(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 104969245 A
(43)申请公布日 2015.10.07

(21)申请号 201480007462.4
(22)申请日 2014.02.06
(30)优先权数据
61/761,654 2013.02.06 US
(85)PCT国际申请进入国家阶段日
2015.08.05
(86)PCT国际申请的申请数据
PCT/US2014/015050 2014.02.06
(87)PCT国际申请的公布数据
WO2014/124108 EN 2014.08.14
(71)申请人 苹果公司
地址 美国加利福尼亚
(72)发明人 D·T·哈格蒂 A·A·柯恩
C·沙普 J·V·豪克 J·林德
K·P·麦克劳克林 M·泽阿特
Y·H·韦德
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李晓芳
(51)Int.Cl.
G06Q 20/40(2006.01)

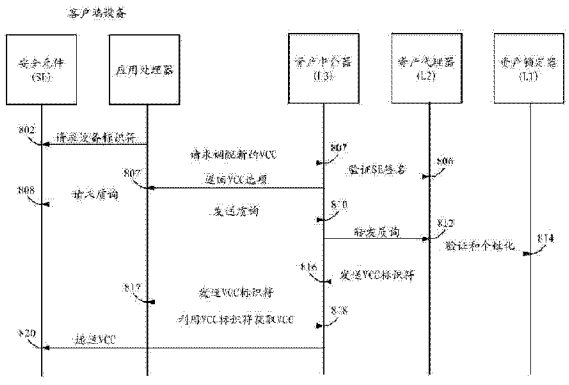
权利要求书3页 说明书17页 附图15页

(54)发明名称

用于安全元件交易和资产管理的装置和方法

(57)摘要

本发明公开了用于部署金融工具和其他资产的方法和装置。在一个实施例中，公开了一种安全软件协议，所述安全软件协议保证所述资产始终被安全地加密，保证资产有且仅有一份副本存在，并且所述资产被递送给已认证的和/或被授权的顾客。另外，公开了调配系统的示例性实施例，其中所述调配系统能够处理大量突发性流量（诸如可在所谓的设备“首发日”发生的情况）。



