程中，对智能卡电子票应用与电子票应用发行端所有交互数据进行消息摘要计算。

6. 如权利要求 4 所述的智能卡电子票应用实现方法，其特征在于：所述约定算法采用对称算法或非对称算法。

7. 如权利要求 1~6 中任一项所述的智能卡电子票应用实现方法，其特征在于，所述对商户身份进行认证的过程如下：

①商户终端发起应用选择指令，选择电子票应用，智能卡返回相应的应用选择结果；

②商户终端发起商户认证请求，向智能卡电子票应用申请认证随机数，智能卡电子票应用生成认证随机数后，返回给商户终端；

③商户终端对所述认证随机数按照约定算法进行加密，向智能卡电子票应用请求进行校验，智能卡电子票应用使用约定算法对所述加密数据进行解密，将解密结果与所述认证随机数进行比较，如果解密结果与所述认证随机数相同，则校验通过，否则校验失败。

8. 如权利要求 7 所述的智能卡电子票应用实现方法，其特征在于：所述约定算法采用对称算法或非对称算法。

9. 一种智能卡电子票应用实现系统，包括电子票应用发行端（1）、商户终端（2）和智能卡（3），其特征在于：

所述电子票应用发行端（1）用于在智能卡电子票应用中存储若干个商户信息，并对智能卡（3）中存储的商户信息进行增加、修改和删除操作；

所述智能卡（3）包括用于存储商户信息的存储装置（31），用于在进行电子票交易时，对商户终端所属商户进行认证的商户认证装置（32）；

所述商户终端（2）用于与所述智能卡（3）中电子票应用进行交易。

10. 如权利要求 9 所述的智能卡电子票应用实现系统，其特征在于：所述智能卡还包括用于对智能卡应用发行端进行认证的发行端认证装置（32）。

一种智能卡电子票应用实现方法及系统

技术领域

[0001] 本发明属于智能卡应用技术领域，具体涉及一种智能卡电子票应用实现方法及系统。

背景技术

[0002] 目前，基于智能卡的电子票技术已经在很多行业和领域有了相应的应用和推广，电子票的生成技术也较为完善，有相对比较好的安全生成策略和验证策略。但是，该类电子票技术一般只能解决同一类型票卡的发行和验证功能，仅能在特定的领域或场所使用，对于具有不同特征的票卡，则无法进行有效管理，阻碍了电子票的推广和应用。

[0003] 不同的商户在拓展业务过程中，根据自身业务特点和业务发展情况，一般会发行多种类型的票卡，包括常规票卡、折扣卡、优惠券、体验券等。同时，不同票卡所能享有的消费服务不同。另外，不同的商户采用的电子票生成和验证算法不同，现有技术无法满足所有商户对电子票生成和验证的个性化要求。

发明内容

[0004] 针对现有技术中存在的缺陷，本发明所要解决的技术问题是提供一种支持多商户、安全性高的智能卡电子票应用实现方法及系统。

[0005] 为解决上述技术问题，本发明采用的技术方案如下：

[0006] 一种智能卡电子票应用实现方法，包括以下步骤：

[0007] 在智能卡电子票应用中存储若干个商户信息；

[0008] 在进行电子票交易时，先对商户身份进行认证；如果通过认证，则允许该商户的商户终端访问电子票应用中与该商户对应的电子票数据，否则不允许访问。

[0009] 如上所述的智能卡电子票应用实现方法，其中，商户信息包括商户认证秘钥和消息摘要秘钥、商户标识和商户电子票存储地址、商户授权信息、电子票和电子票交易记录。

[0010] 如上所述的智能卡电子票应用实现方法，还包括电子票应用发行端在智能卡电子票应用中增加、删除和修改商户信息的步骤，在增加、删除和修改商户信息之前，智能卡电子票应用与电子票应用发行端先进行相互认证。

