(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 105493116 A
(43)申请公布日 2016.04.13

(21)申请号 201480040189.5

(22)申请日 2014.05.15

(30)优先权数据
61/823,840 2013.05.15 US
2013/03719 2013.05.22 ZA
2013/06249 2013.08.20 ZA

(85)PCT国际申请进入国家阶段日
2016.01.14

(86)PCT国际申请的申请数据
PCT/IB2014/061471 2014.05.15

(87)PCT国际申请的公布数据
WO2014/184771 EN 2014.11.20

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚

(72)发明人 霍雷肖·尼尔森·赫克萨姆
艾伦·约瑟夫·奥里甘
塔拉·安妮·莫斯
霍夫·阿瑞·范威克
约翰·福克塞·希茨

(74)专利代理机构 北京聿宏知识产权代理有限公司 11372
代理人 刘华联 张文娟

(51)Int.Cl.
G06Q 20/40(2006.01)
G06Q 20/32(2006.01)

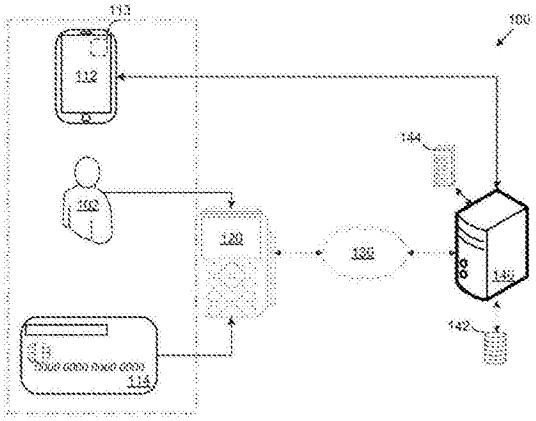
权利要求书4页 说明书24页 附图12页

(54)发明名称

用于提供支付凭证的方法和系统

(57)摘要

一种提供可供移动设备在进行支付时使用的支付凭证的方法和系统。该方法执行在提供系统中，并且包括以下步骤：从接收装置处接收支付凭证，该支付凭证已经从消费者出示在接收设备处的便携式支付设备中获得；从接收设备处接收由消费者输入的标识符；识别对应于标识符的移动设备或安全元件；并且将支付凭证或支付凭证衍生项传递到经识别的移动设备或安全元件中，从而使得该支付凭证或支付凭证衍生项与所述移动设备相关联地被安全地存储。该方法包括：对接收到的支付凭证进行加密，加密的支付凭证具有唯一性解密密钥；并且其中，对支付凭证衍生项进行的传递是来传递唯一性解密密钥。



CN 105493116 A

1.一种用于提供可供移动设备在进行支付时使用的支付凭证的方法，所述方法执行在提供系统中，并且包括以下步骤：

从接收设备处接收支付凭证，所述支付凭证已经从消费者出示在所述接收设备处的便携式支付设备中获得；

从所述接收设备处接收由所述消费者输入的标识符；

识别出对应于所述标识符的移动设备或与所述移动设备相关联的安全元件；并且

将所述支付凭证或支付凭证衍生项传递到经识别的移动设备或所述安全元件，从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储。

2.根据权利要求1所述的方法，其包括：

对接收到的支付凭证进行加密，加密的支付凭证具有唯一性解密密钥；并且

其中，对所述支付凭证衍生项进行的传递是来传递所述唯一性解密密钥；以及

将加密的所述支付凭证存储在所述提供系统中。

3.根据权利要求1所述的方法，其特征在于，所述提供系统是发行机关的远程访问服务器、安全网关或信任服务管理器，并且其中使用安全通信信道将所述支付凭证或所述支付凭证衍生项传递到经识别的移动设备或所述安全元件上。

4.根据权利要求1所述的方法，其特征在于，所述提供系统是在所述接收设备的本地具有处理器的自助服务机，并且其中所述方法包括：

在所述自助服务机和所述移动设备之间建立通信信道，以用于传递所述支付凭证或所述支付凭证衍生项。

5.根据权利要求1所述的方法，包括：

从信任服务管理器请求授权，以访问安全元件；并且

接收安全密钥，以访问所述安全元件。

6.根据权利要求1所述的方法，包括：

将附加凭证传递到经识别的移动设备或所述安全元件上，从而使得所述附加凭证与所述移动设备相关联地被安全地存储，其中在使用中除了需要所述支付凭证或所述支付凭证衍生项之外，还需要所述附加凭证来实施交易。

7.根据权利要求6所述的方法，包括：

使用所述标识符从远程访问服务器中获得所述附加凭证，并且将所述附加凭证转发到所述移动设备。

8.根据权利要求6所述的方法，其特征在于，所述附加凭证是用于生成动态验证值的动态验证算法的形式。

9.根据权利要求1所述的方法，其特征在于，上述接收支付凭证的步骤和上述接收标识符的步骤包括：接收包含了所述支付凭证和所述标识符的单个安全交易消息。

10.根据权利要求1所述的方法，其特征在于，上述识别出对应于所述标识符的移动设备或安全元件的做法包括：

确定是否已经向远程访问服务器注册了对应于所述标识符的移动设备或安全元件，并且如果所述移动设备已经被注册，则识别所述移动设备和/或安全元件的对应通信地址。

11.根据权利要求1所述的方法，其特征在于，上述将所述支付凭证或所述支付凭证衍生项传递到经识别的移动设备从而使得所述支付凭证或所述支付凭证衍生项与所述移动

设备相关联地被安全地存储的做法包括：

将所述支付凭证或支付凭证衍生项传递到所述移动设备，从而使得所述支付凭证或所述支付凭证衍生项被存储在安全元件中，

其中，所述安全元件是如下群组中的一项：设置在所述移动设备中的安全元件、嵌入在位于所述移动设置的通信部件和所述移动设备的通信部件接口之间的层中的安全元件、设置在所述移动设备的通信部件中的安全元件、与所述移动设备相关联的基于云的安全元件。

12.根据权利要求1所述的方法，其特征在于，所述方法重复用于与单个移动设备相关联地对多个支付凭证进行安全存储。

13.根据权利要求1所述的方法，其特征在于，所述方法用于将支付凭证从在第一移动设备上的现有的安全存储传递到第二移动设备上，其中所述便携式支付设备是安全地存储在所述第一移动设备上的现有支付凭证。

14.一种用于提供可供移动设备在进行支付时使用的支付凭证的方法，所述方法执行在销售点设备处，进行并且包括以下步骤：

从消费者出示在接收设备处的便携式支付设备中获得支付凭证；

接收由消费者输入到所述销售点设备中的标识符；

将所述支付凭证和标识符传递到远程访问服务器，以进一步将所述支付凭证或支付凭证衍生项传递到移动设备或者安全元件中，从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储。

15.一种用于提供可供移动设备在进行支付时使用的支付凭证的系统，其包括提供系统，所述提供系统包括：

支付凭证接收器，其用于从接收设备处接收支付凭证，其中已经从消费者出示在所述接收设备处的便携式支付设备中获得了所述支付凭证；

标识符接收器，其用于从所述接收设备处接收由消费者输入的标识符；

识别部件，其用于识别对应于所述标识符的移动设备或与所述移动设备相关联的安全元件；以及

通信模块，其用于将所述支付凭证或支付凭证衍生项传递到经识别的移动设备或者所述安全元件上，从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储。

16.根据权利要求15所述的系统，其特征在于，所述提供系统包括：

加密部件，其用于对接收到的支付凭证进行加密，加密的支付凭证具有唯一性解密密钥；并且其中，对所述支付凭证衍生项的传递是来传递所述唯一性解密密钥。

17.根据权利要求15所述的系统，其特征在于，所述提供系统是发行机关的远程访问服务器、安全网关或信任服务管理器，并且其中用于将所述支付凭证或所述支付凭证衍生项传递到经识别的移动设备或所述安全元件的通信模块使用了安全通信信道。

18.根据权利要求15所述的系统，其特征在于，所述提供系统是在所述接收设备的本地具有处理器的自助服务机，并且其中所述自助服务机包括用于在所述自助服务机和所述移动设备之间建立通信信道的通信模块，以便传递所述支付凭证或者所述支付凭证衍生项。

19.根据权利要求18所述的系统，其特征在于，所述自助服务机用作是远程访问服务器

的中介，并且所述系统包括通信模块，其使用接收到的所述标识符来识别和/或验证远程访问服务器处的用户或账号的服务器。

20.根据权利要求15所述的系统，其特征在于，所述提供系统包括：

授权部件，其用于向信任服务管理器请求授权以访问安全元件，并且接收安全密钥以访问所述安全元件。

21.根据权利要求15所述的系统，其特征在于，所述提供系统包括：

附加凭证部件，其用于将附加凭证传递到经识别的移动设备或所述安全元件，从而使得所述附加凭证与所述移动设备相关联地被安全地存储，其中，在使用中除了需要所述支付凭证或所述支付凭证衍生项以外，还需要所述附加凭证来实施交易。

22.根据权利要求15所述的系统，其特征在于，所述接收设备是如下群组中的一项：与自助服务机相关联的读卡器、销售点设备、自动取款机、商家的销售点终端，或个人PIN输入设备PPED。

23.根据权利要求15所述的系统，其特征在于，所述便携式支付设备是如下群组中的一项：磁条信用卡或借记卡、安全集成电路信用卡或借记卡、银行卡、非接触式银行卡、优惠券卡、存储在移动设备上的现有的支付凭证。

24.根据权利要求15所述的系统，其特征在于，所述标识符是如下群组中一项或多项：移动站国际订户目录号码MSISDN、电子邮件地址、社交网络标识符、预先定义的消费者姓名、消费者帐号。

25.根据权利要求15所述的系统，其特征在于，所述支付凭证接收器和所述标识符接收器经由如下群组中的一项来接收消息：支付处理网络、金融交易消息、ISO8583消息形式的金融交易消息、包含服务器路由代码的金融交易信息。

26.根据权利要求15所述的系统，其特征在于，用于识别出对应于所述标识符的移动设备的识别部件包括以下功能：确定是否已经向远程访问服务器注册了对应于所述标识符的移动设备或安全元件，并且如果所述移动设备已经被注册，则识别出所述移动设备或安全元件的对应通信地址。

27.根据权利要求15所述的系统，其特征在于，上述用于将所述支付凭证或所述支付凭证衍生项传递到经识别的移动设备从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储的所述通信模块包括以下功能：将所述支付凭证或者所述支付凭证衍生项传递到所述移动设备，以将所述支付凭证或者所述支付凭证衍生项存储在安全元件中，

其中，所述安全元件是如下群组中的一项：设置在所述移动设备中的安全元件、嵌在位于所述移动设备的通信部件和所述移动设备的通信部件接口之间的层中的安全元件、设置在所述移动设备的通信部件中的安全元件、与所述移动设备相关联的基于云的安全元件。

28.根据权利要求15所述的系统，其特征在于，所述系统包括销售点设备，所述销售点设备包括：

支付凭证获取得部件，其用于从消费者出示在所述接收设备处的便携式支付设备中获得支付凭证；

标识符接收器，其用于接收由消费者输入到所述销售点设备中的标识符；

通信模块，其用于将所述支付凭证和标识符传递到远程访问服务器，以进一步将所述

支付凭证或所述支付凭证衍生项传递到移动设备，从而使得所述支付凭证或所述付凭证衍生项与所述移动设备相关联地被安全地存储。

29.一种用于提供可供移动设备在进行支付时使用的支付凭证的计算机程序产品，所述计算机程序产品包括存储有用于执行以下步骤的计算机可读程序代码的计算机可读介质：

从接收设备处接收支付凭证，所述支付凭证已经从消费者出示在所述接收设备处的便携式支付设备中获得；

从所述接收设备处接收由消费者输入的标识符；

识别出对应于所述标识符的移动设备或者与所述移动设备相关联的安全元件；并且

将所述支付凭证或者所述支付凭证衍生项传递到经识别的移动设备或所述安全元件，从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储。

30.一种用于提供可供移动设备在进行支付时使用的支付凭证的计算机程序产品，所述计算机程序产品包括存储有用于执行以下步骤的计算机可读程序代码的计算机可读介质：

从消费者出示在接收设备处的便携式支付设备中获得支付凭证；

接收消费者输入到销售点设备中的标识符；

将所述支付凭证和标识符传递到远程访问服务器，以进一步将所述支付凭证或支付凭证衍生项传递到移动设备或安全元件上，从而使得所述支付凭证或所述支付凭证衍生项与所述移动设备相关联地被安全地存储。

用于提供支付凭证的方法和系统

[0001] 相关申请的交叉引用

[0002] 本申请要求于2013年5月15日提交的题为“移动设备供应自助服务机”的美国临时专利申请No.61/823,840、于2013年5月22日提交的题为“向移动设备提供支付凭证”的南非临时专利申请No.2013/03719,以及于2013年8月20日提交的题为“向远程访问服务器提供支付凭证”的南非临时专利申请No.2013/06249的优先权,其全部内容通过引用并入本文。

技术领域

[0003] 本申请涉及提供移动设备可使用的支付凭证的领域。

背景技术

[0004] 随着更多的商家采用能够通过移动设备来进行交易的销售点终端,消费者越来越倾向于用运行在他们的移动设备(例如移动电话)上的数字钱包应用程序来替代他们的实体钱包。通过在移动设备上运行的数字钱包应用程序来进行的交易可以是非接触式的,例如使用移动设备的近场通信(NFC)能力。

[0005] 非接触式支付交易给消费者提供了很大的便利,这是因为其允许消费者进行比基于接触的环境更快而且更便利的采购。在非接触式支付交易中,消费者将能实现非接触的消费者便携式支付设备(CPPD)(例如非接触式智能卡或移动电话)带到接受终端的邻近处。在非接触式CPPD和接受终端之间以无线方式交换例如支付凭证的信息,从而在不需要非接触式CPPD和接受终端之间的直接物理接触的情况下来实施支付交易。在一些情况下,非接触式CPPD和接受终端并非是组合设置的,而是可能位于不同的位置,例如,在不同的城市或国家。在这种情况下,例如经由因特网在非接触式CPPD和接受终端之间传送信息。

[0006] 通常各种标准或合法机关要求被当作非接触CPPD的移动设备需包含安全元件。这样的安全元件与传统的CPPD(例如安全集成电路信用卡)中使用的安全集成电路没什么不同。能与移动设备通信的安全元件通常设有安全存储器和安全处理器,其与移动设备存储器和处理器相分离,并且只能被可信任的应用程序访问,通常仅仅在已经正确地输入特定的个人身份号码(PIN)后才能被访问。其中设置有或嵌入有这样的安全元件的移动设备通常具备邻区通信接口,例如近场通信(NFC)。

[0007] 例如支付凭证的信息可存储在该安全存储器中。在某些情况下,可以经由从信任服务管理器(TSM)发起的空中下载(OTA,over-the-air)通信方法,将这种支付凭证提供给移动设备的安全存储器。通常从安全的数据中心来操作这样的TSM,以便处理能够符合相关标准或合法机关所施加的安全标准。

[0008] 在移动设备上提供数字钱包应用程序是繁琐的任务。例如,为了向移动设备提供凭证以进行非接触式交易(例如非接触支付交易),用户可能需要从他们的移动设备处访问非接触式交易服务提供商以实施OTA提供过程。该提供过程可能需要用户手动地输入用户凭据,例如账号。由于大多数消费者可能有很多个用户希望被包括在数字钱包应用程序中的凭证存储工具(例如来自不同银行的信用卡/借记卡),因此为用户的所有凭证存储工具

输入该信息会是耗时的过程。此外，OTA提供过程可能会给用户带来不期望的无线数据使用费。

[0009] 本发明的实施例旨在至少在一定程度上逐个且共同地解决这些问题和其他问题。

发明内容

[0010] 根据本发明的第一方面，在此提出一种用于提供可供移动设备在进行支付时使用的支付凭证的方法，该方法可以执行在提供系统中，并且包括以下步骤：从接收设备处接收支付凭证，其中该支付凭证已经从消费者出示于接收设备处的便携式支付设备中获得；从接收设备处接收由消费者输入的标识符；识别出对应于标识符的移动设备或与该移动设备相关联的安全元件；并且将支付凭证或支付凭证衍生项传递到经识别的移动设备或安全元件上，从而使得该支付凭证或其衍生项与移动设备相关地被安全地存储。

[0011] 该方法可附加地包括：对接收到的支付凭证进行加密，加密的支付凭证具有唯一性解密密钥。可以以加密的形式来传递支付凭证，同时将唯一性解密密钥存储在提供系统中。在一个实施例中，对支付凭证衍生项的传递是来传递唯一性解密密钥，并且将加密的支付凭证存储在提供系统中。在唯一性解密密钥被传递的情况下，可以从提供系统中清除该唯一性解密密钥。

[0012] 在该方法的实施例中，提供系统是发行机关的远程访问服务器、安全网关或信任服务管理器，并且其中使用安全的通信信道来将支付凭证或支付凭证衍生项传递到经识别的移动设备或安全元件上。

[0013] 在该方法的备选实施例中，提供系统是在接收设备的本地具有处理器的自助服务机，并且其中所述方法包括：在自助服务机和移动设备之间建立通信信道，以用于传递支付凭证或支付凭证衍生项。自助服务机可以用作是远程访问服务器的中介，并且所述方法可以包括：使用所接收的标识符来识别和/或验证远程访问服务器端的用户或帐户。

[0014] 该方法可以包括：从信任服务管理器请求授权，以访问安全元件；并且接收安全密钥以访问安全元件。

[0015] 该方法还可以包括：将附加凭证传递到经识别的移动设备或安全元件中，从而使得该附加凭证与移动设备相关联地被安全地存储，其中在使用中除了支付凭证或支付凭证衍生项之外还需要附加凭证来实施交易。在一个实施例中，附加的凭证可以是卡片验证值。在另一个实施例中，附加凭证可以是用于生成动态验证值的动态验证应用程序或算法的形式。该方法可以包括：使用标识符从远程访问服务器中获得附加凭证，并且将附加凭证转发到移动设备。

[0016] 接收设备可以是以下群组中的一项：与自助服务机相关联的读卡器、销售点设备、自动取款机、商家的销售点终端，或个人PIN输入设备(PPED)。

[0017] 便携式支付设备可以是如下群组中的一项：磁条信用卡或借记卡、安全集成电路信用卡或借记卡、银行卡、非接触式银行卡、优惠券卡、存储在移动设备上的现有的支付凭证。