CN 104969245 A

1. 一种由包括一个或多个账户服务器的资产中介器用来向包括安全元件的客户端设备分发资产的方法，所述方法包括所述资产中介器至少：

从所述客户端设备接收 (i) 将所述资产调配给账户的请求和 (ii) 唯一识别所述客户端设备的设备标识符；

认证将所述资产调配给所述账户的所述请求；

从资产锁定器接收资产标识符，其中所述资产标识符唯一识别被分配给客户端设备的所述资产；

向所述客户端设备发送所述资产标识符；

从所述客户端设备接收对所分配的资产的请求；

从所述客户端设备接收所述资产标识符；以及

向所述客户端设备发送所分配的资产。

2. 根据权利要求 1 所述的方法，还包括所述资产中介器：

在从所述资产锁定器接收所述资产标识符之前：

从所述客户端设备接收与所述设备标识符相关联的数字签名；以及

向资产代理器发送所述数字签名，其中所发送的数字签名由所述资产代理器验证。

3. 根据权利要求 2 所述的方法，还包括所述资产中介器：

在向所述资产代理器发送所述数字签名之后：

从所述客户端设备接收质询，其中所述质询由所述安全元件生成；以及

向所述资产代理器发送所述质询，其中所发送的质询由所述资产代理器验证。

4. 根据权利要求 1 所述的方法，其中认证将所述资产调配给所述账户的所述请求包括验证所述设备标识符与所述账户相关联。

5. 根据权利要求 1 所述的方法，还包括所述资产中介器：

将所分配的资产与所述客户端设备或所述设备标识符相关联。

6. 根据权利要求 1 所述的方法，还包括所述资产中介器：

在向所述客户端设备发送所分配的资产之后，基于所分配的资产的价值在所述账户中记入借项。

7. 根据权利要求 1 所述的方法，其中所述资产包括信用卡号。

8. 根据权利要求 1 所述的方法，其中向所述客户端设备发送所分配的资产包括将所分配的资产发送给所述安全元件。

9. 根据权利要求 3 所述的方法，其中所分配的资产包括基于从所述客户端设备接收的所述质询的质询数据。

10. 根据权利要求 1 所述的方法，还包括所述资产中介器：

在接收将所述资产调配给所述账户的所述请求之前，从所述客户端设备接收用于识别所述用户账户的账户信息。

11. 根据权利要求 10 所述的方法，其中在所述用户购买所述客户端设备时发生从所述用户接收账户信息。

12. 根据权利要求 1 所述的方法，还包括所述资产中介器：

将所分配的资产存储在第一地理位置处和与所述第一地理位置分开的第二地理位置处。

13. 根据权利要求 12 所述的方法，其中向所述客户端设备发送所分配的资产包括从所述第一地理位置或从所述第二地理位置发送所分配的资产，并且其中所述客户端设备被配置为基于所发送的分配的资产中嵌入的质询数据来验证所发送的分配的资产。

14. 一种由一个或多个装置用来向包括安全元件的客户端设备分发资产的方法，每个装置包括存储器和处理器，所述方法包括所述一个或多个装置至少：

通过利用唯一密钥加密所述资产并通过将质询数据嵌入所述资产中来预先配置所述资产，所述唯一秘钥基于唯一识别所述客户端设备的设备标识符；

将所述预先配置的资产与资产标识符相关联；

从所述客户端设备接收请求，所述请求包括所述资产标识符；以及

响应于接收到所述请求，向所述客户端设备递送所述预先配置的资产。

15. 根据权利要求 14 所述的方法，其中所述资产包括信用卡号。

16. 根据权利要求 14 所述的方法，还包括所述一个或多个装置：

在预先配置所述资产之前，从所述客户端设备的用户接收账户信息，所述账户信息用于识别用户账户。

17. 根据权利要求 16 所述的方法，其中在所述用户购买所述客户端设备时发生从所述用户接收账户信息。

18. 根据权利要求 16 所述的方法，其中预先配置所述资产还包括将所述资产与所述用户账户相关联。

19. 根据权利要求 14 所述的方法，还包括所述一个或多个装置：

在预先配置所述资产之前，向所述客户端设备提供所述资产标识符。

20. 根据权利要求 14 所述的方法，还包括所述一个或多个装置：

将所述预先配置的资产存储在第一地理位置处和与所述第一地理位置分开的第二地理位置处。

21. 根据权利要求 20 所述的方法，其中向所述客户端设备递送所述预先配置的资产包括从所述第一地理位置或从所述第二地理位置递送所述预先配置的资产，并且其中所述客户端设备被配置为基于所递送的预先配置的资产中嵌入的所述质询数据来验证所递送的预先配置的资产。

22. 根据权利要求 14 所述的方法，还包括所述一个或多个装置：

在预先配置所述资产之前，从设置在箱盒上的与所述客户端设备相关联的标签或标记获得所述设备标识符。

23. 根据权利要求 14 所述的方法，其中所述请求包括与所述资产标识符相关联的数字签名。

24. 根据权利要求 14 所述的方法，还包括所述一个或多个装置：

在从所述客户端设备接收所述请求之前，向所述客户端设备发送所述资产标识符。

25. 根据权利要求 14 所述的方法，其中所述质询数据基于存储在所述安全元件上的质询。

26. 一种被配置为从远程服务器请求资产的客户端设备，所述客户端设备包括：

应用处理器；

存储设备，所述存储设备被配置为存储指令，所述指令在由所述应用处理器执行时，使

所述客户端设备：

向所述远程服务器发送将资产调配给账户的请求；

向所述远程服务器发送唯一识别所述客户端设备的设备标识符，其中所发送的设备标识符用于认证调配所述资产的所述请求，

从所述客户端设备的安全元件获得质询；以及

向所述远程服务器发送所述质询；并且

所述安全元件包括：

安全处理器；和

安全存储器，所述安全存储器被配置为存储指令，所述指令在由所述安全处理器执行时，使所述安全元件：

从所述远程服务器接收所述资产，所接收的资产包括基于发送给所述远程服务器的所述质询的质询数据；以及

基于所述质询数据来验证所接收的资产。

27. 根据权利要求 26 所述的客户端设备，其中所述安全存储器被进一步配置为存储指令，所述指令在由所述安全处理器执行时，使所述安全元件在验证所接收的资产之后从所述安全元件删除所述质询。