[0011] 如上所述的智能卡电子票应用实现方法，其中，智能卡电子票应用与电子票应用发行端进行相互认证的过程如下：

[0012] （1）电子票应用发行端向智能卡发起应用选择指令，选择电子票应用，智能卡返回相应的应用选择结果；

[0013] （2）电子票应用发行端生成应用认证随机数，向智能卡电子票应用发送应用合法性认证请求及所述应用认证随机数；

[0014] （3）智能卡电子票应用按照预先约定算法对认证随机数进行加密，生成认证密文数据，同时生成发行端认证随机数，将认证密文数据和发行端认证随机数返回给电子票应用发行端；

[0015] （4）电子票应用发行端按照预先约定算法对认证密文数据进行解密，将解密结果与所述应用认证随机数进行比较，如果解密结果与所述应用认证随机数相同，则校验通过，否则校验失败，结束认证过程；如果校验通过，则按照预先约定算法对发行端认证随机数进行加密，生成发行端认证密文数据，并将发行端认证密文数据发送给智能卡电子票应用，进行电子票应用发行端认证；

[0016] （5）智能卡电子票应用使用预先约定算法对所述发行端认证密文数据进行解密，将解密结果与所述发行端认证随机数进行比较，如果解密结果与所述发行端认证随机数相同，则校验通过，否则校验失败，结束认证过程。

[0017] 如上所述的智能卡电子票应用实现方法，其中，在所述认证过程中，对智能卡电子票应用与电子票应用发行端所有交互数据进行消息摘要计算。

[0018] 如上所述的智能卡电子票应用实现方法，其中，约定算法采用对称算法或非对称算法。

[0019] 如上所述的智能卡电子票应用实现方法，其中，对商户身份进行认证的过程如下：

[0020] ①商户终端发起应用选择指令，选择电子票应用，智能卡返回相应的应用选择结果；

[0021] ②商户终端发起商户认证请求，向智能卡电子票应用申请认证随机数，智能卡电子票应用生成认证随机数后，返回给商户终端；

[0022] ③商户终端对所述认证随机数按照约定算法进行加密，向智能卡电子票应用请求进行校验，智能卡电子票应用使用约定算法对所述加密数据进行解密，将解密结果与所述认证随机数进行比较，如果解密结果与所述认证随机数相同，则校验通过，否则校验失败。

[0023] 如上所述的智能卡电子票应用实现方法，其中，约定算法采用对称算法或非对称算法。

[0024] 一种智能卡电子票应用实现系统，包括电子票应用发行端、商户终端和智能卡，所述电子票应用发行端用于在智能卡电子票应用中存储若干个商户信息，并对智能卡中存储的商户信息进行增加、修改和删除操作；

[0025] 所述智能卡包括用于存储商户信息的存储装置，用于在进行电子票交易时，对商户终端所属商户进行认证的商户认证装置；

[0026] 所述商户终端用于与所述智能卡中电子票应用进行交易。

[0027] 如上所述的智能卡电子票应用实现系统，其中，智能卡还包括用于对智能卡应用发行端进行认证的发行端认证装置。

[0028] 本发明所述方法及系统，实现了电子票一卡通用市场需求，一方面，通过对多商户的接入管理，保证了电子票的发行安全；另一方面，通过兼容多商户各自特定的电子票生成和验证方式，避免了商户终端的改造问题，节省了改造成本，对推动电子票业务的一卡通用、一卡多用起到了积极的作用。

附图说明

[0029] 图 1 是具体实施方式中智能卡电子票应用实现系统的结构框图；

[0030] 图 2 是具体实施方式中存储装置存储的文件结构示意图；

[0031] 图 3 是具体实施方式中智能卡电子票应用实现方法的流程图；

[0032] 图 4 是具体实施方式中智能卡对商户进行认证的过程流程图；

[0033] 图 5 是具体实施方式中智能卡对智能卡应用发行端进行认证的过程流程图。

具体实施方式

[0034] 本发明通过在智能卡中实现一套通用的电子票应用，实现对多商户、多类型电子票发行的支持，并实现了对多商户接入的管理；通过仅存储生成后的电子票数据信息，不对实际电子票的生成和验证进行强制规定，完全由商户自己定义，实现了对电子票生成和验证算法的兼容性问题。下面结合附图对本发明的具体实施方式进行详细描述。