[0018] 接收到的支付凭证可以包括接收到的磁道1数据、磁道2数据、磁道3数据和磁道2等效数据中的一项或多项。接收到的支付凭证可以包括如下群组中的一项或多项：轨道数据、帐户号码、帐户持有人姓名和/或出生日期、银行识别码(BIN)、主账户号码(PAN)、服务

代码、到期日期、卡片验证值(CVV1或CVV2)、帐户持有人个人详细信息、PIN块或偏移量、银行账号、分支代码、积分账号或标识符、信用卡和/或借记卡号码信息、账户余额信息。

[0019] 标识符可以是如下群组中的一项或多项:移动站国际订户目录号码(MSISDN)、电子邮件地址、社交网络标识符、预先定义的消费者姓名、消费者账号。

[0020] 接收支付凭证的步骤和接收标识符的步骤可以包括:接收包含了支付凭证和标识符在内的单个安全交易消息。该安全交易消息可以是如下群组中的一项或多项:支付处理网络信息、金融交易信息、ISO8583消息形式的金融交易信息、包含服务器路由代码的金融交易消息。服务器路由代码可以用于通过支付处理网络将金融交易消息路由到远程访问服务器。

[0021] 上述识别对应于标识符的移动设备或安全元件的做法可以包括:确定是否已经向远程访问服务器注册了对应于标识符的移动设备或安全元件,并且如果该移动设备已经被注册,则识别移动设备和/或安全元件的对应通信地址。

[0022] 针对识别对应于标识符的移动设备的步骤提出的进一步特征包括:使用标识符来查询数据库的步骤,以便获得与该标识符相关联的移动设备的通信地址。针对将支付凭证传递到移动设备的步骤提出的进一步特征包括:使用通信地址将支付凭证传递到移动设备。

[0023] 上述将支付凭证或支付凭证衍生项传递到经识别的移动设备从而使得该支付凭证或其衍生项与移动设备相关联地被安全地存储的步骤可以包括:将支付凭证或者支付凭证衍生项传递到移动设备,以将该支付凭证或其衍生项存储在安全元件中,其中安全元件是如下群组中的一项:设置在移动设备中的安全元件、嵌入在位于移动设置的通信部件和移动设备的通信部件接口之间的层中的安全元件、设置在移动设备的通信部件中的安全元件、与移动设备相关联的基于云的安全元件。在一个实施例中,安全元件可以嵌入在位于移动设备的通信部件和移动设备的通信部件接口之间的标签,卡或托盘中。

[0024] 该方法可以重复用于与单个移动设备相关联地对多个支付凭证进行安全地存储。

[0025] 该方法可以用于将支付凭证从在第一移动设备上的现有的安全存储器传递到第二移动设备上,其中便携式支付设备是安全地存储在第一移动设备上的现有支付凭证。

[0026] 根据本发明的第二方面,提出了一种用于提供可供移动设备在进行支付时使用的支付凭证的方法,该方法可以执行在销售点设备处,并且包括以下步骤:从消费者出示在接收设备处的便携式支付设备中获得支付凭证;接收由消费者输入到销售点设备中的标识符;将支付凭证和标识符传递到远程访问服务器,以进一步将支付凭证或支付凭证衍生项传递到移动设备或安全元件中,从而使该支付凭证或其衍生项与移动设备相关联地被安全地存储。

[0027] 根据本发明的第三方面,提出了一种用于提供可供移动设备在进行支付时使用的支付凭证的系统,该系统包括提供系统,所述提供系统包括:支付凭证接收器,其用于从接收设备处接收支付凭证,其中已经从消费者出示在接收设备处的便携式支付设备中获得了该支付凭证;标识符接收器,其用于从接收设备处接收由消费者输入的标识符;识别部件,其用于识别对应于标识符的移动设备或与该移动设备相关联的安全元件;以及通信模块,其用于将支付凭证或支付凭证衍生项传递到经识别的移动设备或者安全元件,从而使得该支付凭证或其衍生项与移动设备相关联地被安全地存储。

[0028] 所述提供系统可以包括：加密部件，其用于对接收到的支付凭证进行加密，加密的支付凭证具有唯一性的解密密钥；并且其中对支付凭证衍生项的传递是来传递唯一性解密密钥。

[0029] 在系统的实施例中，所述提供系统是发行机关的远程访问服务器、安全网关或信任服务管理器，并且其中用于将支付凭证或支付凭证衍生项传递到经识别的移动设备或安全元件的通信模块使用了安全通信信道。

[0030] 在备选的实施例中，提供系统是在接收设备本地具有处理器的自助服务机，并且其中自助服务机包括用于在自助服务机和移动设备之间建立通信信道的通信模块，以便传递支付凭证或者支付凭证衍生项。自助服务机可以用作远程访问服务器的中介，并且所述系统包括服务器通信模块，其使用接收到的标识符来识别和/或验证远程访问服务器处的用户或账号。

[0031] 所述提供系统还可以包括：授权部件，其用于向信任服务管理器请求授权以访问安全元件，并且接收安全密钥以访问安全元件。

[0032] 所述提供系统还可以包括：附加凭证部件，其用于将附加凭证传递到经识别的移动设备或安全元件，从而使得该附加凭证与移动设备相关联地被安全地存储，其中，在使用中除了支付凭证或支付凭证衍生项以外，还需要附加凭证来实施交易。在一个实施例中，附加凭证可以是卡片验证值。在另一个实施例中，附加凭证可以是用于生成动态验证值的动态验证应用程序或算法的形式。该方法可以包括使用标识符从远程访问服务器中获得附加凭证，并且将附加凭证转发到移动设备。

[0033] 用于识别对应于标识符的移动设备的识别部件可以包括以下功能：确定是否已经向远程访问服务器注册了对应于该标识符的移动设备或安全元件，如果已经注册了移动设备，则识别出移动设备和/或安全元件的对应的通信地址。

[0034] 上述用于将支付凭证或支付凭证衍生项传递到经识别的移动设备从而使得该支付凭证或支付凭证衍生项与移动设备相关联地被安全存储的通信模块包括以下功能：将支付凭证或者支付凭证衍生项传递到移动设备，以将其存储在安全元件中，其中，安全元件是如下群组中的一项：设置在移动设备中的安全元件、嵌入在位于移动设置的通信部件和移动设备的通信部件接口之间的层中的安全元件、设置在移动设备的通信部件中的安全元件、与移动设备相关联的基于云的安全元件。

[0035] 在另一个的实施例中，所述系统可以包括销售点设备，该销售点设备包括：支付凭证获取部件，其用于从消费者出示在接收设备处的便携式支付设备中获得支付凭证；标识符接收器，其用于接收由消费者输入到销售点设备中的标识符；通信模块，其用于将支付凭证和标识符传递到远程访问服务器，以进一步将支付凭证或支付凭证衍生项传递到移动设备，从而使得该支付凭证或支付凭证衍生项与移动设备相关联地被安全地存储。

[0036] 在本发明的另一个方面中，提供了自助服务机以允许用户从用户凭证存储工具(也被称作便携式支付设备)处向移动设备供应凭证。自助服务机包括凭证存储工具读取器，以从凭证存储工具中检索凭证。自助服务机还包括移动设备接口，以建立与移动设备的通信信道，并且经由该通信信道将凭证从凭证存储工具处加载到移动设备上。

[0037] 根据本发明的第四方面，提供了一种用于提供可供移动设备在进行支付时使用的支付凭证的计算机程序产品，该计算机程序产品包括计算机可读介质，该计算机可读介质

存储有用于执行本发明的第一方面的步骤以及上述列出的一项或多项附加的限定特征的计算机可读程序代码。

[0038] 根据本发明的第五方面，提供了一种用于提供可供移动设备在进行支付时使用的支付凭证的计算机程序产品，计算机程序产品包括计算机可读介质，该计算机可读介质存储有用于执行本发明的第二方面的步骤以及上述列出的一项或多项附加的限定特征的计算机可读程序代码。

[0039] 本发明的进一步的特征提出，计算机可读介质是非暂时性的计算机可读介质，并且通过处理电路来运行该计算机可读程序代码。

[0040] 为了更加充分地理解本发明，现在将参照附图对其实施例进行描述。

附图说明

[0041] 图1是根据本发明的系统的第一实施例的示意图；

[0042] 图2是示出了图1的第一实施例的变体的示意图；

[0043] 图3是示出了图1的第一实施例的变体的示意图；

[0044] 图4A是执行在根据本发明的提供系统处的方法的流程图；

[0045] 图4B是图4A的方法实施例的流程图；

[0046] 图5是执行在根据本发明的销售点设备处的方法的流程图；

[0047] 图6A是根据本发明的系统的一方面的框图；

[0048] 图6B是根据本发明的系统的一方面的框图；

[0049] 图7是根据本发明的方法的一实施例的泳道式流程图；

[0050] 图8是根据本发明的方法的另一实施例的泳道式流程图；

[0051] 图9A示出了根据本发明的系统的第二实施例；

[0052] 图9B是图9A的系统实施例的自助服务机的框图；

[0053] 图9C是图9A的系统实施例的示意图；

[0054] 图9D是图9A的方法实施例的流程图；

[0055] 图10是图9A的实施例的泳道式流程图；

[0056] 图11示出了能实现本发明的各个方面的计算设备的框图；并且

[0057] 图12示出了可以在本发明的各种实施例中使用的通信设备的框图。

具体实施例

[0058] 在下文的详细描述中阐述了许多具体的细节，以提供对本发明的全面理解。但是，本领域技术人员可以理解的是，没有这些具体细节也可以实施本发明。在其他示例中，没有对公知的方法、程序和部件进行详细描述，以便不对本发明造成混淆。

[0059] 对用于提供支付凭证或支付凭证衍生项的方法和系统进行了说明，其中移动设备在进行非接触支付时可以使用该支付凭证或支付凭证衍生项。

[0060] 本发明的实施例包括一种执行在远程访问服务器处的、用于经由接收设备将支付凭证或其衍生项提供给移动设备的方法，其中在该接收设备处可以放入便携式支付设备或凭证存储工具，例如支付卡。接收设备例如可以是销售点设备、自动取款机或其他中间设备。

[0061] 可经由与移动设备相关联的安全元件相连的信道，将支付凭证从远程访问服务器处安全地提供到移动设备。

[0062] 可以将支付凭证提供给移动设备，或者备选地，可以将支付凭证以加密的形式存储在远程访问服务器中并向移动设备提供唯一性解密密钥。

[0063] 本发明的其他实施例提出一种自助服务机，以允许用户从用户的凭证存储工具向移动设备提供凭证。通过提供自助服务机作为用户移动设备和用户凭证存储工具之间的接口，能够避免的手动输入凭证，这是因为这样的凭证能够直接从用户的凭证存储工具被读取。另外，自助服务机可以用作移动设备与参与提供过程的实体(例如发行方或可信服务管理器)之间的通信中介，以避免在提供过程中移动设备使用无线数据。因此，本发明的实施例提供了一种便利且节省成本的方式来使得移动设备具有在非接触式交易中使用的数字钱包应用程序。

[0064] 现在，对这些和其他的实施例进行详细说明。

[0065] 图1示出了根据本发明的实施例的示例性系统(100)的框图。该系统包括消费者(102)的移动设备(112)和便携式支付设备(114)。该系统还包括用于便携式支付设备(114)的接收设备，并且在该实施例中，接收设备是销售点设备(120)的形式。该系统还包括远程访问服务器(140)，在示例性系统(100)中，该远程访问服务器经由支付处理网络(130)与销售点设备(120)进行通信。虽然图中仅示出了一个消费者(102)、一个移动设备(112)、一个便携式支付设备(114)和一个销售点设备(120)，但是应该理解的是，这仅仅是为了说明的目的，并且本发明设想每种设备均有一个或多个。

[0066] 移动设备(112)可以是具有安全元件(113)的任何合适的移动设备。安全元件(113)可以嵌入在移动设备中，可以设置在放置于移动设备(112)的微型SD卡插槽中的微型安全数字(SD)卡中或类似的卡规格中。

[0067] 备选地，安全元件(113)可以设置在移动设备的通信部件内，例如通用集成电路卡(UICC)内。本发明还设想，在一些实施例中，安全元件(113)可以设置在可连接到移动设备上的扩容设备中，或者备选地设置在随后被放置于UICC和移动设备的UICC接口之间的标签、托盘或卡中，以便安全元件可以拦截并适当地处理在UICC和移动设备之间发送的任何通信，并因此可以拦截并适当地处理在移动设备和移动通信网络之间发送的任何通信。

[0068] 还设想安全元件(113)可以是采用主机卡仿真(HCE)的基于云的安全元件，该主机卡仿真(HCE)通过移动设备(112)上被配置为能模仿卡功能的应用程序，来实现外接于移动设备(112)的可网络访问存储。

[0069] 示例性的移动设备包括智能电话、功能性电话、平板电脑、个人数字助理等。移动设备(112)通过例如移动数据或移动通信网络与远程访问服务器进行数据通信，并且至少配置成能安全地接收、存储、发布和传递支付凭证或支付凭证衍生项。例如，移动设备(112)可以是能满足任何适当的金融或支付方案标准(例如，全球平台卡规范)的任何此类设备。本发明的实施例提出，在移动设备(112)上安装合适的移动软件应用程序，所述应用程序允许其用户与耦接于该应用程序(或以基于云的架构与该应用程序相关联)的安全元件(113)进行交互，并且还可促进移动设备(112)和安全元件(113)之间的通信。

[0070] 软件应用程序可以提供：用户接口，其促使将密码输入到移动设备(112)中以便与存储在安全元件(113)中的偏移量进行比较；可供用户从中选择待使用的支付凭证的列表；

针对接收、使用或支付凭证等的通知。用户接口可以包括菜单，从该菜单可以发起这些通信中的至少几项。本发明的实施例还提出，这种接口由SIM应用工具包协议(通常称为STK协议)方案等提供。

[0071] 图示的实施例中的便携式支付设备(114)是安全集成电路银行卡。这种卡也被称为“芯片和密码”卡或“EMV智能卡”。便携式支付设备(114)具有支付凭证，该支付凭证可以是存储在便携式支付设备(114)中的磁道2和/或磁道2等效信息(例如EMV标签57的数据)。磁道2和/或磁道2等效信息可以包括银行识别码(BIN)、主账户号码(PAN)、到期日期、服务代码、自定义数据(例如卡片验证值(CVV))，以及任何相关的间距和冗余校验。除此之外，本发明的实施例提出，便携式支付设备(114)包含支付凭证，该支付凭证可包括如下各项中的任意一项或多项：客户姓名和/或出生日期、BIN、PAN、服务代码、到期日期、CVV1或CVV2号码、PIN块或偏移量、银行账号、分支代码、积分帐号或标识符、信用卡和/或借记号码信息、帐户余额信息和/或其他消费信息。在本发明的其他实施例中，支付凭证可以包括磁道1和/或磁道3信息。

[0072] 销售点设备(120)可以是配置为从合适的便携式支付设备获得支付凭证并且将这些支付凭证传递到支付处理网络或金融机构网络的任何合适的设备。销售点设备(120)可配置为经由任何合适的接触式或非接触式通信接口(例如是可适用的ISO/IEC 7813、ISO/IEC 7816或ISO/IEC 14443标准)从便携式支付设备获得支付凭证。

[0073] 销售点设备(120)可以包括用于从便携式支付设备检索信息的多种手段中的一种或多种，这包括：用户例如通过将磁条卡刷过或插入磁条读卡器或通过将芯片卡插入芯片卡读卡器插槽中，使得便携式支付设备(114)放置为与销售点设备(120)物理接触；或者用户例如通过将非接触式卡放置得非常接近非接触式读卡器或通过将印刷介质(例如，带有条码或快速响应(QR)码)放置在红外线扫描器前，使得便携式支付设备(114)非常靠近点销售设备(120)。

[0074] 在示出的示例性系统(100)中，销售点设备(120)的是手持销售点设备。除此之外，销售点设备(120)配置为接收由消费者经由例如销售点设备(120)的键盘而输入的标识符。

[0075] 销售点设备(120)进一步配置为将支付凭证以及标识符格式化成金融交易消息，并且将该消息传递到支付处理网络(130)。金融交易消息例如可以是ISO8583消息。此外，销售点设备(120)配置为将服务器路由代码插入到金融交易消息中，以便使用服务器路由代码通过支付处理网络(130)将金融交易消息路由到远程访问服务器(140)。服务器路由代码可以设置在金融交易信息的“BIN”字段中。

[0076] 支付处理网络(130)是金融机构和支付处理机构的网络，并且配置为例如在商家、收单方、发行方和其他各方之间引导金融交易消息。这种支付处理网络的一个示例是VisaNet™，其具有作为网络的一部分的多个收单金融机构和发行金融机构。

[0077] 远程访问服务器(140)可以是任何合适的服务器计算机或分布式服务器计算机系统，并且其具有存储在其中的数字存储器内的数据库(142)，并且还具有安全存储器，在优选的实施例中该安全存储器位于远程访问服务器的硬件安全模块(144)中。远程访问服务器(140)配置为从销售点设备(例如120)端接收支付凭证，此时已经从消费者(例如102)出示在该销售点设备(例如120)端的便携式支付设备(例如114)中获得支付凭证。

[0078] 远程访问服务器可配置为对支付凭证进行加密，加密的支付凭证具有唯一解密密

钥。加密可在硬件安全模块(144)中进行。在一个实施例中,对支付凭证进行解密的密钥由远程访问服务器(140)保存,并且将加密的支付凭证发送到移动设备(112)以便将其存储在与移动设备(112)相关联的安全元件(114)中。在另一个实施例中,加密的支付凭证存储在远程访问服务器(140)的硬件安全模块(144)中,并且将解密密钥发送到移动设备(112)以便将其存储在与移动设备(112)相关联的安全元件(113)中。

[0079] 除此之外,远程访问服务器(140)配置为从销售点设备(120)接收由消费者(102)输入到该销点售设备(120)中的标识符。远程访问服务器(140)配置为随后识别与标识符对应的移动设备(例如112)或与移动设备(112)相关联的安全元件(113),并且将支付凭证传递给移动设备(112)以便将其存储在与该移动设备(112)相关联的安全元件(113)中。