28. 根据权利要求 27 所述的客户端设备，其中所述安全存储器被进一步配置为存储指令，所述指令在由所述安全处理器执行时，使所述安全元件：

生成新的质询；以及

将所述新的质询存储在所述安全元件上。

29. 根据权利要求 26 所述的客户端设备，其中所述存储设备被进一步配置为存储指令，所述指令在由所述应用处理器执行时，使所述客户端设备：

从所述远程服务器接收资产标识符；以及

将所接收的资产标识符发送回所述远程服务器。

30. 根据权利要求 26 所述的客户端设备，其中所述存储设备被进一步配置为存储指令，所述指令在由所述应用处理器执行时，使所述客户端设备在将所述设备标识符发送给所述远程服务器之前，从所述安全元件获得所述设备标识符。

31. 根据权利要求 26 所述的客户端设备，其中所述资产包括信用卡号。

32. 根据权利要求 26 所述的客户端设备，其中所述存储设备被进一步配置为存储指令，所述指令在由所述应用处理器执行时，使所述客户端设备在从所述远程服务器接收所述资产之后，从所述远程服务器接收用于指示基于所述资产的价值在所述账户中记入借项的通知。

33. 根据权利要求 26 所述的客户端设备，其中所述存储设备被进一步配置为存储指令，所述指令在由所述应用处理器执行时，使所述客户端设备在发送所述请求之前，将识别所述账户的账户信息发送给所述远程服务器。

34. 根据权利要求 33 所述的客户端设备，其中在用户购买所述客户端设备时发送所述账户信息。

35. 根据权利要求 26 所述的客户端设备，其中所述质询是一次性使用的质询。

用于安全元件交易和资产管理的装置和方法

技术领域

[0001] 本公开整体涉及安全设备交易领域，并且更具体地讲，在一个示例性实施例中，涉及金融工具和其他资产的部署。

背景技术

[0002] 顾客和商户通常期望使用方便且安全的装置来执行金融交易和其他相关交易。资产，诸如信用卡、借记卡、预付费卡、礼品卡、礼券等，全都是货币越来越“虚拟化”的性质的示例。具体地讲，不是实际用现实货币或现实礼券兑换商品和/或服务，而是利用例如账号或“代理”账号（例如，为了在销售点处理交易而创建的账号，但其并非实际的贷记账号或借记账号）执行交易，并且资金是以电子方式进行贷记/借记。

[0003] 遗憾的是，由于在本文中更详细描述的原因，用于分发这些资产的现有解决方案的效率低下并且容易失败。例如，虚拟钱包范型可以基于已有账户；并且为了执行货币交易，客户端设备的用户必须具有带钱包服务已有账户（例如，提供与钱包相关联的会计数据库的可信实体），或已对钱包服务预付费。另外，现有资产并非“可取代的”，并在它们形成时就专门用于特定用途。

[0004] 随着顾客和商户对交易的复杂性和/或方便性（包括越来越普遍地使用移动设备）需求的稳定增长，需要新的改进方案来分发资产。理想的是，此类解决方案应为顾客、商户以及发放实体提供合理且方便的管理能力，而不损害资产的灵活性。

发明内容

[0005] 本公开通过尤其提供用于安全元件交易和资产管理的装置和方法，解决了上述需求。

[0006] 在一个实施例中，公开了一种用于将资产分发给客户端设备的方法。可通过从客户端设备接收对将资产调配给账户的请求来执行该方法。资产调配请求可伴随有唯一识别客户端设备的设备标识符。接着，认证资产调配请求。在一种情况下，使用设备标识符验证客户端设备与账户是否关联，来认证资产调配请求。一旦认证了该请求，就将资产调配给账户并且将资产分配给客户端设备。接着，从远程设备诸如资产锁定器接收到唯一识别所分配资产的资产标识符。然后将资产标识符发送给客户端设备。随后，客户端设备可使用资产标识符来请求所分配资产。一旦从客户端设备接收到对所分配资产的请求和资产标识符，就将所分配资产递送给客户端设备。