[0035] 如图 1 所示，本实施方式中智能卡电子票应用实现系统包括智能卡应用发行端 1、商户终端 2 和智能卡 3，智能卡 3 包括存储装置 31、发行端认证装置 32 和商户认证装置 33。

[0036] 智能卡应用发行端 1 用于与智能卡 3 进行交互，将所述商户终端 2 所属商户信息存入智能卡 3 中，并对智能卡 3 中存储的商户终端 2 所属商户信息进行增加、修改和删除等操作。商户终端 2 用于与智能卡 3 进行交互，完成智能卡电子票交易过程。

[0037] 存储装置 31 主要用于存储智能卡主控秘钥文件、目录文件和 ADF（Application Dedicated File，应用专有文件），所述应用专有文件包括电子票主控秘钥文件、商户目录文件、电子票文件和用户信息文件。存储装置 31 可以存储多个商户信息，每个商户信息可以包括多种类型的电子票。存储装置 31 存储的文件结构如图 2 所示。

[0038] 其中，智能卡主控秘钥文件用于存储智能卡应用的主控密钥，该密钥由智能卡应用发行端 1 掌控，对电子票应用中的商户目录文件和电子票文件具有管理控制权限，所有进行商户目录文件和电子票文件的创建、修改、删除操作，均需要通过该主控密钥进行认证校验后，方可进行。

[0039] 商户目录文件为动态文件，根据商户信息的变化情况进行动态更新，包括 KEY 文件、商户信息文件和商户授权信息文件。所述 KEY 文件用于存储商户认证密钥和消息摘要密钥，商户认证密钥用于进行商户电子票新增、删除和交易使用，所有该商户的电子票在新增、删除和交易时，均需要通过商户认证密钥的认证；消息摘要密钥主要用于保证商户通讯安全，确保在进行通讯过程中，通讯数据的完整性。所述商户信息文件用于存储商户标识和商户对应的电子票文件地址，用于进行商户识别和电子票地址索引使用。所述商户授权信息包括商户的权限范围、授权级别等信息，由智能卡应用发行端 1 控制，用于对商户的业务行为进行授权和规范。

[0040] 电子票文件用于存储电子票和电子票交易记录，由智能卡应用发行端 1 在创建商户信息时，同时对应创建相应的电子票文件。商户在发售电子票时或用户使用电子票时，使用其对应的商户认证密钥认证通过后，可以对电子票文件进行管理，包括进行电子票交易、新增电子票、查看电子票使用情况等。其中，电子票用于存储可由商户自行识别的电子票数据信息，其存储空间由智能卡应用发行端 1 在创建商户时进行分配。电子票交易记录与电子票对应，当发生电子票交易后，进行交易记录的存储，一般为循环文件，可根据智能卡容量由智能卡应用发行端 1 自行定义其记录的交易笔数。

[0041] 用户信息文件用于唯一标识一个用户的用户信息文件，包括用户使用的智能卡电子票应用唯一序列号、用户身份信息、用户认证信息等内容，商户对其内容的访问权限由商

户授权信息决定。

[0042] 发行端认证装置 32 用于在增加、删除和修改商户终端 2 信息时，对智能卡应用发行端 1 进行认证。商户认证装置 33 用于当商户终端 2 访问智能卡电子票应用时，对商户终端 2 所属商户进行认证。

[0043] 如图 3 所示，采用图 1 所示系统实现智能卡电子票应用方法的过程包括以下步骤：

[0044] (1) 在智能卡电子票应用中存储若干个商户终端所属商户信息。

[0045] 智能卡应用发行端 1 将商户终端所属商户信息存入智能卡内。智能卡中可存储若干个商户，每个商户可包含多种类型的电子票。智能卡内商户终端所属商户信息的增加、修改和删除等操作均由智能卡应用发行端 1 负责。在进行商户终端所属商户信息操作前，智能卡 3 和智能卡应用发行端 1 先进行相互认证。如图 4 所示，认证过程包括以下步骤：