[0080] 这可以这样来进行:使用标识符来查询数据库(142),以便获得与该标识符相关联的移动设备(112)的通信地址。随后,使用该通信地址将支付凭证发送到移动设备(112)。远程访问服务器接收的标识符例如可以是移动站国际订户目录号码(MSISDN)、电子邮件地址、社交网络标识符、预先定义的消费者姓名、消费者账号等中的任意一项或多项。类似地,移动设备的通信地址例如可以是MSISDN、电子邮件地址、社交网络标识符、预先定义的消费者姓名、消费者账号等中的任意一项或多项。标识符和通信地址可以是相同的。

[0081] 本发明的实施例提出,远程访问服务器配置为使由如下项构成的群组中的一项或多项相关联:标识符、解密密钥、加密支付凭证,以及具有数据库中的用户文档的通信地址。

[0082] 在本发明的一些实施例中,远程访问服务器(140)所起的作用可类似于信任服务管理器(TSM)的作用,并且其可相应地满足由相关的金融或支付方案标准(例如,全球平台卡规范)所施加的任何安全性要求或数据完整性要求。

[0083] 在使用中,消费者(102)可能希望将他或她的支付凭证或其衍生项提供给他或她的移动设备上(112)安全元件(113),以便移动设备(112)可用于在实体商家或网上商家处进行非接触式支付。

[0084] 为此,例如,那种已经向远程访问服务器(140)注册了他或她的移动设备(112)并且已将该移动设备(112)与标识符和通信地址进行了关联的消费者可以到访实体商家,并且向商家出示他或她的便携式支付设备(114)。便携式支付设备(114)与商家的销售点设备(120)交互,并且在销售点设备(120)上选择例如“凭证传送”菜单选项。消费者(102)被提示输入他或她进入销点售设备(120)的PIN,此后,消费者(102)被提示输入他或她的标识符。消费者(102)将其预设的标识符(已向远程访问服务器(140)注册了该标识符)输入到销售点设备(120)中。

[0085] 接收到消费者的PIN后,销售点设备(120)能够从便携式支付设备(114)中提取出的支付凭证。销售点设备(120)将支付凭证格式化成金融交易的消息。销售点设备(120)还可在金融交易消息中包括标识符以及服务器路由代码。服务器路由代码可以类似于BIN并确保通过支付处理网络(130)将金融交易消息路由到远程访问服务器(140)。

[0086] 金融交易消息在远程访问服务器(140)处被接收。远程访问服务器使用包含在金融交易消息中的标识符来识别与移动设备(112)相关联的通信地址。远程访问服务器(140)使用通信地址将支付凭证或支付凭证衍生项传递给移动设备(112),以便将该支付凭证或支付凭证衍生项存储在与该移动设备(112)相关联的安全元件(113)中。

[0087] 随后,支付凭证被移动设备(112)接收并且被安全地存储在移动设备(112)的安全

元件(113)中。在支付凭证被存储在安全元件之前，可以提示用户输入PIN。在一些实施例中，经由空中下载式(OTA)提供，从远程访问服务器(140)向移动设备(112)提供支付凭证，并将支付凭证存储在安全元件(113)中。因此，这能够让用户使用他或她的移动设备(112)作为便携式支付设备来进行非接触式支付，其中由移动设备(112)提供给经适当配置的商家销售点设备的凭证是用户的便携式支付设备(114)的凭证。

[0088] 在一些实施例中，远程访问服务器(140)可以对支付凭证进行加密，并且将唯一性解密密钥与支付凭证相关联。然后，可将加密的支付凭证或解密密钥中的任一者存储在安全存储器(例如远程访问服务器的硬件安全模块(144))中。可将加密支付凭证或解密密钥中的另一者发送到与移动设备(112)相关联的安全元件(113)中。可使用任何合适的加密算法对支付凭证进行加密，使得一旦被加密，则仅可使用唯一性解密密钥对支付凭证进行解密。如果将解密密钥发送到移动设备(112)以便将其存储在安全元件(113)中，则该解密密钥既不会存储在远程访问服务器中，也不会存储在其硬件安全模块中。

[0089] 移动设备(112)接收到的加密支付凭证或解密密钥安全地存储在移动设备(112)的安全元件(113)中。用户可能会被提示在加密支付凭证或解密密钥被存储在安全元件中之前输入PIN。在一些实施例中，经由空中下载(OTA)式提供，将解密密钥从远程访问服务器(140)提供到移动设备(112)并存储在安全元件(113)中。

[0090] 在将作为解密密钥形式的支付凭证衍生项存储在与移动设备(112)相关联的安全元件(113)中的预案中，作为进行交易的支付方法，用户可将标识符出示给商家。商家可以从远程访问服务器(140)端请求支付凭证，并且于此同时将标识符传递到远程访问服务器(140)。远程访问服务器(140)可以使用接收到的标识符来识别移动设备(112)，并且从经识别的移动设备(112)处请求解密密钥。在接收到该请求时，移动设备(112)随后在向远程访问服务器(140)传递相关的解密密钥之前提示用户输入PIN、密符或密码，以便可以对对应的加密支付凭证进行解密，并将其传递给商家和/或商家的收单方和/或支付处理网络，以便能够完成交易。

[0091] 图2示出了根据本发明第二实施例的示例性系统(200)。该系统类似于图1中示出的系统，并且类似的附图标记指代相同的系统、实体或设备。图2的系统(200)不同于图1的系统之处在于，本实施例中的销售点设备是自动取款机(ATM)(222)。ATM(222)可以是任何合适的ATM，并且配置为从消费者(202)的便携式支付设备(214)处获得支付凭证并将这些支付凭证传递到支付处理网络(230)或金融机构网络。ATM(222)可配置为经由任何适当的接触式或非接触式通信接口(例如读卡器接口或近场通信(NFC)接口)从便携式支付设备(214)处获得支付凭证。

[0092] 示出的实施例中的ATM(222)配置为接收由消费者(202)通过例如ATM(222)键盘而输入的标识符。ATM(222)还配置为将支付凭证以及标识符格式化为金融交易消息，并将该消息传递到支付处理网络(230)。金融交易消息例如可以是ISO 8583消息。此外，ATM(222)配置为将服务器路由代码插入到金融交易消息中，以便使用该服务器路由代码将金融交易消息通过支付处理网络(230)路由到远程访问服务器(240)。服务器路由代码可以设置在金融交易信息的“BIN”字段中。

[0093] 如在上文中已经描述的那样，一旦在远程访问服务器处接收到支付凭证，则将支付凭证或支付凭证衍生项传递给移动设备，以便将其存储在移动设备的安全元件中。

[0094] 用户(202)可以以与图1的系统类似的方式来使用系统(200)。用户(202)将他或她的便携式支付设备(214)出示给ATM(222)的便携式支付设备接口。用户会被提示输入PIN，响应于PIN的正确输入，用户(202)从ATM(222)的屏幕上显示的菜单中选择“凭证传送”选项。用户(202)还会被提示输入标识符，他或她经由ATM(222)的键盘将该标识符输入ATM(222)。ATM(222)从便携式支付设备(214)获得支付凭证，并且将支付凭证、标识符、以及服务器路由代码格式化成金融交易消息，该金融交易消息随后被发送到支付处理网络(230)并且从那里被路由到远程访问服务器(240)。类似于图1的使用中预案，支付凭证随后被传递到用户的移动设备(926)，以便存储在该移动设备的安全元件中。

[0095] 图3示出了根据本发明的第三实施例的又一示例性系统(300)。该系统(300)类似于图1和2示出的系统，并且类似的附图标记指代相同的系统、实体或设备。图3的系统(300)不同于图1和图2的系统之处在于，移动设备(316)不具有嵌入式的安全元件。但是，移动设备(316)具有其中设置有安全元件的加密扩展标签(318)。加密扩展标签(318)具有设置在其顶面和底面上的电触点，这些电触点分别与移动设备(316)的通信部件(317)和通信部件接口配合。随后，可将加密扩展标签(318)附接到插入在移动设备(316)的通信托架中的通信部件(317)上，使得安全元件可以拦截并适当地处理在通信部件(317)和移动设备(316)之间发送的任何通信，并因此拦截并适当地处理在移动设备(316)和移动通信网络之间发送的任何通信。在示出的实施例中，通信部件是通用集成电路卡(UICC)。

[0096] 图4A示出了根据本发明方面的一个实施例的方法的流程图。该方法执行在提供系统中，该提供系统可以是类似于上文中参照图1到图3描述的那种远程访问服务器，或者可以是下文中相对于图9A至图9D进一步描述的专用自助服务机。

[0097] 该方法包括一系列步骤，其第一步骤(402)是：从接收设备接收支付凭证，该接收设备可以是参照图1到图3描述的销售点设备，或者该接收设备可以合并到销售点设备中或要与销售点设备相关联地使用，或者可以是参照图9A至图9D的自助服务机的凭证存储工具读取器，或者是用于接收支付凭证的另一种形式的接收设备。销售点设备例如可以是自动取款机、商家销售点终端或个人PIN输入设备(PPED)。

[0098] 从销售点设备接收到的支付凭证是从消费者出示在接收设备处的便携式支付设备(以下关于图9A到图9D的实施例中也被称作凭证存储工具)中获得的。便携式支付设备可以是信用卡或借记卡，其可以是磁条银行卡、安全集成电路银行卡或非接触式银行卡中的任意一种。支付凭证可以是磁道1数据、磁道2数据、磁道3数据或磁道2等效数据(例如EMV标签57数据)。此外，支付凭证可以包括账户持有人姓名和/或出生日期、银行识别码(BIN)、主账户号码(PAN)、服务代码、到期日期、卡片验证值(CVV1或CVV2)、PIN块或偏移量、银行账号、分支代码、积分账号或标识符、信用卡和/或借记卡号码信息、帐户余额信息，和/或消费者信息(例如姓名、出生日期)。支付凭证可经由支付处理网络被远程访问服务器接收。

[0099] 该方法包括从接收设备接收的标识符的步骤(404)，所述接收设备例如是销售点设备或自助服务机用户输入接口。标识符可以是移动站国际订户目录号码(MSISDN)、电子邮件地址、社交网络标识符、预先定义的消费者姓名或消费者账号中的任意一项或多项。在本发明的优选实施例中，在远程访问服务器处接收金融交易消息(例如是ISO8583消息)中的支付凭证和标识符。另外，也可以经由支付处理网络将金融交易消息从销售点设备处传递到远程访问服务器。金融交易消息可以相应地包括服务器路由代码，以便支付处理网络

能够将金融交易消息路由到远程访问服务器。

[0100] 该方法包括下一步骤(406):识别与标识符对应的移动设备和/或移动设备的安全元件。该步骤可包括这样的步骤:即,确定是否已经在远程访问服务器上注册了对应于该标识符的移动设备和/或安全元件,以及如果已经注册了移动设备和/或安全元件,则识别出该移动设备和/或安全元件的对应的通信地址。这可以通过使用标识符来查询远程访问服务器的数据库来进行,从而获得与该标识符相关联的移动设备和/或安全元件的通信地址。

[0101] 作为任选的附加步骤(408),可以向信任服务管理器(TSM)发送注册或激活请求,所述信任服务管理器管理用于访问安全元件的安全密钥或令牌。请求可以包括标识符。TSM可以授权对与移动设备相关联的安全元件进行解锁。TSM可以设置在远程访问服务器上,或者可以由单独的远程访问服务器上提供的远程服务来提供。

[0102] 该方法包括步骤(410):将支付凭证传递到移动设备以便将其存储在与移动设备相关联的安全元件中。这可以包括:使用通信地址将支付凭证传递到移动设备。这还可以包括:使用安全元件的识别代码将支付凭证传递到与移动设备相关联的安全元件,以建立与安全元件通信的安全信道,该安全通道可以经由移动设备来建立。在一些进一步相对于图4B描述的实施例中,将支付凭证衍生项传递到移动设备或安全元件,例如,支付凭证衍生项可以是对应于远程存储的加密支付凭证的解密密钥。

[0103] 作为又一任选的附加步骤(412),可以由远程访问服务器请求或提供附加凭证。附加凭证可以是不能从便携式支付设备中自动地读取的凭证,例如是可由人从便携式支付设备上读取的印刷卡片验证值(例如CVV2号码)。在这种情况下,附加凭证可以由远程访问服务器来请求,并经由销售点设备从消费者处获得。

[0104] 附加凭证还可以包括用于生成针对个体交易的动态卡片验证值(dCVV)的动态卡片验证值软件。在提供过程中,这种附加凭证可以使用标识符来识别,并且通过远程访问服务器或单独的远程访问服务器来提供。可以将附加凭证传递到与移动设备相关联的安全元件。可以将这些附加凭证与支付凭证或支付凭证衍生项分开传递。

[0105] 如上文所描述的那样,根据本发明的一些实施例,移动设备的安全元件可以嵌入在标签、卡或托盘中。在将支付凭证传递到移动设备之前,远程访问服务器可以使用多种加密算法中的任意一种对支付凭证进行加密。示例性的加密算法包括:高级加密标准(AES)、数据加密标准(DES)、三重数据加密标准/算法(TDES/TDEA)、安全套接字层(SSL)、Blowfish算法、Serpent算法、Twofish算法、国际数据加密算法(IDEA)、Rivest,Shamir和Adleman(RSA)算法、数字签名算法(DSA)、微型加密算法(TEA)、扩展TEA(XTEA),和/或其他的加密算法或协议。在一些实施例中,解密密钥(也被称为专用密钥)存储在与标识符相关联的远程访问服务器的安全存储器中,以便在例如向商家出示之前只有远程访问服务器或其硬件安全模块可以对支付凭证进行解密。在本实施例中,支付凭证以其加密形式存储在移动设备的安全元件中。

[0106] 图4B示出了根据本发明方面的另一实施例的方法的流程图。该方法执行在远程访问服务器(例如图1到图3中的远程访问服务器)中。该方法包括一系列步骤,其中的第一步骤(422)是从接收设备(例如类似于图4A的步骤(402)中的销售点设备)接收支付凭证。

[0107] 该方法包括下一步骤(424):从接收设备(例如类似于图4A的步骤(404)的销售点设备)接收标识符。

[0108] 该方法包括以下步骤(426):对支付凭证进行加密。可以使用任何适当的算法对支付凭证进行加密,并且一旦被加密则仅具有唯一性解密密钥。示例性加密算法包括但不限于:高级加密标准(AES)、数据加密标准(DES)、三重数据加密标准/算法(TDES/TDEA)、安全套接字层(SSL)、Blowfish算法、Serpent算法、Twofish算法、国际数据加密算法(IDEA)、Rivest,Shamir和Adleman(RSA)算法、数字签名算法(DSA)、微型加密算法(TEA)、扩展TEA(XTEA),和/或其他的加密算法或协议。

[0109] 由于对于那些支付凭证来说解密密钥是唯一的,因此仅可以用那个解密密钥来对那些支付凭证进行解密。唯一性解密密钥(在一些实施例中是专用密钥)与加密支付凭证存储在不同的位置中。

[0110] 该方法包括下一步骤(428):将加密支付凭证或解密密钥中的一者存储在远程访问服务器的安全存储器中,在优选的实施例中,该安全存储器是硬件安全模块。可以将加密支付凭证或唯一性解密密钥、通信地址以及标识符与存储在远程访问服务器的数据库中的用户文档相关联。例如,一旦接收到唯一性解密密钥,则可以识别出存储在硬件安全模块中的对应的支付凭证。

[0111] 该方法包括以下步骤(430):识别对应于标识符的移动设备和/或安全元件。这个步骤类似于图4A的步骤(406)。

[0112] 该方法包括最终步骤(432):将加密支付凭证和唯一性解密密钥中的另一者传递给移动设备,以便将其存储在与移动设备相关联的安全元件中。这可以包括通过通信地址来传递到移动设备。如上文所描述的那样,根据本发明的一些实施例,移动设备的安全元件可以嵌入在标签、卡或托盘中。

[0113] 由于仅能将加密支付凭证和解密密钥中的一者存储在移动设备的安全元件中,因此无法对加密支付凭证进行解密,并且因此无法使用该加密支付凭证。

[0114] 在将加密支付凭证存储在远程访问服务器处并且将唯一性解密密钥传送到移动设备的安全元件的预案中,唯一性解密密钥被清除并且不得存储在远程访问服务器的硬件安全模块中。

[0115] 这个预案被认为是与将支付凭证存储在移动设备的安全元件中的预案相反的,该预案的优势在于,如果移动设备的安全元件被入侵,则仅可能获得加密支付凭证的解密密钥。此外,在该安全元件被入侵的情况下,可以简单地撤销存储在该安全元件中的解密密钥,而不必重新颁发支付凭证。

[0116] 图5示出了根据本发明另一方面的方法的流程图。该方法执行在经适当修改的销售点设备(例如是上文参照图1到图3所描述的那些销售点设备中的任一者)中。

[0117] 该方法包括第一步骤(502):从消费者出示在销售点设备处的便携式支付设备上获得支付凭证。这可以通过与传统支付凭证访问操作相类似的方式来进行,例如通过ISO 7816或ISO/IEC 14443通信协议等来进行。所获得的支付凭证可被当作“持卡”支付凭证,这是由于这些支付凭证为后续交易提供了足以被认为是持卡交易所能使用的充分支付凭证。支付凭证例如可以是磁道1数据、磁道2数据、磁道3数据或磁道2等效数据(例如EMV标签57数据)。此外,支付凭证可以包括账户持有人姓名和/或出生日期、银行识别码(BIN)、主账户号码(PAN)、服务代码、到期日期、卡片验证值(CVV1或CVV2)、PIN块或偏移量、银行账号、分支代码、积分账号或标识符、信用卡和/或借记卡号码信息、帐户余额信息,或消费者信息

(例如姓名、出生日期)。

[0118] 该方法包括下一步骤(504):接收由消费者输入到销售点设备中的标识符。标识符可以是移动站国际订户目录号码(MSISDN)、电子邮件地址、社交网络标识符、预先定义的消费者姓名或消费者账号中的一种或多种中的任意一项或多项。