[0007] 在另一个实施例中，公开了一种用于将资产分发给客户端设备的方法。客户端设备与唯一识别该客户端设备的设备标识符相关联。通过为客户端设备预先配置资产来执行该方法。预先配置过程可包括：(i)利用基于设备标识符的唯一密钥加密资产；(ii)将质询数据嵌入资产中；并且/或者(iii)将资产与用户账户相关联。因此，为客户端设备配置或“个性化”资产。接着，所述预先配置的资产与资产标识符相关联。在该实施例的一个方面，在预先配置资产之前将资产标识符提供给客户端设备。客户端设备可随后请求所述预

先配置的资产。请求可包括资产标识符。一旦接收到请求，就可将所述预先配置的资产递送给客户端设备。

[0008] 在另一个实施例中，公开了一种计算机可读存储介质。该计算机可读存储介质存储指令，该指令在被客户端设备的处理器执行时，使客户端设备发送对将资产调配给账户的请求。可将请求发送给远程设备。账户可与客户端设备的用户相关联。连同请求一起，客户端设备可发送唯一识别该客户端设备的设备标识符。在该实施例的一个方面，设备标识符存储在设置于客户端设备中的安全元件上。此外，一个或多个质询也可存储在安全元件上。所述指令还使客户端设备将质询发送给远程设备。客户端设备可随后从远程设备接收资产。所接收的资产可包括安全元件可用来验证所接收的资产是否有效的质询数据。质询数据可基于所发送的质询。

[0009] 提供本发明内容仅出于概述一些示例性实施例以便提供对本文所述主题的一些方面的基本了解的目的。因此，应当理解，上文所述的特征仅为示例，且不应理解为以任何方式缩小本文所述的主题的范围或实质。本文所述的主题的其他特征、方面和优点将根据以下具体实施方式、附图和权利要求书而变得显而易见。

[0010] 根据结合以举例的方式示出所述实施例的原理的附图而进行的以下详细描述，本发明的其他方面和优点将变得显而易见。

附图说明

[0011] 参考以下描述以及附图可更好地理解所述实施例。此外，参考以下描述和附图可更好地理解所述实施例的优点。

[0012] 图 1 是根据本公开的交易网络的一种示例性配置的图形表示。

[0013] 图 2 是根据本公开的调配系统的一种示例性配置的图形表示。

[0014] 图 3A 是根据本公开的客户端设备的一个示例性实施例的逻辑框图。

[0015] 图 3B 是根据本公开的商户端设备的一个示例性实施例的逻辑框图。

[0016] 图 4 是根据本公开的资产代理器的一个示例性实施例的逻辑框图。

[0017] 图 5 是根据本公开的资产中介器的账户服务器的一个示例性实施例的逻辑框图。

[0018] 图 6 是根据本公开的资产锁定器的一个示例性实施例的逻辑框图。

[0019] 图 7 是根据本公开的用于分发资产的一般化方法的一个实施例的逻辑流程图。

[0020] 图 8 是根据本公开的表示示例性调配交易的逻辑梯形图。

[0021] 图 9A 和图 9B 示出根据本公开的用于分发资产的一般化方法的另一个实施例的逻辑流程图。

[0022] 图 10A 和图 10B 示出根据本公开的用于分发资产的一般化方法的另一个实施例的逻辑流程图。

[0023] 图 11 是根据本公开的用于分发资产的一般化方法的另一个实施例的逻辑流程图。

[0024] 图 12 是根据本公开的用于分发资产的一般化方法的另一个实施例的逻辑流程图。

[0025] 图 13A、图 13B 和图 13C 示出根据本公开的用于分发资产的一般化方法的另一个实施例的逻辑流程图。

具体实施方式

[0026] 在本部分描述了根据本专利申请的方法与装置的代表性应用。提供这些示例仅是为了添加上下文并有助于理解所述实施例。因此，对于本领域的技术人员而言将显而易见的是，可在没有这些具体细节中的一些或全部的情况下实践所述实施例。在其他情况下，为了避免不必要地模糊所述实施例，未详细描述熟知的过程步骤。其它应用是可能的，使得以下示例不应视为是限制性的。