[0046] ①智能卡应用发行端 1 向智能卡 3 发起电子票应用选择指令，智能卡 3 向智能卡应用发行端 1 返回相应的应用选择结果；

[0047] ②智能卡应用发行端 1 生成应用认证随机数，向智能卡 3 电子票应用发送电子票应用合法性认证请求；

[0048] ③发行端认证装置 32 接收到电子票应用合法性认证请求后，使用双方预先约定的算法对应用认证随机数进行加密，生成认证密文数据，同时生成发行端认证随机数，将认证密文数据和发行端认证随机数返回给智能卡应用发行端 1；

[0049] ④智能卡应用发行端 1 校验认证密文数据的合法性，即使用双方预先预定的算法对认证密文数据进行解密，将解密结果与所述应用认证随机数进行比较，如果解密结果与所述应用认证随机数相同，则校验通过，否则校验失败；如果校验通过，则使用双方预先约定的算法对发行端认证随机数进行加密，生成发行端认证密文数据，并将发行端认证密文数据发送给发行端认证装置 32，进行发行端认证；

[0050] ⑤发行端认证装置 32 对发行端认证密文数据进行验证，即使用双方预先约定的算法对所述发行端认证密文数据进行解密，将解密结果与所述发行端认证随机数进行比较，如果解密结果与所述发行端认证随机数相同，则校验通过，否则校验失败；校验通过后，方可准许智能卡应用发行端 1 进行相应的业务操作。

[0051] 整个认证过程可以使用消息摘要密钥保证认证数据的完整性，即在进行认证过程时，对智能卡电子票应用与电子票应用发行端所有交互数据进行消息摘要计算，其计算算法可以采用 MD5 或 SHA1 算法。

[0052] 所述双方预先约定的算法根据智能卡应用发行端 1 对安全性的要求可以采用现有的对称算法或非对称算法。

[0053] (2) 在进行电子票交易时，先对商户身份进行认证；如果通过认证，则允许该商户的商户终端访问电子票应用中与该商户对应的电子票数据，否则不允许访问。

[0054] 如图 5 所示，对商户终端 2 进行认证的过程如下：

[0055] ①商户终端 2 发起应用选择指令，选择电子票应用，智能卡 3 返回相应的应用选择结果；

[0056] ②商户终端 2 发起商户认证请求，向商户认证装置 33 申请认证随机数，商户认证装置 33 生成认证随机数后，返回给商户终端 2；

[0057] ③商户终端 2 对所述认证随机数按照约定算法进行加密，向商户认证装置 33 请求进行校验，商户认证装置 33 对加密数据进行合法性校验，即使用双方预先约定的算法对所述加密数据进行解密，将解密结果与所述认证随机数进行比较，如果解密结果与所述认证随机数相同，则校验通过，否则校验失败。

[0058] 所述约定算法可以采用现有的对称算法或非对称算法。

[0059] 商户终端 2 认证通过后，可以对商户终端 2 所属商户的电子票数据进行操作，包括查询、消费、添加和删除等操作。

[0060] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其同等技术的范围之内，则本发明也意图包含这些改动和变型在内。