[0119] 该方法还包括下一步骤(506):将支付凭证和标识符传递到远程访问服务器,以便进一步传递到与消费者移动设备相关联的安全元件。这个步骤可能包括将支付凭证和标识符格式化成金融交易消息。金融交易消息例如可以是ISO8583金融交易消息。销售点设备还可配置为将服务器路由代码插入到金融交易消息中,以便通过支付处理网络将金融交易消息路由到远程访问服务器,而不是路由到例如由原本包含在支付凭证中的BIN所指示的发行银行。

[0120] 如果要求,则可以由消费者在销售点设备处输入附加凭证(例如,非机器可读的卡片验证值(例如,CVV2数据)),并将其传递到远程访问服务器。

[0121] 图6A中示出了用于提供支付凭证的远程访问服务器,其例如是图1、图2和图3中的远程访问服务器。远程访问服务器(140)具有用于接收支付凭证的支付凭证接收器(602)。可以从销售点设备接收到支付凭证,其中销售点设备已从消费者出示的便携式支付设备上获得了支付凭证。远程访问服务器(140)具有用于从销售点设备处接收由消费者输入的标识符的标识符接收器(604)。在一些实施例中,支付凭证接收器(602)和标识符接收器(604)可以设置成单个的接收器,该单个的接收器可配置为接收金融交易消息中的支付凭证和标识符。在一些实施例中,金融交易消息可以是ISO 8583消息。

[0122] 远程访问服务器(140)可以包括用于对接收到的支付凭证进行加密的加密部件(606),加密的支付凭证具有唯一性的解密密钥。远程访问服务器(140)可以具有合并在其中的或与远程访问服务器(140)相关联的安全存储器(608),以便存储加密支付凭证或唯一性解密密钥中的一者。在示出的实施例中,安全存储器(608)和加密部件(606)位于远程访问服务器(140)的硬件安全模块(644)内。

[0123] 远程访问服务器(140)可以包括用于识别对应于标识符的移动设备和/或安全元件的识别部件(610)。在示出的实施例中,识别部件(610)构成了远程访问服务器(140)的数据库(642)的一部分,其中可以将标识符、解密密钥、加密支付凭证和通信地址的群组中的一项或多项与用户文档相关联。

[0124] 远程访问服务器(140)还包括用于与经识别的移动设备通信或与关联于该移动设备相的安全元件通信的通信模块(612)。通信模块可以经由任何合适的移动通信网络或移动数据网络来与移动设备进行通信。通信模块(612)可以经由移动设备来建立与安全元件的安全通信信道,以用于传递加密支付凭证或唯一性解密密钥中的一者。

[0125] 远程访问服务器(140)可以任选地包括用于将注册或激活请求发送到可信任管理服务器(TSM)的授权部件(646),其中所述可信任管理服务器对用于访问安全元件的安全密钥或令牌进行管理。

[0126] 远程访问服务器(140)可以任选地包括附加凭证部件(648),该附加凭证部件(648)用于请求或提供用以传递到移动设备或安全元件的附加凭证。附加凭证部件(648)可以经由销售点设备向消费者请求附加凭证(例如,可由人来读取的卡片验证值),该附加凭证被转发用以存储在与移动设备相关联的安全元件上。备选或附加地,附加凭证部件(648)

可提供存储在远程访问服务器或相关的远程服务器处的附加凭证，其中该附加凭证部件(648)例如是以用于生成针对个体交易的动态卡片验证值(dCVV)的动态卡片验证值软件的形式。转发所提供的附加凭证，以将其存储在与移动设备相关联的安全元件上。

[0127] 图6B中示出了用于提供支付凭证的销售点设备，其例如是图1、图2和图3中的销售点设备。

[0128] 销售点设备(120)可以包括支付凭证获取部件(652)，其可以是如上所述的读卡器或扫描器的形式。销售点设备(120)还可以包括用于接收由消费者输入的标识符的标识符接收器(654)。

[0129] 销售点设备(120)可以包括用于与远程访问服务器通信的通信模块(656)。通信模块(656)可以使用金融交易消息与远程访问服务器安全地进行通信。

[0130] 在一些实施例中，销售点设备(120)可以包括用于将注册或激活请求发送到可信任管理服务器(TSM)的授权部件(658)，其中所述可信任管理服务器对用于访问安全元件的安全密钥或令牌进行管理。

[0131] 在其他实施例中，销售点设备(120)可以包括用于从消费者处接收附加凭证的附加凭证接收器(659)，该附加凭证例如是不能被支付凭证获取部件(652)获得的印刷卡片验证值的形式。

[0132] 图7示出的根据实施例的泳道式流程图示出了在移动设备(112)、销售点设备(120)和远程访问服务器(140)之间的流程。远程访问服务器(140)可以由金融机构或服务提供商来提供。在一个实施例中，远程访问服务器(140)是支付处理网络的一部分。

[0133] 消费者可以在销售点设备处出示(701)他的便携式支付设备(例如，支付卡)，该销售点设备可以从便携式支付设备中提取支付凭证。消费者还可以提供(702)标识符。例如，消费者可以向商家出示他的支付卡(可将其插入到销售点设备中)，并且可以请求“凭证传送”交易。消费者会被提示输入支付卡PIN，该支付卡PIN可通过键盘输入到销售点设备中。销售点设备还可以提示消费者输入用作是消费者和他的移动设备的标识符的“别名”。

[0134] 销售点设备可以将所提取的支付凭证和标识符格式化(703)成交易消息，例如ISO 8583消息。这个消息类似于是普通的销售交易消息加上所提供的标识符。BIN字段可以填充以支付处理网络BIN，以便将消息路由到支付处理网关，而不是路由给发行方。消息中还设置消费者的BIN。

[0135] 远程访问服务器接收(704)交易信息，并提取出支付凭证和标识符。该标识符用于识别(705)以下的一项或多项：具有经注册的移动设备和/或安全元件的消费者、具有经注册的移动设备和/或安全元件的帐户，或者移动设备和/或安全元件自身。

[0136] 远程访问服务器可以对支付凭证进行加密(706)，并且可以特别针对支付凭证产生唯一性的解密密钥。可以将加密的支付凭证和唯一性解密密钥中的一者安全地传递(707)到与移动设备相关联的安全元件，而将加密支付凭证和唯一性解密密钥元件中的另一者存储(708)在远程访问服务器处。

[0137] 与移动设备相关联的安全元件可以接收(709)加密支付凭证或唯一性解密密钥，并且可以提示用户输入PIN(710)，其中对PIN偏移量的存储与支付凭证或解密密钥相关联，从而使得仅在输入正确的PIN的情况下安全元件才能释放支付凭证。

[0138] 图8是示出了根据所描述的方法实施例在移动设备(112)、销售点设备(120)以及

远程访问服务器(140)之间的流程的泳道流程图，在该方法中将支付凭证的解密密钥提供到与移动设备相关联的安全元件。

[0139] 作为进行交易的支付方法，消费者可以向商家出示(801)的标识符。商家可以从远程访问服务器处请求(802)支付凭证，该远程访问服务器根据请求发送标识符。

[0140] 远程访问服务器可以使用所接收的标识符来识别(803)与安全元件相关联的移动设备，该安全元件中存储有解密密钥。远程访问服务器可以通过经由移动设备的、与安全元件进行的安全通信来请求(804)解密密钥。

[0141] 移动设备在接收到请求时，会在将解密密钥传递(806)到远程访问服务器之前提示(805)消费者输入PIN。

[0142] 远程访问服务器可以从其存储器中检索(807)加密支付凭证，并且使用解密密钥对支付凭证进行解密(808)。随后传送(809)支付凭证，并且使用安全信道在销售点设备或其他中介处接收(810)该支付凭证以完成交易。

[0143] 根据本发明的实施例，在远程访问服务器处而不是在移动设备的安全元件中存储加密的支付凭证的优势在于，如果移动设备的安全元件受到恶意的第三方的入侵并且被那个第三方获得了存储于其中的信息，则第三方获得的信息将不包括支付凭证。这与将支付凭证存储在安全元件中的预案相反，在这种预案下第三方可以获得支付凭证并欺诈性地利用这些支付凭证。

[0144] 除了这一点以外，在安全元件被入侵或丢失的情况下，可以简单地撤销存储在其中的解密密钥，而不必重新颁发支付凭证。

[0145] 在远程访问服务器处而不是在移动设备的安全元件中存储加密的支付凭证的另一优点在于，移动设备不需要满足相关标准或合法机关施加的安全标准。例如，安全元件不必遵循EMV，或可以不必须满足PCI DSS要求。

[0146] 类似地，由于唯一性解密密钥仅存储在消费者移动设备的安全元件中，因此在解密密钥没有从安全元件(该解密密钥安全地存储在该安全元件)中释放的情况下，无法对相应的加密支付凭证进行解密，并因此无法对其加以使用。因此，消费者对何时使用他或她的支付凭证具有终极的控制权。此外，如果远程访问服务器被恶意的第三方入侵，则在没有对应的唯一性解密密钥的情况下，存储在远程访问服务器中的加密支付凭证对于该第三方来说将是无用的。

[0147] 现在描述图9A至图9D，其示出了本发明的备选实施例，在该实施例中提供系统由自助服务机(901)来提供。

[0148] 图9A示出了自助服务机(901)，其可以设置在零售商店、商场、机场以及其他公共场所中。例如，自助服务机(901)可便捷地设置在移动设备零售商或移动网络运营商那里，以允许用户向其新购买的移动设备提供数字钱包功能。在一些实施例中，自助服务机(901)可以和防盗硬件一起被螺栓固定在地板或墙壁上。自助服务机(901)也可以实现为足够小型、轻巧且紧凑以方便携带，从而可以容易地将自助服务机(901)从一个位置移动到另一个位置。例如，在一些实施例中，自助服务机(901)可以实现为类似于平板计算机或笔记本电脑的规格。

[0149] 自助服务机(901)包括显示器(902)、移动设备接口(910)和凭证存储工具读取器(920)。显示器(902)可以用壳体包围。可以将显示器(902)放置在合适的高度(例如，放置在

支架上),以允许用户容易地阅读或看到显示器(902)上提供的信息或图像。显示器(902)可用于在数字钱包提供过程中向用户提供指令。在自助服务机(901)不使用时,显示器(902)还可以用于显示广告、视频和/或其他图像。显示器(902)还可用作例如触摸屏显示器的用户输入接口,以接收用户输入。

[0150] 移动设备接口(910)用于在自助服务机(901)和移动设备之间建立通信信道或链路。移动设备可以是移动电话、个人数字助理、平板计算设备、便携式媒体播放设备,或能够存储和运行数字钱包应用程序的其他合适的便携式计算设备。移动设备接口(910)可以是如图所示的可插入在移动设备的物理通信端口中的物理连接器。例如,物理连接器可以是可插入在移动设备的USB端口(例如,迷你USB)中的USB连接器。物理连接器还可以是与一些移动设备制造商的专用通信端口相兼容的专用连接器。物理连接器可以设置为插头、从自助服务机(901)的壳体延伸出的电缆(例如,伸缩电缆、外部电缆等)的一部分,或者设置为内置于自助服务机(901)壳体内的扩展坞或支架的一部分。在一些实施例中,自助服务机(901)可以包括多种类型的连接器,以便自助服务机(901)可以与多个移动设备制造商相兼容。在一些实施例中,移动设备接口(910)可以是无线接口(例如,无线收发器),该无线接口用于在数字钱包提供过程中使用NFC、RF、蓝牙、Wi-Fi或其他无线通信协议来建立与移动设备的点对点通信信道。自助服务机(901)还可以包括一个或多个物理连接器与一个或多个无线接口的结合,其可用于建立与移动设备的通信信道。

[0151] 自助服务机(901)的凭证存储工具读取器(920)用于读取或访问凭证存储工具(905)(本文中也称作便携式支付设备),以获得存储在凭证存储工具(905)上的凭证和/或其他用户或帐户信息。凭证存储工具读取器(920)可以是磁条读取器或芯片卡读取器,其经由与凭证存储工具(905)进行物理接触而从凭证存储工具(905)处读取凭证。凭证存储工具读取器(920)可以是例如条形码或QR码扫描器的红外线扫描器,以读取被编码为图像的凭证,或者凭证存储工具读取器可以是能够经由NFC、RF、蓝牙、Wi-Fi或其他无线通信协议与凭证存储设备(905)进行通信的非接触式读卡器,以在凭证存储工具(905)非常接近自助服务机(901)时以非接触方式从凭证存储工具(905)处读取凭证。在一些实施例中,自助服务机(901)可以包括一种或多种上述凭证存储工具读取器。

[0152] 凭证存储设备(905)可以是卡片(例如,信用卡/借记卡或其他支付卡、身份证卡、驾驶执照卡、交通卡、通达卡、保险卡、零售积分卡、礼品卡等)的形式或其他合适的结构。凭证存储工具(905)可以包括用于存储用户的凭证的磁条和/或存储芯片。凭证存储设备(905)还可以是打印介质,其包括对用户凭证进行编码的图像(例如条形码或QR码)。在一些实施例中,凭证存储工具(905)还可以是其中存储有用户凭证的用户的现有移动设备。

[0153] 凭证可以包括存储在凭证存储工具上的、可用于通过凭证存储工具来进行交易的信息。例如,凭证可以是用于识别和/或验证用户的信息,或者用于识别或访问与凭证存储工具相关联的帐户的信息。凭证可以包括财务信息、身份信息、账户信息、交通信息(例如,地铁票或火车票中的信息)、通行信息(例如,通行徽章中的信息)等。凭证的一些示例包括银行账户信息、主账户号码(PAN)、银行识别码(BIN)、信用卡或借记卡号码、到期日期、姓名、用户名、出生日期、驾驶执照号码、地址、社交安全号码、护照号码、保险单号码(例如医疗或自动保险账号)、零售或旅行积分计划账号、礼品卡号码、交通费用账号、雇员身份号码等。凭证还可以包括用于促成交易的附加信息。例如,凭证可以包括用于促成交易处理的卡

片验证值(CVV)和/或服务代码。

[0154] 在一些实施例中，凭证还可以包括用于促成交易、但是没有存储在凭证存储设备(905)上或者不能被自助服务机(901)的凭证存储工具读取器(920)检索到的附加信息。例如，凭证可以包括印刷在信用卡的表面上但可能无法通过读取卡片的磁条而被检索到的卡片验证值2(CVV2)。凭证还可以动态地包括用于生成针对个体交易的动态卡片验证码(dCVV)的动态卡片验证码软件。对于这种未存储在凭证存储设备(905)上或者无法通过凭证存储工具读取器(920)检索到的凭证，自助服务机(901)可以在提供过程中从凭证存储工具(905)的发行方处获得这样的凭证，以便可以将这些凭证加载到移动设备上。

[0155] 凭证可以存储在凭证存储工具(905)的存储器芯片中，或可以被编码为印刷在凭证存储工具(905)上的图像。存储在凭证存储工具(905)中的凭证也可以以磁数据磁道(例如那些与信用卡相关联的常规磁数据磁道)的形式来存储。这样的磁道可以包括磁道1和磁道2。磁道1(“国际航空运输协会”)比磁道2存储更多的信息，并包括持卡人姓名和账户号码，以及其他任意的数据。在用信用卡来确保预订时，航空公司有时会使用该磁道。目前最常用的是磁道2(“美国银行业协会”)。其是由ATM和信用卡检验器来读取的磁道。ABA(美国银行业协会)设计了这个磁道的规格，并且该规格被世界上所有的银行所遵守。磁道2包含持卡人账户、加密PIN，以及其他任意的数据。

[0156] 图9B示出了根据各个实施例的自助服务机(901)的框图。自助服务机(901)包括耦接到存储介质(204)上的一个或多个处理器(921)。存储介质(204)存储能够由处理器(921)运行以给移动设备提供数字钱包功能的机器可读代码。自助服务机(901)包括一个或多个移动设备接口(910)和一个或多个凭证存储工具读取器(920)。自助服务机(901)还包括显示器(925)和声音系统(924)，其在数字钱包提供过程中可用于给用户提供视觉和声音指令。当自助服务机(901)不用来向移动设备提供时，显示器(925)和声音系统(208)可以用于展示其他媒体，例如广告或信息性视频和声音。自助服务机(901)还包括用户输入接口(926)以接收用户输入。用户输入接口(926)可实现为具有触摸屏、小键盘、键盘、触控板、鼠标、轨迹板、麦克风或其他合适的用户输入接口部件中的一种或多种。

[0157] 在一些实施例中，自助服务机(901)可以包括网络接口(923)以允许自助服务机(901)在需要时与可能涉及数字钱包提供过程的实体进行通信。例如，自助服务机(901)可以使用网络接口(923)来与凭证存储工具的发行方(例如，发行信用卡的银行、发行交通通行卡的交通机构、发行身份证的政府机构、发行积分计划卡的零售商等)进行通信。自助服务机(901)也可以使用网络接口(923)来与信任服务管理器进行通信，以获得用于给移动设备提供数字钱包功能的安全密钥或令牌。自助服务机(901)还可以经由网络接口(923)与移动网络运营商进行通信，以验证或访问与移动设备相关联的信息。网络接口(923)可实现为有线接口(例如以太网端口)或无线接口(例如，可以使用诸如Wi-Fi或其他无线通信协议来无线地访问网络的无线收发器)。

[0158] 图9C示出了利用自助服务机(901)来为移动设备(931)提供数字钱包功能的系统(930)。移动设备(931)可以是新购买的移动设备，或者可以是用户已经拥有的现有的移动设备。在一些实施例中，移动设备(931)可以预先装载有数字钱包应用程序，并且自助服务机(901)用于将凭证加载到移动设备(931)的数字钱包应用程序上。在其他实施例中，如果移动设备(931)不包括预先装载的数字钱包应用程序，则自助服务机(901)可用于将数字钱

包应用程序和个性化凭证一起装载到移动设备(931)上。

[0159] 根据一些实施例,自助服务机(901)例如经由网络(932)以通信方式耦接到信任服务管理器(TSM)(933)上。TSM(933)提供服务来支持要通过移动设备来进行的非接触式交易服务。TSM(933)可以提供的基本功能包括对用于访问移动设备的安全元件(SE)芯片(例如,安全存储芯片或存储器的受保护分区)的安全密钥或令牌进行管理的能力,该安全元件(SE)芯片中存储有数字钱包应用程序的凭证。移动设备(931)使用SE来控制和存储需要高度安全性的数据和应用程序。例如,可以通过支付处理网络的实体(例如信用卡的发行方)、通过非接触式交易服务提供商、通过移动网络运营商(MNO)、通过移动设备制造商或通过其他合适的实体来将SE提供给移动设备(931)。通过从SE提供商处获得合适的安全密钥或令牌,可以实现对移动设备(931)的SE的访问。