[0027] 在以下详细描述中，参考了形成说明书的一部分的附图，并且在附图中以举例说明的方式示出了根据所述实施例的具体实施例。尽管足够详细地描述了这些实施例以使得本领域的技术人员能够实践所述实施例，但应当理解，这些实例不是限制性的，使得可以使用其它实施例并且可在不脱离所述实施例的实质和范围的情况下作出修改。

[0028] 虚拟“钱包”可为顾客、商户以及金融机构带来重要的益处。虚拟钱包中的虚拟“内容”可包括一种或多种资产。任何实体（例如，用户、商户、金融机构等）可在适当启用且安全的设备之间自由转移这些资产；此外，这些资产可灵活地存储、备份等。现有解决方案经由互联网协议（IP）网络提供某些基本交易，例如，分发、更新、修补等。然而，由于金融交易和信息的敏感性质，因此需要有效的安全措施来阻止盗窃、滥用、恶意行为等。

[0029] 应当注意，对于本论述的上下文，贯穿本发明的实施例描述了呈虚拟交换媒介（VME）形式的资产。常见的虚拟交换媒介的示例包括但不限于：信用“卡”号、借记“卡”号、预付费“卡”号、账户信息以及虚拟货币等。更一般地，虚拟交换媒介还涵盖了没有实际价值的票据，例如，电子礼券、电子代金券、电子票、电子通行证等。应当理解，本描述并非限制性的，并且所描述的实施例可用于分发任何有用和/或有价值的事物。此外，VME 可在复杂性不同的各种数据结构（例如，字串、数组、对象、密码元件等）内实施；例如，简单的具体实施可为简单账号，更复杂的具体实施可结合账户信息和/或校验值。在一些情况下，VME 可提供额外的特征，诸如密码保护、可衡算性（即，交易历史）、匿名性、欺诈检测等。

[0030] 所描述的实施例涉及用于安全交易和 VME 管理的方法和装置。在一个实施例中，一种调配系统向客户端设备分发资产。该调配系统包括根据安全协议管理 VME 并向客户端设备分发 VME 的一个或多个实体，其中安全协议具有可被称为 L1、L2 和 L3 的三个级别。在 L1 级别，VME 被安全地生成、存储并被加密。L1 可由一个或多个资产锁定器促成。L2 控制并管理 VME 的有效副本数目。L2 可阻止对 VME 的不利且/或恶意的克隆。在该实施例的一个方面，L2 可使用一个或多个质询，来使得一旦 VME 的第一副本被分发，VME 的重复副本就失效。L2 可由一个或多个资产代理器促成。L3 对向预期的客户端设备分发资产进行认证并授权。在该实施例的一个方面，在认证过程中，L3 可使用从设置于客户端设备中的安全元件获得的标识符。在认证过程中，L3 还可使用与用户的账户相关联的信息。L3 可由一个或多个资产中介器促成。

[0031] 在一个实施例中，公开了客户端设备与调配系统之间的调配交易。该调配系统包括资产中介器、资产代理器以及资产锁定器。客户端设备包括与该客户端设备相关联的设备标识符。标识符可在设置于客户端设备中的安全元件中存储并被加密。用户账户可在客户端设备被用户（即，顾客）购买时创建。另选地，用户账户可为已有账户，在客户端设备被购买时，该账户被用户识别。客户端设备从资产中介器请求 VME，并且提供识别信息，例

如，设备标识符。资产中介器认证识别信息并确定 SE/ 客户端设备是否与用户账户相关联。一旦认证，资产中介器就可向资产代理器转发 SE 签名。资产代理器验证安全元件的身份并为安全元件识别 VME。接着，安全元件向调配系统提供质询。基于所提供的质询的质询数据可由资产代理器嵌入在 VME 中。因此，质询数据可用来阻止 VME 的重复副本被发放。资产锁定器可随后为客户端设备的安全元件提供与 VME 相关联的标识符，例如，VME 标识符。一旦接收到 VME 标识符，该客户端设备随后就可使用 VME 标识符请求从资产中介器递送 VME。