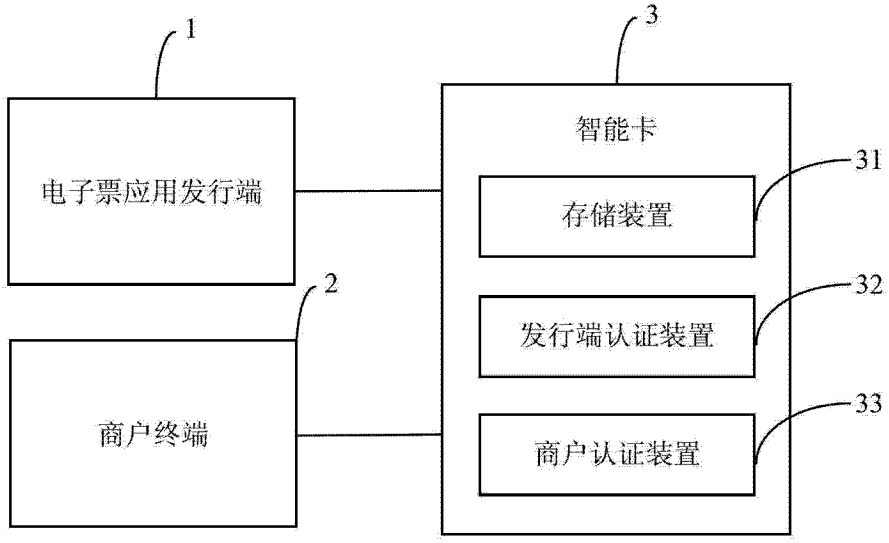

1
3
电子票应用发行端
智能卡
31
存储装置
2
32
发行端认证装置
商户终端
33
商户认证装置

图 1

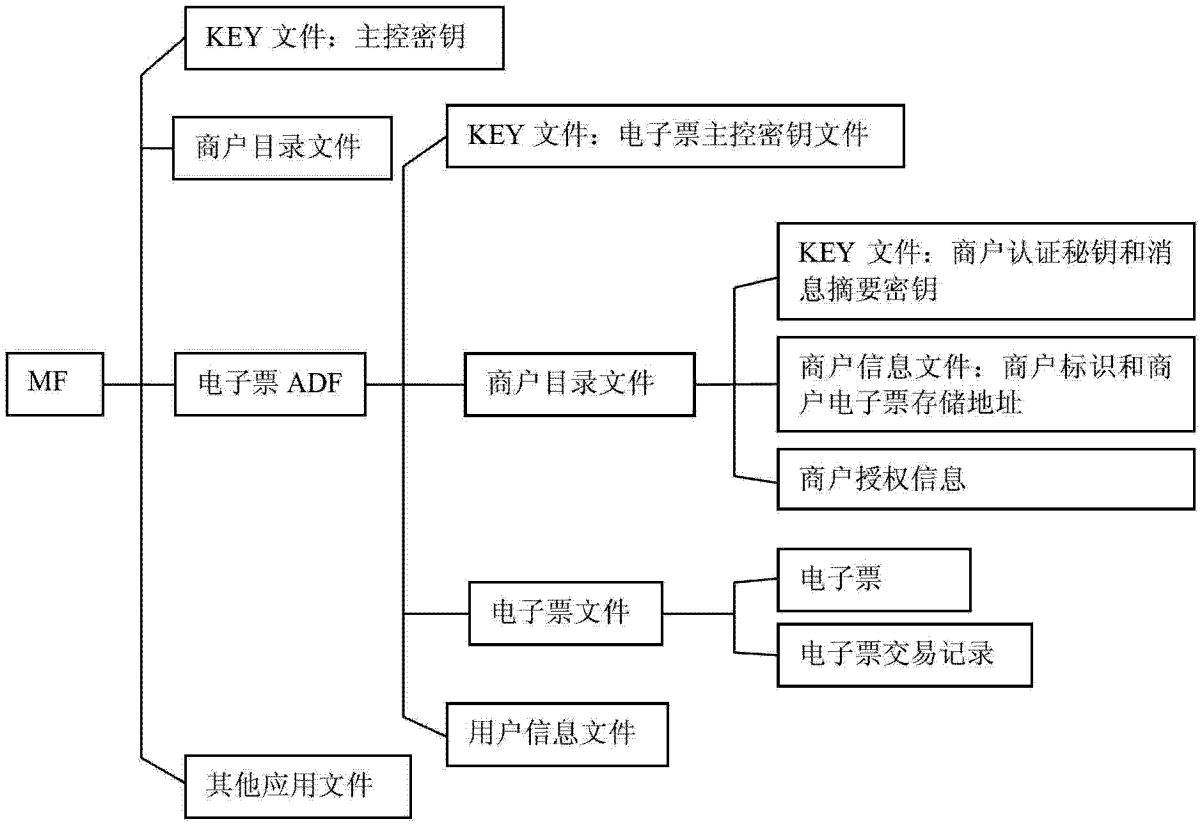

KEY 文件：主控密钥
商户目录文件
KEY 文件：电子票主控密钥文件
KEY 文件：商户认证秘钥和消息摘要密钥
MF
电子票 ADF
商户目录文件
商户信息文件：商户标识和商户电子票存储地址
商户授权信息
电子票
电子票文件
电子票交易记录
用户信息文件
其他应用文件