[0160] 尽管在一些实施例中TSM(933)显示为单独的实体,但是TSM(933)可以与发行方系统(935)(其通过用户凭证来对数字钱包应用程序进行激活和个性化处理)集成在一起,或者与自助服务机(901)集成在一起。根据请求,TSM(933)可以从SE提供商处获得合适的安全密钥或令牌以锁定或解锁移动设备(931)上的SE,以例如允许自助服务机(901)将用户凭证加载到移动设备(931)的SE上。

[0161] 当用户通过向自助服务机(901)的用户输入界面提供用户输入(例如,通过触摸自助服务机(901)的触摸屏,或通过按压自助服务机(901)的键盘上的按键等)来操作自助服务机(901)时,可以发起向移动设备(931)提供数字钱包功能。根据用户操作,自助服务机(901)可以向用户提供视觉和/或声音指令,以完成该提供过程。例如,自助服务机(901)可以显示用于指示用户将用户移动设备(931)通信地连接到自助服务机(901)上的消息。

[0162] 为了将用户移动设备(931)通信地连接到自助服务机(901)上,用户可以将移动设备(931)物理地连接到自助服务机(901)的移动设备接口(例如,连接器或电缆)上以得到有线通信信道,或通过将移动设备(931)放置得非常接近自助服务机(901)的移动设备接口(例如,无线收发器)以允许在移动设备(931)和自助服务机(901)之间建立点对点式无线通信信道。点对点式无线通信信道可以经由NFC、RF、蓝牙、Wi-Fi或其他合适的无线通信协议来建立。在一些实施例中,当自助服务机(901)感应到移动设备(931)非常接近时,自助服务机(901)会显示用于询问用户是否授权允许自助服务机(901)与移动设备(931)建立无线通信信道的消息。

[0163] 一旦在移动设备(931)和自助服务机(901)之间建立起通信信道(有线或无线式),则自助服务机(901)可以给用户提供进一步的视觉和/或声音指令来使该用户出示凭证存储工具(905),以便继续数字钱包提供过程。例如,自助服务机(901)可以指示用户将凭证存储工具(905)放置成与自助服务机(901)的凭据存储工具读取器进行物理接触(例如,通过使磁条卡划过或插入磁条读取器中,或通过将芯片卡插入芯片卡读取器槽中),或者将凭证存储工具(905)放置得非常接近自助服务机(901)的凭证存储工具读取器(例如,通过将非接触式卡片放置得非常接近非接触式读卡器,或者通过将具有条形码或QR码的印刷介质放置在红外扫描器的前面)。当向自助服务机(901)的凭证存储工具读取器出示凭证存储工具(905)时,自助服务机(901)访问凭证存储工具(905)以从凭证存储工具(905)中读取用户凭据。

[0164] 应当注意的是,虽然在上述过程中,在向自助服务机(901)出示凭证存储工具之前

首先建立了移动设备(931)和自助服务机(901)之间的通信信道,但是在一些实施例中,向自助服务机(901)出示凭证存储工具可以先于将移动设备(931)通信地连接到自助服务机(901)上。此外,除了在自助服务机(901)的用户输入界面上提供用户输入以发起该过程之外,还可以备选地通过简单地将移动设备(931)通信地连接到自助服务机(901)上,或者可以通过向自助服务机(901)出示凭证存储工具,来发起数字钱包提供过程。

[0165] 一旦自助服务机(901)从凭证存储工具(905)检索到用户凭证,则自助服务机(901)可以实施验证过程,以确认用户被授权从凭证存储工具(905)向移动设备(931)提供凭证。在一些实施例中,验证过程可以由自助服务机(901)来进行,而不需要任何附加的用户输入。例如,自助服务机(901)可以从移动设备(931)上检索到移动电话号码和/或移动设备标识符,该移动电话号码和/或移动设备标识符可用于从移动网络运营商(936)处查找与移动设备(931)相关联的移动订户姓名。自助服务机(901)也可以检索凭证存储工具(905)上的姓名,或者通过联系发行方系统(935)来使用从凭证存储工具(905)检索到的凭证来查找与该凭证存储工具(905)相关联的姓名。如果移动订户姓名与凭证存储工具(905)的用户姓名相匹配,则可以假定该用户同时是移动设备(931)和凭证存储工具(905)的合理所有者,并且假定该用户已被授权从凭证存储工具(905)向移动设备(931)提供凭证。

[0166] 应当注意的是,本发明的实施例提供了一种与一些空中下载(OTA)式提供过程相比更安全的移动装置(931)提供方法,这是因为在自助服务机的提供过程期间用户物理地拥有凭证存储设备(905)。例如,这可以在欺诈用户没有物理地拥有凭证存储工具时,阻止欺诈用户向移动设备提供盗取的凭证。

[0167] 在一些实施例中,为了增加安全性,在进一步进行提供过程之前,自助服务机(901)可以要求用户输入与凭证存储工具(905)相关联的PIN号码,以鉴别用户。备选或附加地,自助服务机(901)可要求用户经由可使用网络的浏览器登录到由凭证存储工具(905)的发行方所提供的在线账户上,和/或要求用户登录到由移动设备(931)的移动网络运营商所提供的在线帐户上。

[0168] 在自助服务机(901)确定了用户被授权从凭证存储工具(905)向移动设备(931)提供凭证时,自助服务机(901)会将注册或激活请求发送到TSM(933)。在一些实施例中,将注册或激活请求与合适的个性化数据(例如,从凭证存储工具(905)中检索到的凭证)一起进行发送。TSM(933)可以通过以下操作来处理注册或激活请求:使用合适的个性化数据对数字钱包应用程序进行个性化,解锁移动设备(931)的SE,并且向自助服务机(901)提供个性化后的数字钱包应用程序以使其下载到移动设备(931)。例如,在一些实施例中,移动设备(931)包括预先加载的数字钱包应用程序,TSM(933)通过解锁移动设备(931)的SE来处理请求,以允许自助服务机(901)将从凭证凭证存储工具(905)检索到的凭证传送到移动设备(931)的SE上。根据一些实施例,由TSM(9)来执行的一些或全部功能都可以集成到自助服务机(901)中。

[0169] 取决于所使用的凭证存储工具(905)的类型,可能需要那些未存储在凭证存储工具(905)上的附加凭证或者那些不能被自助服务机(901)的凭证存储工具读取器所读取的附加凭证,以使移动设备(931)能够执行非接触式交易。例如,如果凭证存储工具(905)是信用卡,则可能需要动态卡片验证值(dCVV)来进行由移动工具(931)实施的非接触支付交易。在这样的实施例中,在数字钱包提供过程中,自助服务机(901)可以将注册或激活请求发送

到发行方系统(935),以获得附加凭证(例如是可以由移动设备(931)使用以在执行非接触式支付交易时生成dCVV的dCVV软件)。在数据钱包提供过程中,从发行方系统(935)处获得的附加凭证(例如,dCVV软件)可以与从凭证存储工具(905)检索到的凭证一起存储在移动设备(931)的SE中。在一些实施例中,从凭证存储工具(905)检索到的凭证在被存储在移动设备(931)中之前,还可以由发行方系统(935)进行修改或添加。由自助服务机(901)加载到移动设备(931)的SE中的凭证也可以使用数据加密标准,例如具有至少1024位密钥的RSA、三重数据加密标准(DES)、128位高级加密标准(AES)、使用最小128位的密钥长度的RC4流加密算法等。

[0170] 一旦来自凭证存储工具(905)的凭证已经加载到移动设备(931)的数字钱包应用程序上,则自助服务机(901)可以提供视觉和/或声音指令以向用户询问:用户是否希望将凭证从附加的凭证存储工具加载到移动设备(931)上。如果是希望,则可以针对每个凭证存储工具重复上述过程。在一些实施例中,可以以批处理模式来对凭证存储工具进行处理。例如,在自助服务机(901)开始将各个凭证加载到移动设备(931)上之前,自助服务机(901)可以首先允许用户刷用多个凭证存储工具。来自多个凭证存储工具的凭证可以暂时存储在自助服务机(901)中,并且一旦用户已经向自助服务机(901)出示所需数量的凭证存储工具,则自助服务机(901)开始进行将凭证加载到移动设备(931)上的提供过程。

[0171] 根据一些实施例,自助服务机(901)也可以用于将凭证从一个数字钱包应用程序传送到另一个数字钱包应用程序。例如,当用户购买了新移动设备时,用户可能已经在其旧移动设备上具有个性化的数字钱包应用程序。用户可能希望将存储的旧移动设备上的凭证传送到新移动设备上。替代于出示个人的凭证存储工具以供自助服务机(901)读取的做法,用户可以将用户的旧移动设备放置得非常接近自助服务机(901)的凭证存储工具读取器。随后,自助服务机(901)可以访问存储在旧移动设备上的数字钱包应用程序,以检索存储在其中的凭证。当从旧移动设备检索到凭证之后,自助服务机(901)可以使用上述提供过程来向新移动设备提供检索到的凭证。

[0172] 附加于或替代提供移动设备(931)的做法,自助服务机(901)也可以将凭证加载到基于云的数字钱包(934)中。基于云的数字钱包(934)允许将凭证存储在外接于移动设备(931)的网络访问存储器中。使用基于云的数字钱包(934)具有的优点是:一旦凭证已经加载到基于云的数字钱包(934)上,则用户可避免在用户每次更换移动设备时必须将凭证传送到新的移动设备上。因此,在一些实施例中,用户可以在不出示移动设备的情况下,使用自助服务机(901)将凭证从凭证存储工具加载到基于云的数字钱包(934)中。

[0173] 在一些实施例中,自助服务机(901)可以执行附加的数字钱包管理功能。例如,一旦已经提供了移动设备(931)上的数字钱包应用程序并将其个性化,则自助服务机(901)可以允许用户使用加载到数字钱包应用程序上的凭证来购买移动设备(931)的数字媒体。自助服务机(901)还可以允许用户向与存储在数字钱包应用程序中的凭据相关联的账户中存入或添加金额值。例如,自助服务机(901)可以允许用户向存储在数字钱包应用程序中的交通费账户添加金额值。但是,应该注意的是,这些附加的功能与数字钱包提供过程的不同之处在于,在执行这些附加功能之前,这些附加功能需要数字钱包应用程序具有必要的凭证。与此相反,本文所描述的提供过程则用于在由自助服务机(901)提供凭证之前,给移动设备提供数字钱包应用程序所缺少的凭证。根据本发明的实施例,自助服务机可以提供或可以

不提供上述的附加功能。

[0174] 图9D示出了根据一些实施例的用于向移动设备提供数字钱包应用程序的方法(950)的流程图，该方法由自助服务机或其他合适的计算设备来执行。在框(951)处，在用户的移动设备之间建立通信信道。通信信道可以是上述的有线连接或无线连接。在框(952)处，访问凭证存储工具(例如上述的磁条卡、芯片卡、或其他凭证存储工具)，以检索存储在该凭证存储工具中的凭证。在框(953)处，确定用户是否被授权向移动设备的数字钱包应用程序提供检索到的凭证。可以根据任何上述的任意过程来进行该确定。如果确定用户没有被授权，则在方框(956)处，终止该过程，且不向移动设备提供。如果确定该用户被授权，则在框(954)处，发出请求以解锁移动设备的安全元件(SE)。可以使用由TSM或者由具有集成的TSM功能的自助服务机所提供的安全密钥或令牌来解锁SE。一旦移动设备的SE被解锁，则通过将从凭证存储工具检索到的用户凭证加载到SE中来向移动设备提供数字钱包应用程序。在一些实施例中，在用户凭证被存储到移动设备的SE中之前，可以对用户凭证进行修改、添加(例如，添加CVV2)和/或加密。方法(950)可重复用于多个凭证存储工具。在提供过程之后，锁定移动设备的SE，以阻止未经授权的访问。

[0175] 应当理解的是，用于提供移动设备的数字钱包应用程序的方法(950)可以包括未在图9D中显示的附加操作，或者在其他实施例中可以包括较少的操作。此外，某些操作可以以与所图示的顺序不同的顺序来执行。

[0176] 图10图示的泳道流程图显示了根据实施例在移动设备(931)、自助服务机(901)以及远程访问服务器(例如支付凭证发行方(935)或者TSM(933))之间的流程。

[0177] 消费者可以在自助服务机处出示(1001)他的便携式支付设备或凭证存储工具(例如，支付卡)，该自助服务机可以从便携式支付设备中提取出支付凭证。例如，消费者可以将他的信用卡插入自助服务机，并请求“凭证传送”交易。消费者会被提示输入他的支付卡PIN，支付卡PIN可以经由键盘而输入到自助服务机中。消费者还可以提供(1002)标识符，例如，自助服务机也会提示消费者输入用作是消费者和他的移动设备的标识符的“别名”。

[0178] 自助服务机可以如上文所述地连接(1003)到消费者的移动设备上，以建立(1004)连接。例如，如果这是非接触方式，则自助服务机可以使用消费者提供的标识符来识别要连接的移动设备。

[0179] 自助服务机可以将激活请求发送(1005)到由TSM提供的远程访问服务器，以便获得将支付凭证存储在与移动设备相关联的安全元件处并解锁该安全元件的授权。激活请求可以使用由消费者提供的标识符(其针对消费者的移动设备和/或安全元件来进行注册)，并且该识别符可用于识别(1006)移动设备和移动设备的安全元件。TSM可以解锁(1007/1008)与移动设备相关联的安全元件。

[0180] 可以使用与自助服务机的连接，来将支付凭证提供(1009/1010)到移动设备的安全元件。这些支付凭证可以安全地被提供到安全元件中。

[0181] 可能还需要将未存储在便携式支付设备上的附加凭据存储在安全元件处，以便移动设备能够执行非接触式交易。例如，由移动设备实施的非接触式支付交易可能需要动态卡片验证值(dCVV)。在这种实施例中，自助服务机可以向发行方系统的远程访问服务器发生注册请求(1011)，以获得附加凭证。该标识符可以包括在该请求中，并且远程访问服务器使用该标识符来识别(1012)正确的附加凭证。在一个示例中，附加凭证可以是dCVV软件，在

执行非接触式支付交易时移动设备使用该dCVV软件来生成dCVV。注册请求可以包括消费者为了获得用于消费者便携式支付设备的正确附加凭证所提供的标识符。

[0182] 在数字钱包提供过程中，可以将从发行方系统获得的附加凭证(例如，dCVV软件)与从自助服务机检索到的支付凭证一起传输(1013/1014)并存储在与移动设备相关联的安全元件中。备选地，附加凭证可以直接被传递到移动设备的安全元件。

[0183] 图11示出了能实现本发明各个方面的计算设备(1100)的示例。计算设备(1100)适合于存储并运行计算机程序代码。上述系统示意图中的各个参与者和要素可使用任何适当数量的计算设备(1100)的子系统或部件，以促进本文所描述的功能。

[0184] 计算设备(1100)可包括经由通信基础设施(1105)(例如，通信总线、交叉杆设备或网络)互连的子系统或部件。计算设备(1100)可包括至少一个中央处理器(1110)以及，以及以计算机可读介质形式的至少一个存储器部件。

[0185] 存储器部件可包括系统存储器(1115)，其可包括只读存储器(ROM)和随机访问存储器(RAM)。基础输入/输出系统(BIOS)可存储在ROM中。系统软件可存储在系统存储器(1115)中，这包括了操作系统软件。

[0186] 存储器部件还可以包括辅助存储器(1120)。辅助存储器(1120)可包括例如硬盘驱动器的硬盘(1121)，以及任选的用于可拆卸存储器部件(1123)的一个或多个可拆卸存储器接口(1122)。

[0187] 可拆卸存储器接口(1122)可以是用于对应的可拆卸存储器部件(例如，磁带、光盘、软盘等)的可拆卸存储器驱动器(例如，磁带驱动器、光盘驱动器、软盘驱动器等)的形式，其中可拆卸存储器部件可由可拆卸存储器驱动器进行写入和读取。

[0188] 可拆卸存储器接口(1122)也可以是用于与其他形式的可拆卸存储其部件(1123)(例如，闪存驱动器、外部硬盘驱动器或可拆卸存储器芯片等)互联的端口或插槽的形式。

[0189] 计算设备(1100)可包括用于在能实现多个计算设备(1100)之间的数据传输的联网环境下操作计算设备(1100)的外部通信接口(1130)。经由外部通信接口(1130)传送的数据可以是信号的形式，其可以是电子信号、电磁信号、光信号、无线电信号或其他类型的信号。

[0190] 外部通信接口(1130)可实现计算设备(1100)与其他计算设备(包括服务器和外部存储设施)之间的数据通信。Web服务可由计算设备(1100)通过通信接口(1130)来访问。

[0191] 外部通信接口(1130)也可以实现往来于计算设备(1100)的其他形式的通信，这包括语音通信、近场通信、蓝牙等。

[0192] 以各种存储器部件形式的计算机可读介质可以提供对计算机可运行指令、数据结构、程序模块和其他数据的存储。计算机程序产品可通过计算机可读介质来提供，其中该计算机可读介质具有可由中央处理器(1210)运行的经存储的计算机可读程序代码。

[0193] 计算机程序产品可以由非暂时性计算机可读介质来提供，或者可以通过通信接口(1130)通过信号或其他瞬时机构来提供。

[0194] 经由通信基础设施(1105)的互连允许中央处理器(1110)与每个子系统或部件进行通信并控制来自于存储器部件的指令的运行，以及允许子系统或部件之间的信息交换。

[0195] 外围设备(例如打印机、扫描仪、照相机等)和输入/输出(I/O)设备(例如鼠标、触摸板、键盘、话筒、操纵杆等)可直接或通过I/O控制器(1135)来耦接到计算设备(1100)上。

这些部件可通过本领域已知的任何数目的机构(例如,串行端口)连接到计算设备(1100)上。

[0196] 一个或多个监测器(1245)可经由显示器或视频适配器(1240)来耦接到计算设备(1200)上。

[0197] 图12示出了可使用在本发明实施例中的通信设备(1200)的框图。通信设备(1200)可以是蜂窝电话、功能手机、智能电话、卫星电话,或具有电话功能的计算设备。

[0198] 通信设备(1200)可包括用于处理通信设备(1200)各功能的处理器(1205)(例如,微处理器),以及允许用户看到电话号码和其他信息及消息的显示器(1220)。通信设备(1200)还可以包括允许用户将信息输入到该通信设备中的输入元件(1225)(例如,输入按钮、触摸屏等),允许用户收听语音通信、音乐等的扬声器(1230),以及允许用户通过通信设备(1200)来传送他或她的语音的麦克风(1235)。

[0199] 可以将通信设备(1200)的处理器(1210)连接到存储器(1215)上。存储器(1215)可以是用于存储数据和(任选的)计算机可运行指令的计算机可读介质的形式。存储器(1215)。

[0200] 通信设备(1200)也可包括用于连接通信信道(例如,蜂窝式电话网络、数据传输网络、Wi-Fi网络、卫星电话网络、互联网网络、卫星互联网网络等)的通信元件(1240)。通信元件(1240)可包括相关联的无线传输元件,例如天线。

[0201] 通信元件(1240)可包括集成电路形式的订户身份模块(SIM),其用于存储国际移动订户身份以及使用通信设备(1200)来识别和验证订户的相关密钥。可以将一个或多个订户身份模块从通信设备(1200)上拆除,或嵌入在通信设备(1200)中。

[0202] 通信设备(1200)还可包括非接触元件(1250),其通常实现为具有相关联的无线传输元件(例如天线)的半导体芯片(或其他数据存储元件)的形式。非接触元件(1250)可以与通信设备(1200)相关联(例如,嵌入内部),并且经由蜂窝网络传送的数据或控制指令可以通过非接触元件接口(未示出)施加到非接触元件(1250)上。非接触元件接口可以起到允许在移动设备电路(以及相应的蜂窝网络)与非接触元件(1250)之间交换数据和/或控制指令的作用。

[0203] 非接触元件(1250)能够使用通常符合标准化协议或数据传输机制(例如ISO14443/NFC)的近场通信(NFC)功能(或近场通信介质)来传送和接收数据。近场通信功能是短程通信能力,例如射频识别(RFID)、蓝牙、红外,或其他可用于在通信设备(1200)和问询设备之间交换数据的传输能力。因此,通信设备(1200)能够通过蜂窝网络和近场通信能力来进行数据和/或控制指令的通信和传输。

[0204] 支持移动非接触式支付的通信设备(1200)通常使用基于ISO 14443的EMV非接触式通信协议(EMV-CCP)来支持非接触式交易,以便与商家访问设备进行交互。通常通过实现NFC来满足此功能。可以通过嵌入式NFC芯片或通过附加有包含了NFC芯片的外部存储卡或附件来实现通信设备(1200)上的NFC功能。此外,通信设备(1200)通常包括嵌入在手机或在订户身份模块(SIM)卡片中的安全元件(SE)(1260)。SE(1260)还可以包括在附加设备中,附加设备例如是微型安全数字(microSD)卡或者用于添加在通信设备(1200)的通信元件上的扩容元件。

[0205] 存储在存储器(1215)中的数据可包括:与数据通信设备(1200)的操作有关的操作

数据、个人数据(例如,姓名、出生日期、身份号码、等)、金融数据(例如,银行账户信息、银行识别码(BIN)、信用卡或借记卡号码信息、账户余额信息、到期日期、信用提供商帐号等)、交通信息(例如,地铁票或火车票)、通行信息(例如,通行徽章中的信息)等。用户可将该数据从通信设备(1200)传送,是选定接收器。

[0206] 除其他事项外,通信设备(1200)可以是:能够接收警报消息和访问报告的通知设备,能够用于传送可识别待用折扣的控制数据的便携式商家设备,以及可进行支付的便携式消费者设备。

[0207] 本发明实施例的上述说明出于说明性目的给出;其并非旨在穷举本发明或将将本发明限制到所公开的具体形式中。相关领域技术人员可以理解,可根据上述公开内容来进行多种修改和变型。

[0208] 本说明书的某些部分根据算法和信息操作的符号表示对本发明实施例加以描述。这些算法描述和表示是数据处理领域中的技术人员所惯用的,以便有效地将他们的工作传达给本领域的其他技术人员。尽管以功能性、计算性或逻辑性方式对这些操作进行描述,但是其应当理解为可由计算机程序或等效电路、微代码等来实现。所描述的操作可以体现在软件、固件、硬件或其任意组合中。

[0209] 本申请中所描述的软件部件或功能可以实现为例如采用传统或面向对象技术的、使用任何合适的计算机语言(例如,Java、C++或Perl)的、待由一个或多个处理器运行的软件代码。软件代码可存储为非暂时性计算机可读介质(例如,随机访问存储器(RAM)、只读存储器(ROM)、磁性介质(例如,硬盘驱动器或软盘),或光介质(例如,CD-ROM))上的一系列指令或命令。任何这样的计算机可读介质还可驻留在单个计算设备上或单个计算设备内,并且可以驻留在系统或网络内的不同计算设备上或计算设备内。

[0210] 本文所述的任何步骤、操作、过程可以用一个或多个硬件或软件模块以单独方式或与其他设备相结合的方式来实现。在一个实施例中,软件模块实现为包括非暂时性计算机可读介质的计算机程序产品,其中该非暂时性计算机可读介质包含可由计算机处理器运行的、用于实现上述任何或全部步骤、操作或过程的计算机程序代码。

[0211] 最后,在说明书中使用的语言主要选择用于可读性和指导性目的,可能并非选择用于勾勒或划定本发明主题。因此,意图在于,本发明的范围不受该详细描述所限制,而是由以基于本文的应用为出发点的权利要求所限定。因此,本发明实施例的公开意在说明性,而非对由所附权利要求阐述的本发明范围进行限制。

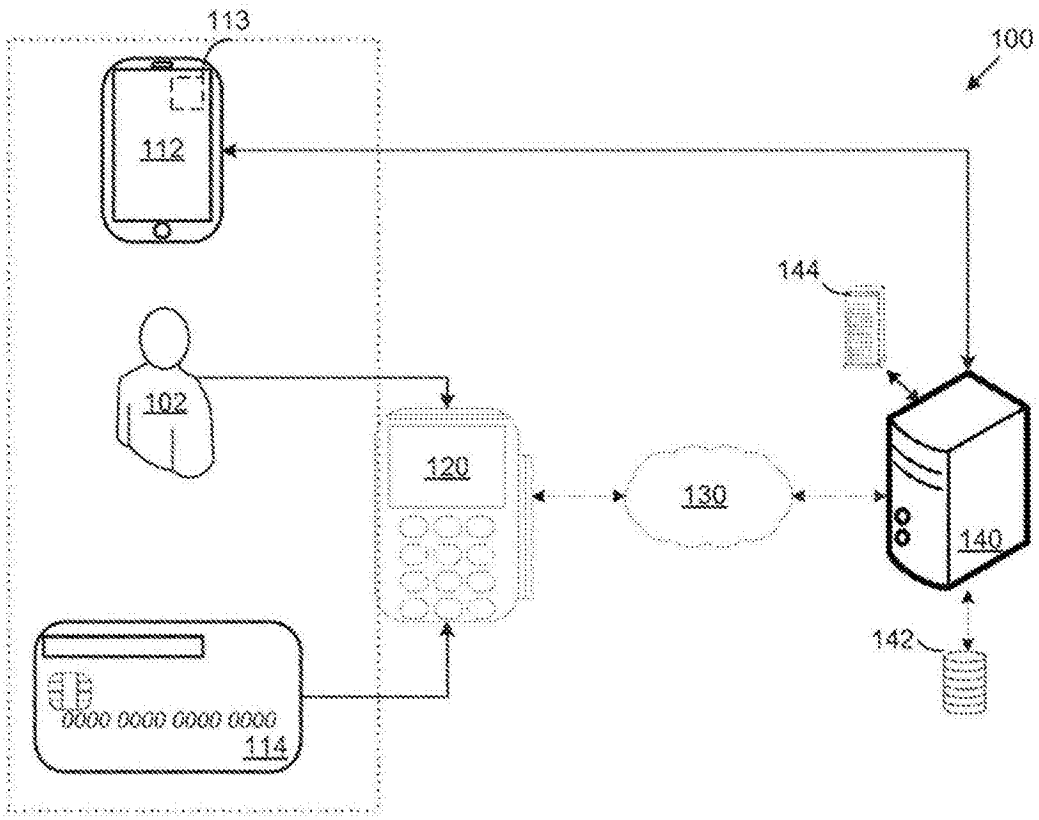

113
100
112
144
102
120
130
140
142
0000 0000 0000 0000
114

图1

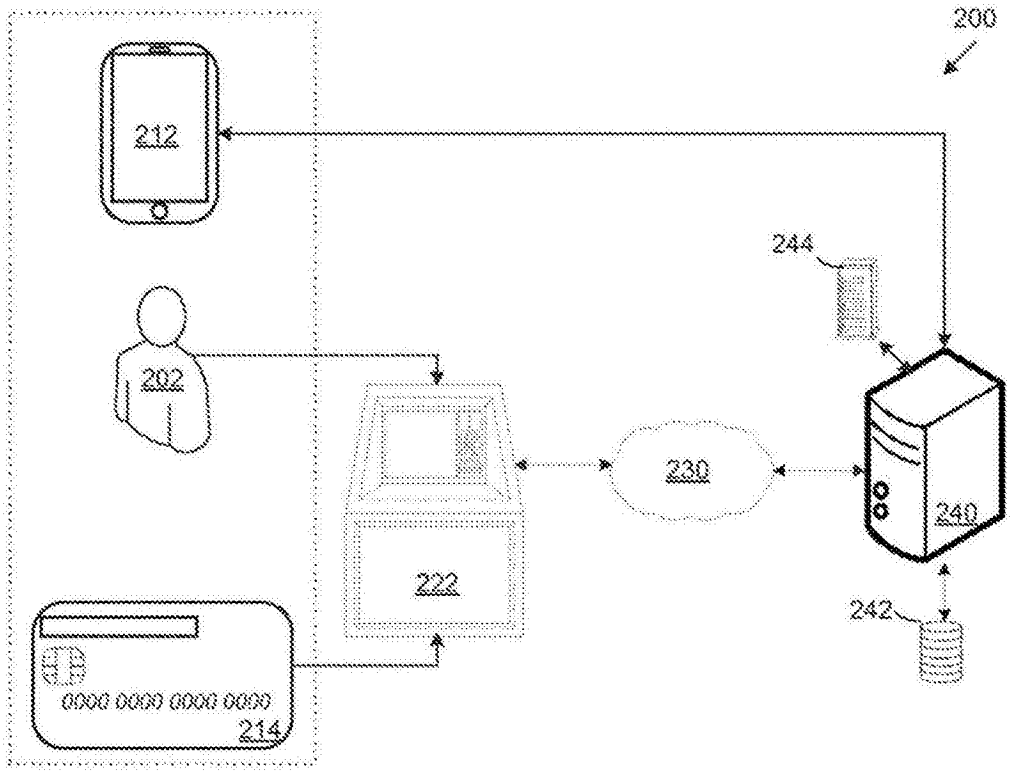

200
212
244
202
230
240
222
242
0000 0000 0000 0000
214

图2

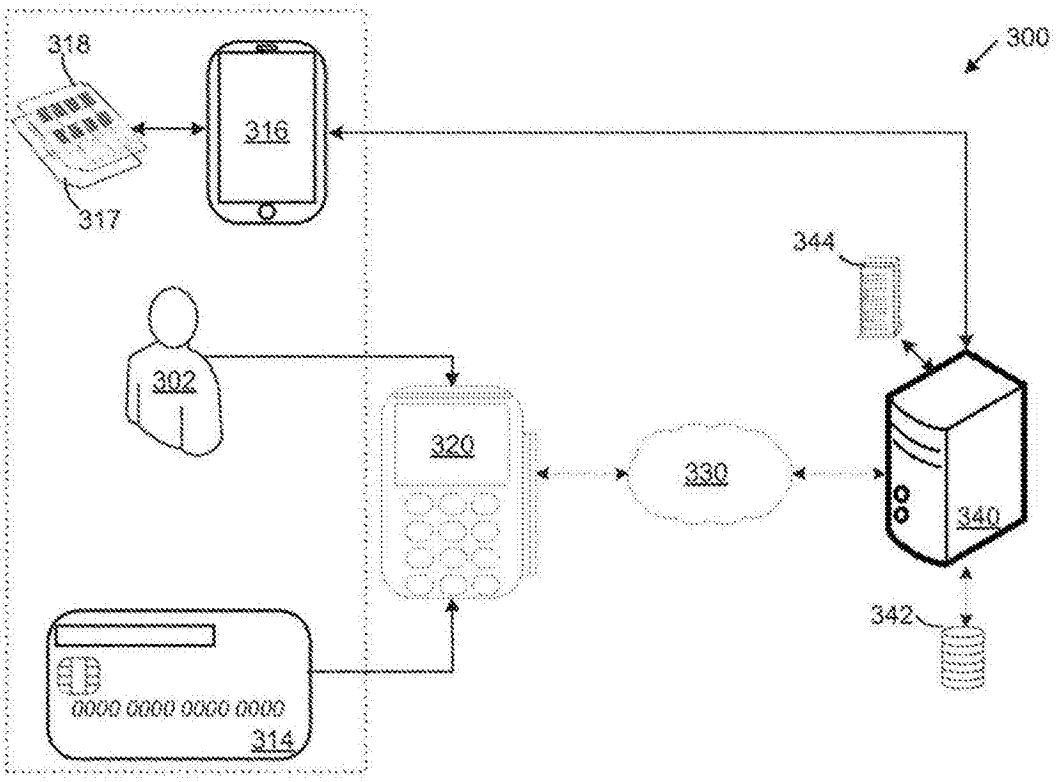


图3

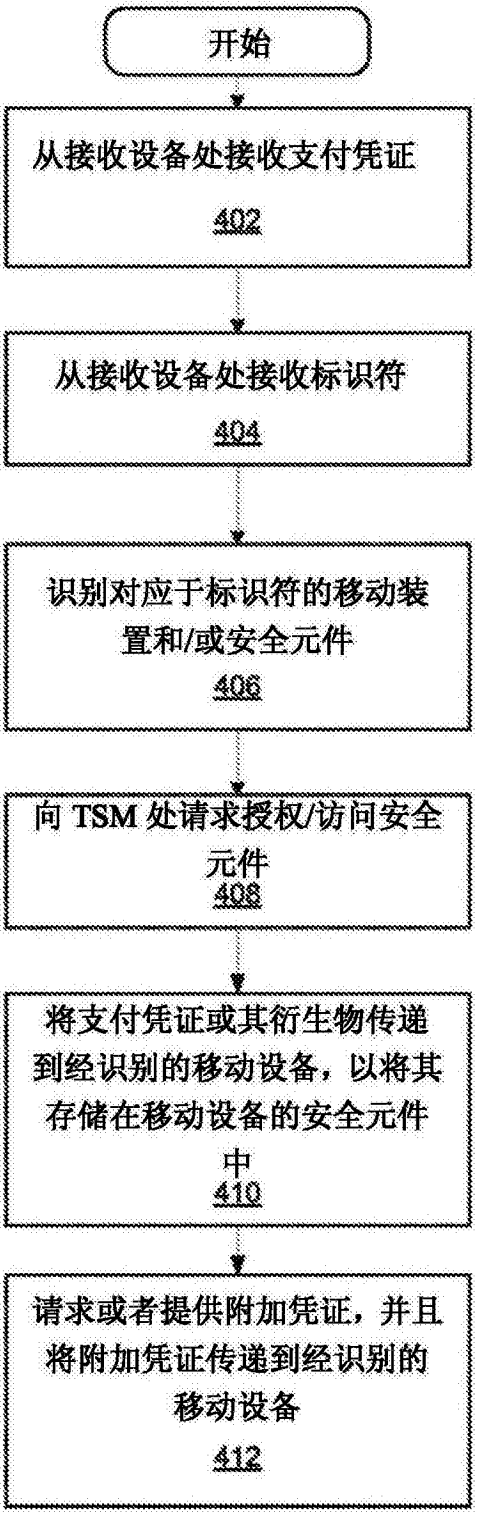

开始
从接收设备处接收支付凭证
402
从接收设备处接收标识符
404
识别对应于标识符的移动装置和/或安全元件
406
向 TSM 处请求授权/访问安全元件
408
将支付凭证或其衍生物传递到经识别的移动设备，以将其存储在移动设备的安全元件中
410
请求或者提供附加凭证，并且将附加凭证传递到经识别的移动设备
412

图4A

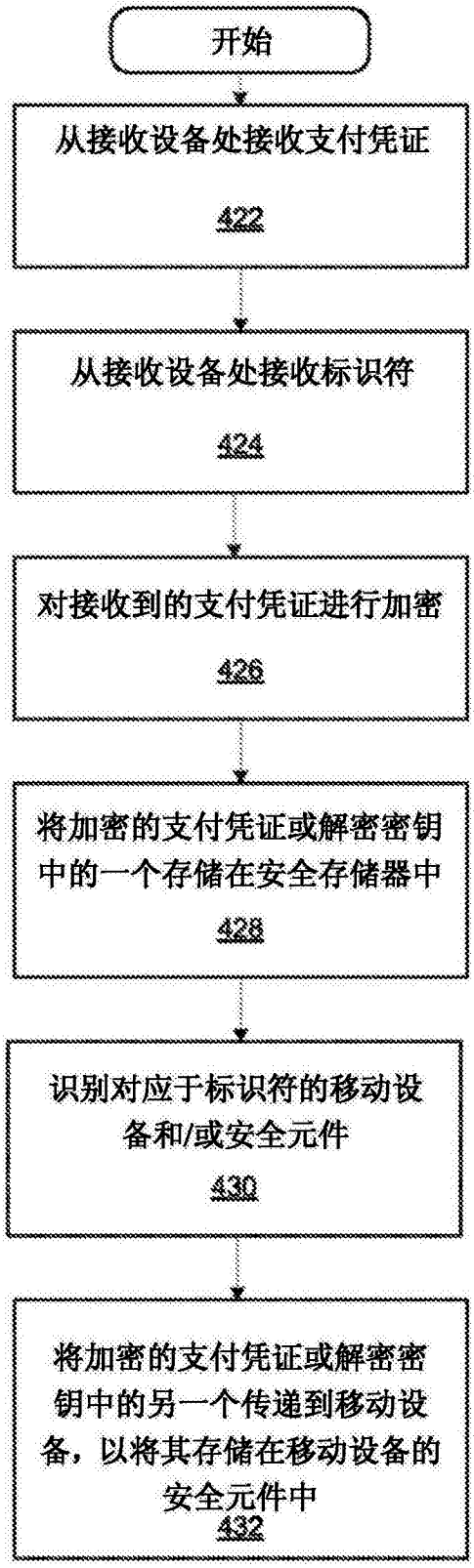

开始
从接收设备处接收支付凭证
422
从接收设备处接收标识符
424
对接收到的支付凭证进行加密
426
将加密的支付凭证或解密密钥中的一个存储在安全存储器中
428
识别对应于标识符的移动设备和/或安全元件
430
将加密的支付凭证或解密密钥中的另一个传递到移动设备，以将其存储在移动设备的安全元件中
432