图 2

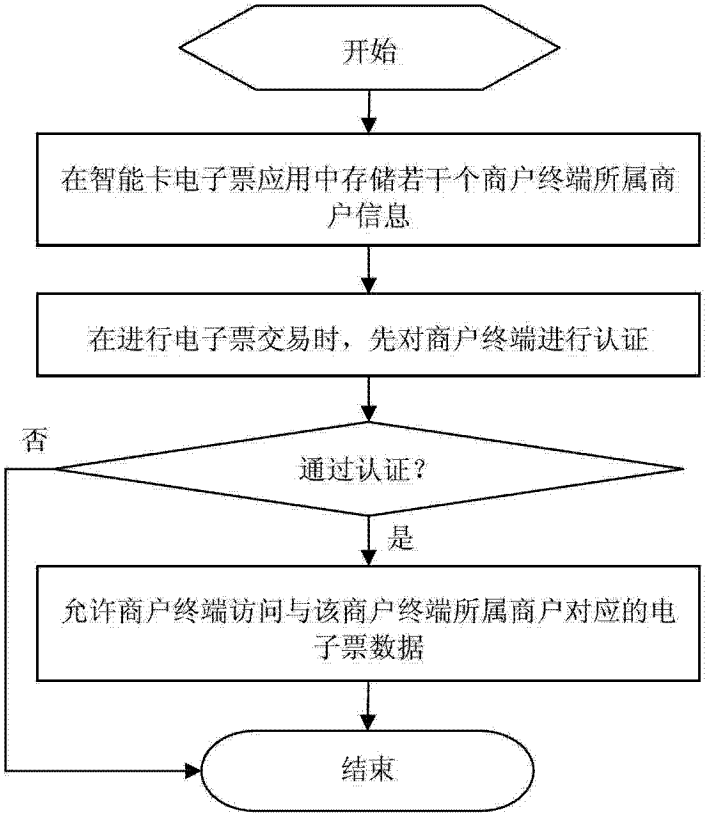

开始
在智能卡电子票应用中存储若干个商户终端所属商户信息
在进行电子票交易时，先对商户终端进行认证
否
通过认证？
是
允许商户终端访问与该商户终端所属商户对应的电子票数据
结束