图4B

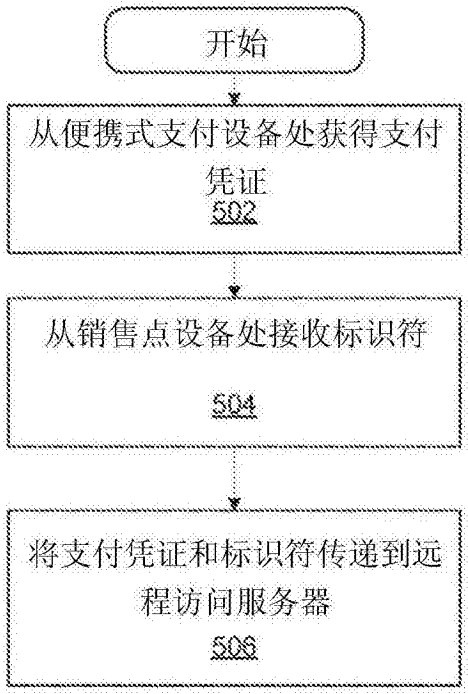

开始
从便携式支付设备处获得支付凭证
502
从销售点设备处接收标识符
504
将支付凭证和标识符传递到远程访问服务器
506

图5

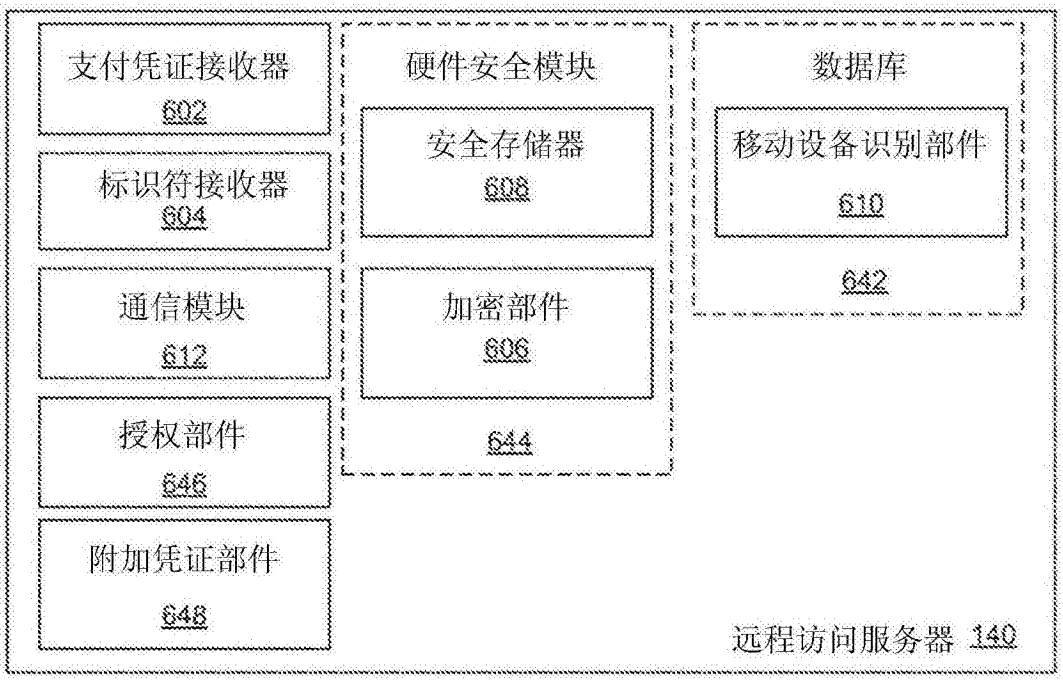

支付凭证接收器
602
标识符接收器
604
通信模块
612
授权部件
646
附加凭证部件
648
硬件安全模块
安全存储器
608
加密部件
606
644
数据库
移动设备识别部件
610
642
远程访问服务器 140

图6A

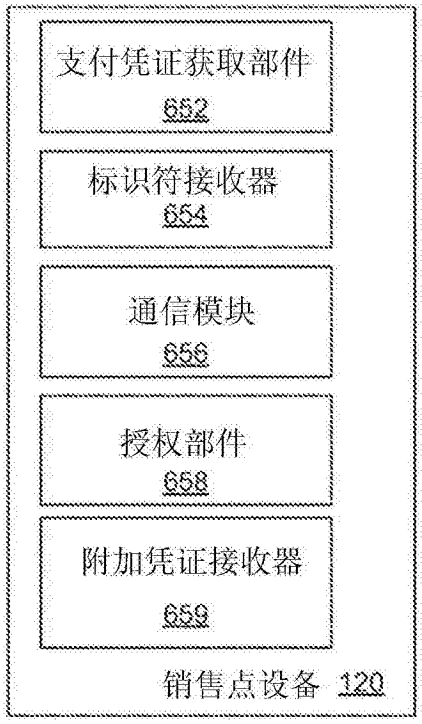

支付凭证获取部件
652
标识符接收器
654
通信模块
656
授权部件
658
附加凭证接收器
659
销售点设备 120

图6B

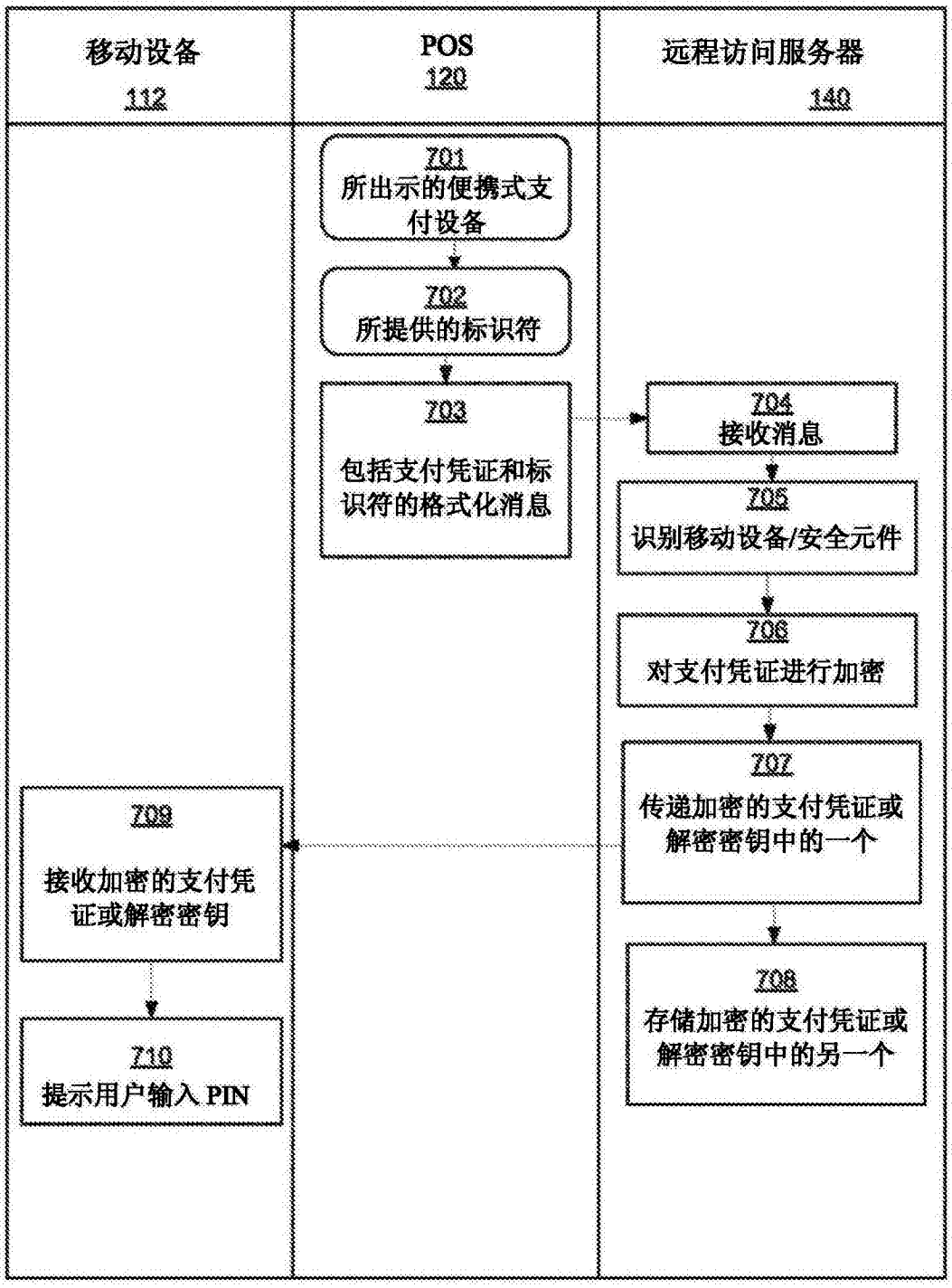

移动设备
112
POS
120
远程访问服务器
140
701
所出示的便携式支付设备
702
所提供的标识符
703
包括支付凭证和标识符的格式化消息
704
接收消息
705
识别移动设备/安全元件
706
对支付凭证进行加密
707
传递加密的支付凭证或解密密钥中的一个
708
存储加密的支付凭证或解密密钥中的另一个
709
接收加密的支付凭证或解密密钥
710
提示用户输入 PIN

图7

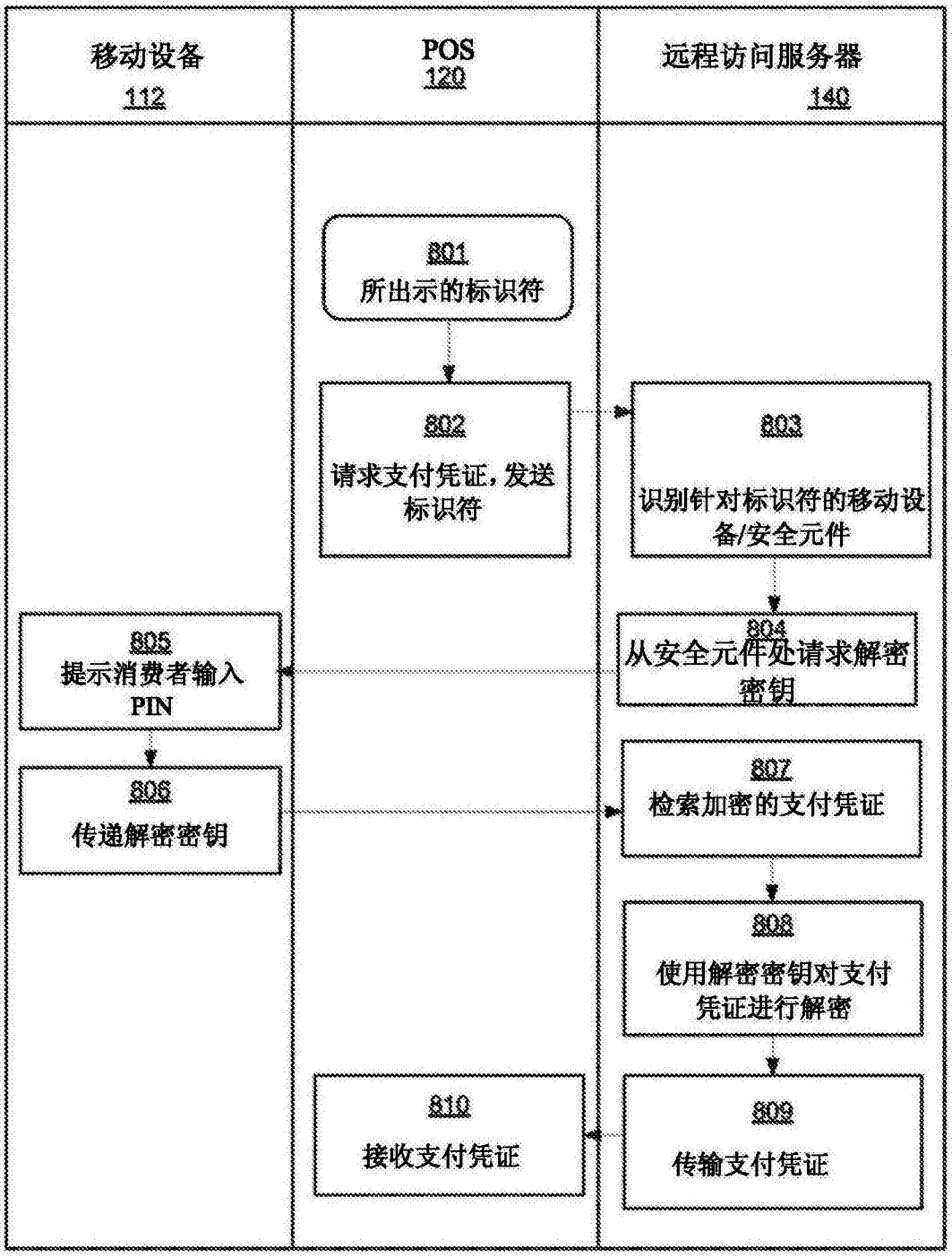

移动设备
112
POS
120
远程访问服务器
140
801
所出示的标识符
802
请求支付凭证，发送标识符
803
识别针对标识符的移动设备/安全元件
804
从安全元件处请求解密密钥
805
提示消费者输入PIN
806
传递解密密钥
807
检索加密的支付凭证
808
使用解密密钥对支付凭证进行解密
809
传输支付凭证
810
接收支付凭证

图8

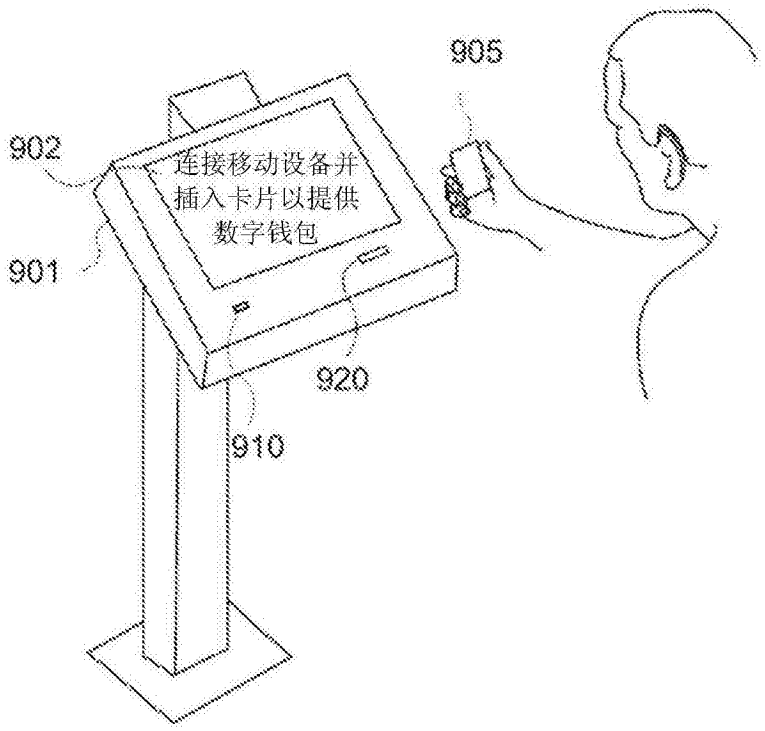

905
902
连接移动设备并
插入卡片以提供
数字钱包
901
920
910

图9A

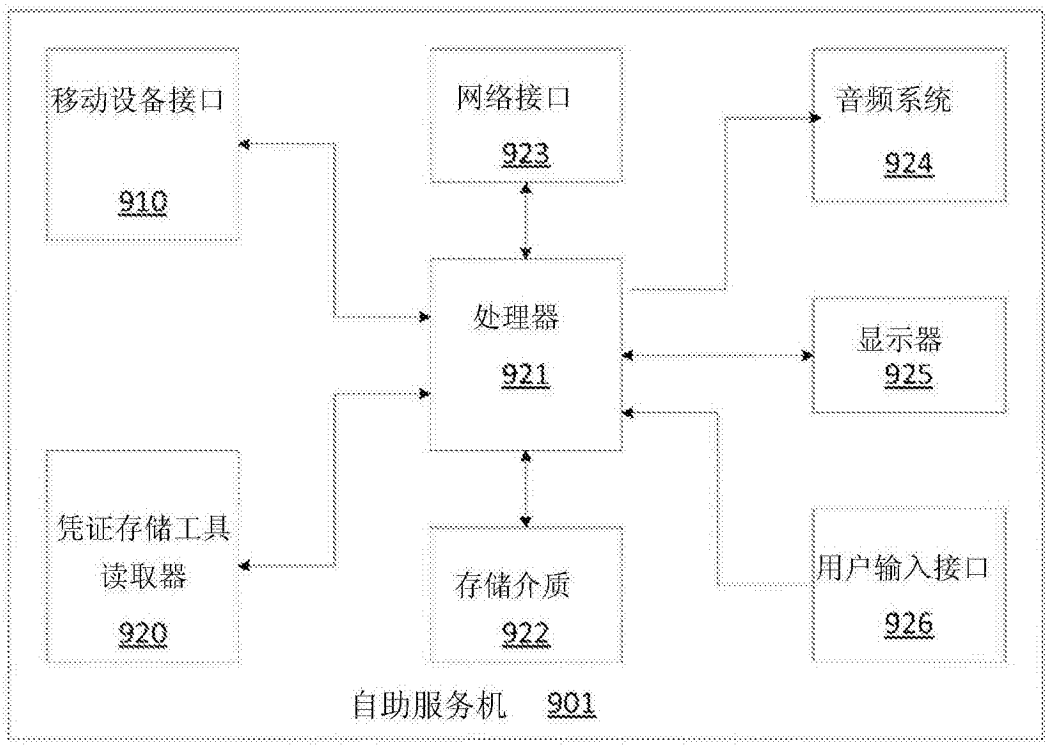

移动设备接口
910
网络接口
923
音频系统
924
处理器
921
显示器
925
凭证存储工具
读取器
920
存储介质
922
用户输入接口
926
自助服务机 901