图 3

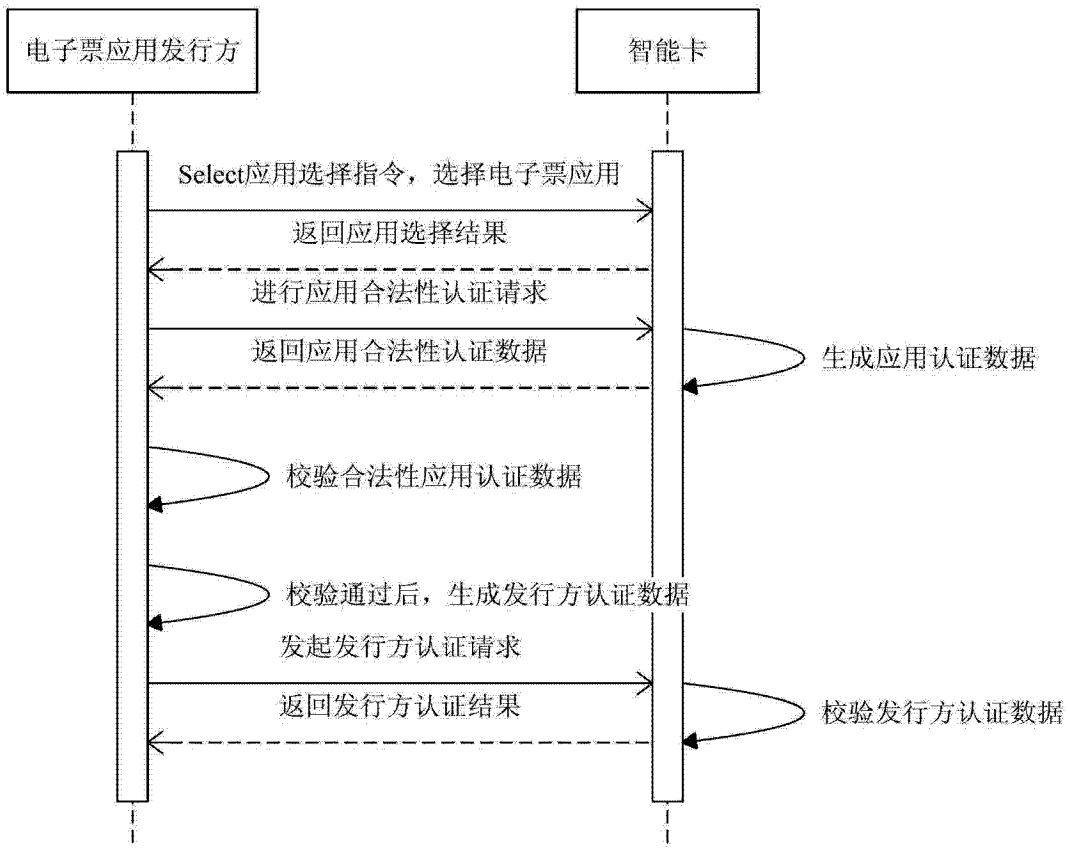

电子票应用发行方
智能卡
Select应用选择指令，选择电子票应用
返回应用选择结果
进行应用合法性认证请求
返回应用合法性认证数据
生成应用认证数据
校验合法性应用认证数据
校验通过后，生成发行方认证数据
发起发行方认证请求
返回发行方认证结果
校验发行方认证数据

图 4

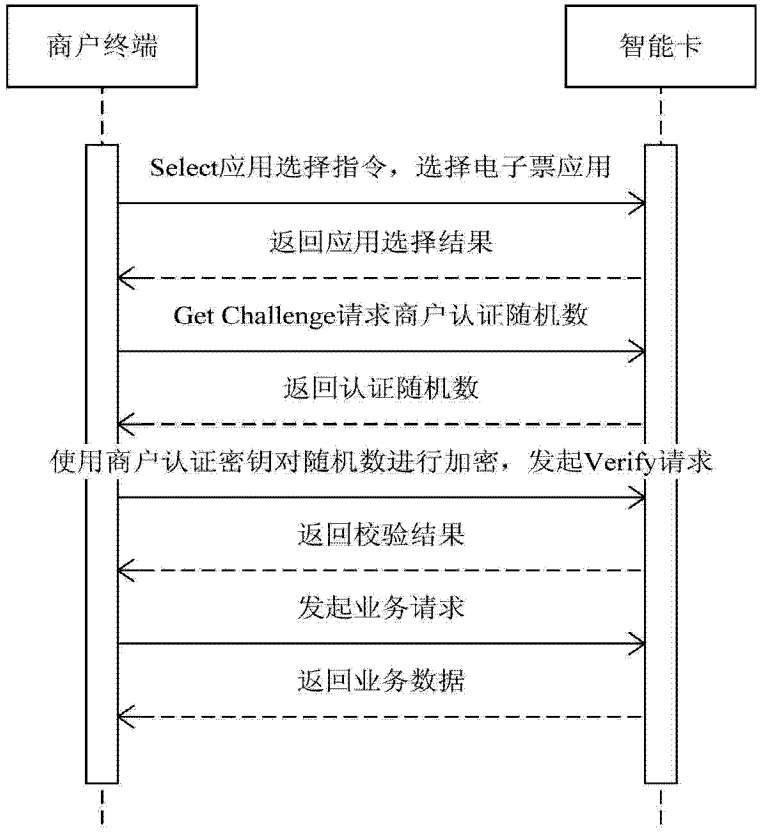

商户终端
智能卡
Select应用选择指令，选择电子票应用
返回应用选择结果
Get Challenge请求商户认证随机数
返回认证随机数
使用商户认证密钥对随机数进行加密，发起Verify请求
返回校验结果
发起业务请求
返回业务数据

图 5