图9B

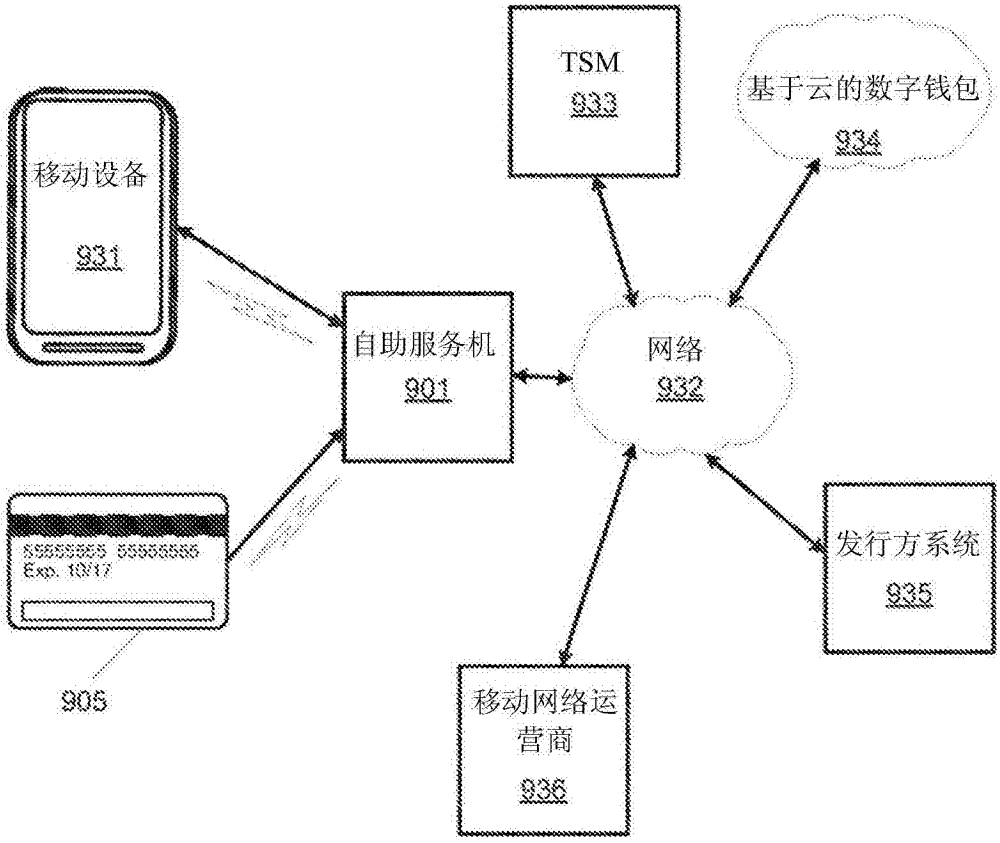

TSM
933
基于云的数字钱包
934
移动设备
931
自助服务机
901
网络
932
发行方系统
935
移动网络运营商
936
905

图9C

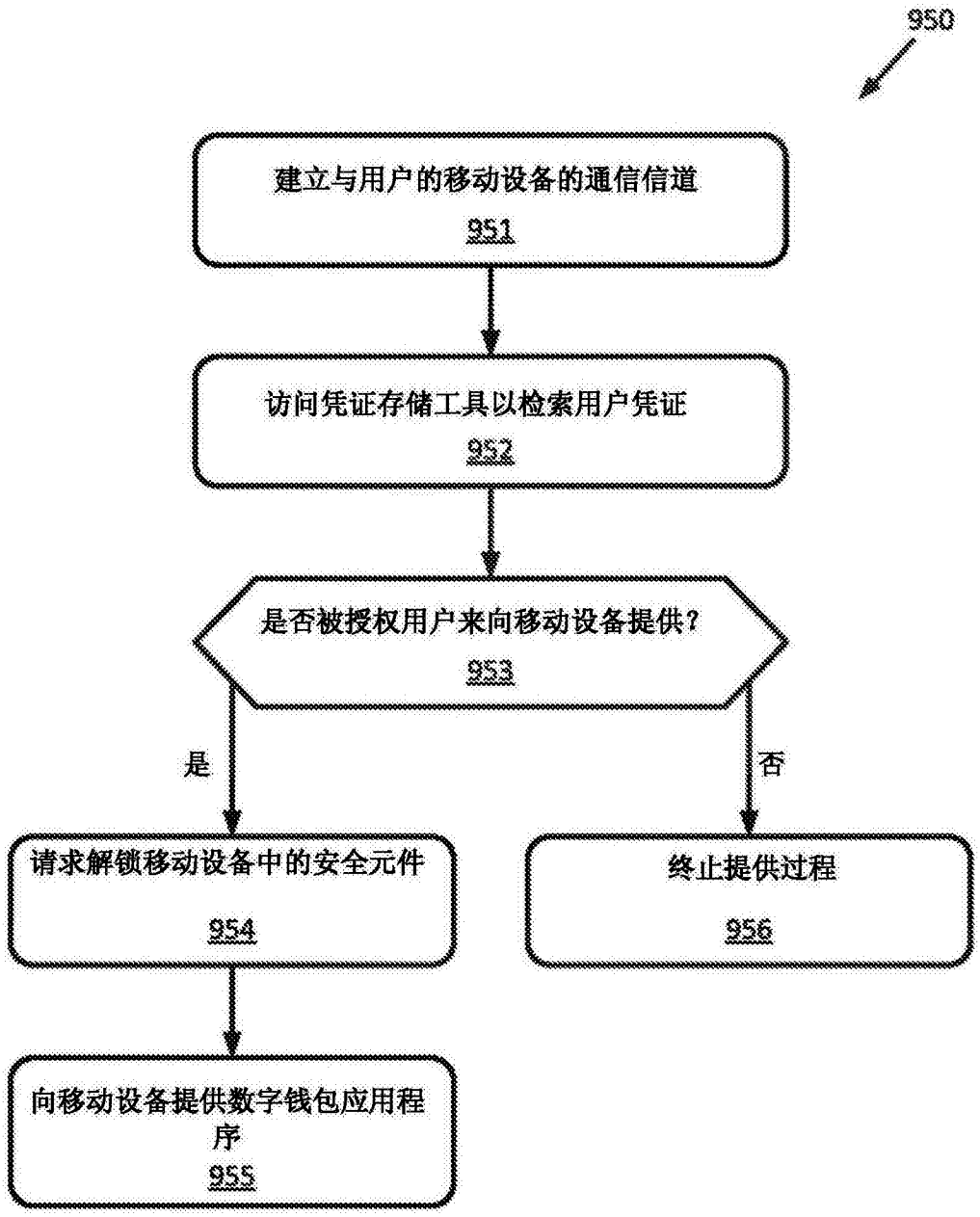

950
建立与用户的移动设备的通信信道
951
访问凭证存储工具以检索用户凭证
952
是否被授权用户来向移动设备提供？
953
是
否
请求解锁移动设备中的安全元件
954
终止提供过程
956
向移动设备提供数字钱包应用程序
955

图9D

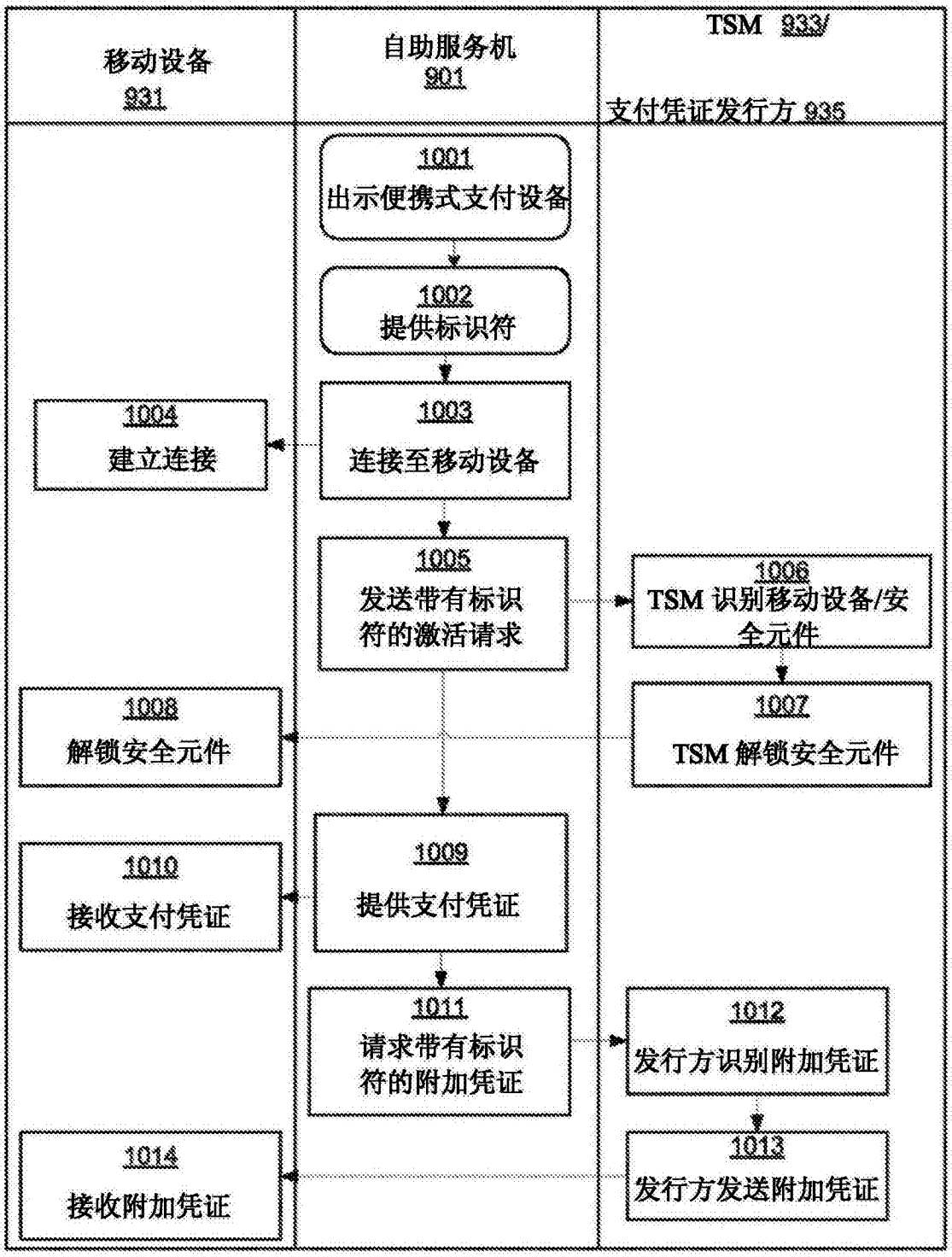

移动设备
931
自助服务机
901
TSM 933/
支付凭证发行方 935
1001
出示便携式支付设备
1002
提供标识符
1003
连接至移动设备
1004
建立连接
1005
发送带有标识符的激活请求
1006
TSM 识别移动设备/安全元件
1007
TSM 解锁安全元件
1008
解锁安全元件
1009
提供支付凭证
1010
接收支付凭证
1011
请求带有标识符的附加凭证
1012
发行方识别附加凭证
1013
发行方发送附加凭证
1014
接收附加凭证

图10

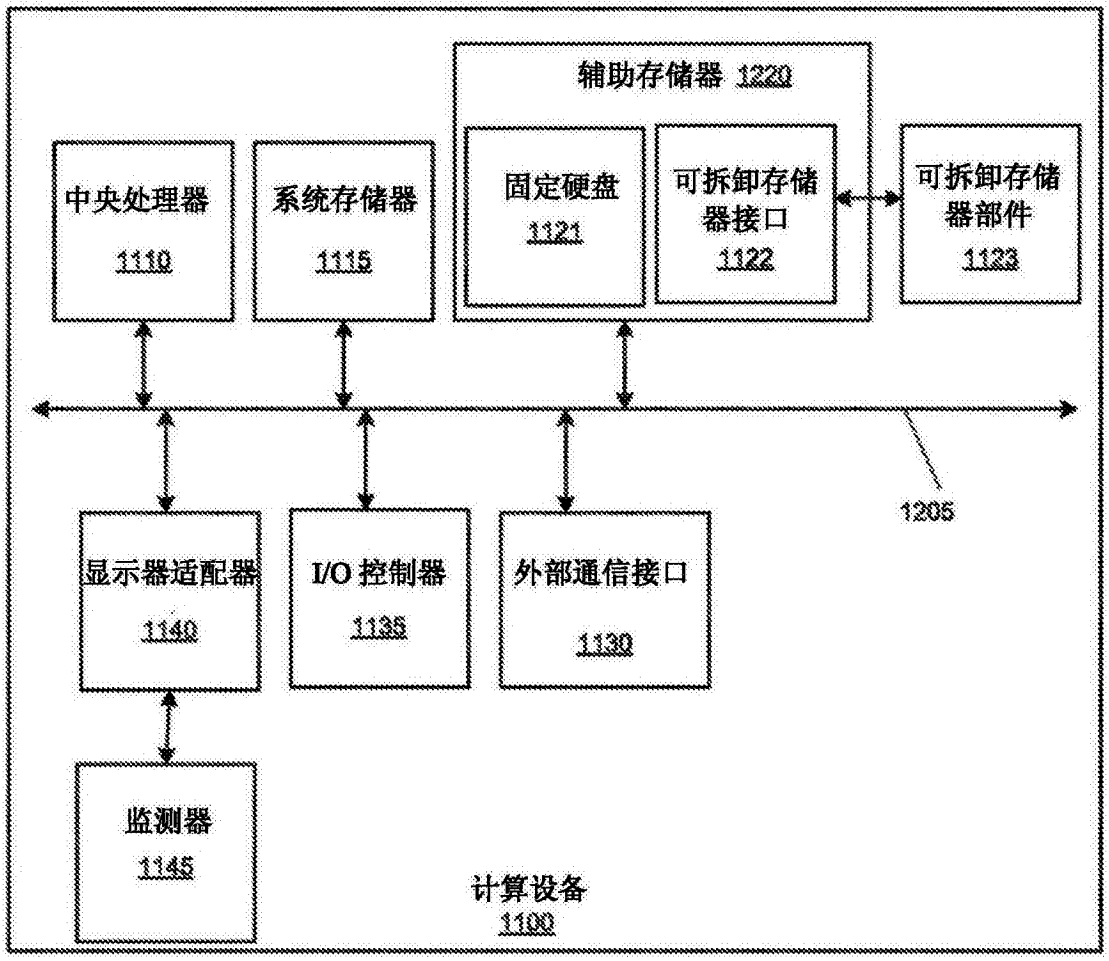

辅助存储器 1220
中央处理器
1110
系统存储器
1115
固定硬盘
1121
可拆卸存储器接口
1122
可拆卸存储器部件
1123
1205
显示器适配器
1140
I/O 控制器
1135
外部通信接口
1130
监测器
1145
计算设备
1100

图11

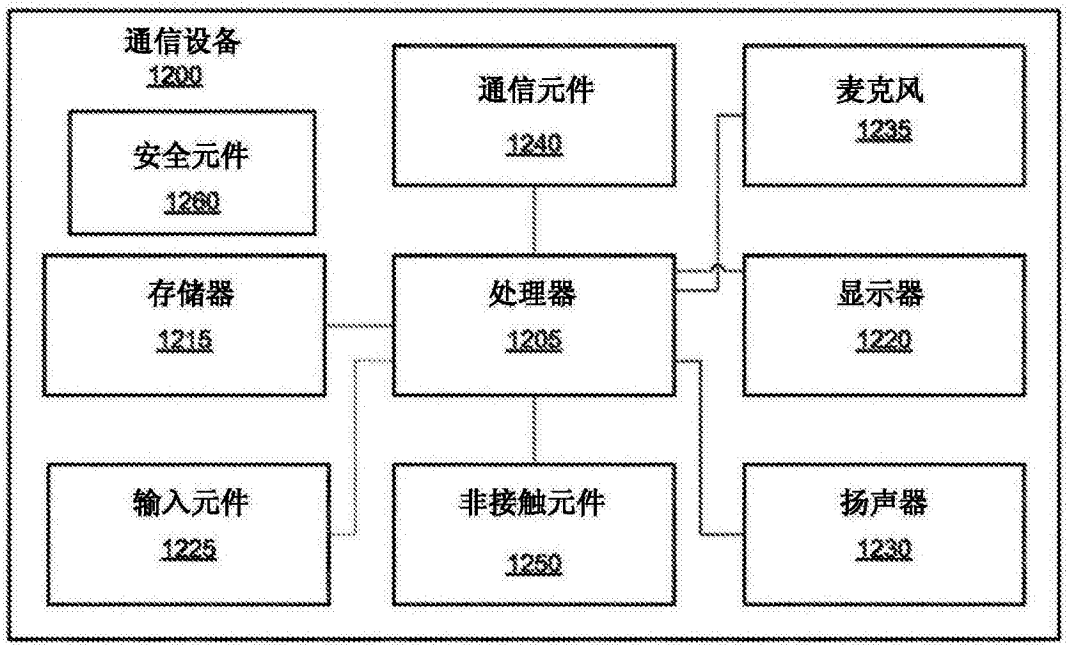

通信设备
1200
通信元件
1240
麦克风
1235
安全元件
1260
存储器
1215
处理器
1205
显示器
1220
输入元件
1225
非接触元件
1250
扬声器
1230

图12