[0032] 在另一个实施例中，可使 VME 的配置和递送延期，直到用户购买具有安全元件的客户端设备。这样，客户端设备未被制造或预编程有 VME。相反，客户端设备被“预个性化”，使得在向用户递送客户端设备前，客户端设备预先分配有 VME。“预个性化”过程可包括将调配系统中存储的 VME 与同客户端设备相关联的标识符相关联。在购买时，认证信息是由用户提供。在运输时（例如，在用户购买客户端设备与用户请求 VME 之间的时间，和 / 或将客户端设备装运给用户花费的时间），可为客户端设备预先配置 VME。预先配置 VME 可包括：(i) 利用特定于安全元件的密钥加密 VME；(ii) 将质询数据嵌入 VME 中；并且 (iii) 将 VME 与认证信息相关联。VME 即会与 VME 标识符相关联。接着，客户端设备可使用 VME 标识符来请求 VME。反过来，调配系统可向预先配置的客户端设备递送 VME。这样，在不需要实时流量的情况下请求 VME 时，VME 可被无缝加载到客户端设备上。

[0033] 在另一个实施例中，在从客户端设备接收对 VME 的请求之前，为客户端设备分配来自 VME 池的 VME（例如，VME 池中的每个 VME 一开始不与特定客户端设备相关联）。在购买客户端设备时，认证信息由用户提供。客户端设备可被提供给用户。除了客户端设备之外，还向用户提供可用来认证该客户端设备的识别信息，例如，唯一识别该客户端设备的设备标识符。例如，可从封装客户端设备的箱盒上设置的标贴上取得设备标识符。随后，在请求激活 VME 时，客户端设备可在用户的指令下，向调配系统提供设备标识符。

[0034] 下文参考图 1 至图 13C 论述了这些和其他实施例；然而，本领域的技术人员将容易地理解，本文相对于这些附图的所给出的详细描述仅出于说明性目的并且不应理解为限制性的。

[0035] 现在参考图 1，示出了一种示例性交易网络 100。示例性交易网络 100 包括一个或多个客户端设备 102、一个或多个商户端设备（也称为“销售点”(POS)）104、以及一个或多个后端服务器 106。相关领域的普通技术人员将容易地理解，上述交易网络 100 仅仅例示了可能的网络拓扑和功能的较广阵列。此外，应当认识到，各种具体实施可组合并且 / 或者进一步划分成图 1 所示的各种实体。

[0036] 当客户端设备 102 以密码方式加密交易信息并将其发送给商户端设备 104 时，执行交易。在一个示例中，客户端设备 102 可包括虚拟“钱包”，该虚拟“钱包”被配置为通过例如刷过适当的读取器（诸如近场通信 (NFC) 等）、目视检查来自图形用户界面 (GUI) 的交易标识符（例如，条形码、数字等）等，执行与商户端设备 104 的交易。在另一个示例中，客户端设备 102 可包括全球定位系统 (GPS) 接收器或其他定位信息（例如，Wi-Fi 存在情况等），该信息用以提醒商户端设备 104（例如，寄存器、移动平板电脑等）客户端设备 102 的存在，并且随后进行客户端设备 102 的用户的验证（例如，生物识别，诸如用户脸部照片），以便授权对已知用户账户的收费。交易信息可包括以下项的组合：(i) 别名；(ii) 递增计数器；(iii) 随机数字；(iv) 商户端标识符；(v) 其他交易勘误表（例如，交易量、时间戳、位置

戳等）。

[0037] 商户端设备 104 向后端服务器 106 提供受保护的交易信息。此后，后端服务器 106 可对受保护的交易信息进行解密，验证交易，并且适当处理交易。例如，别名值被映射至信用卡号，并且如果加密信息正确，则后端服务器 106 利用映射至别名值的信用卡号来处理交易。相反，如果交易信息损坏，或呈现欺骗性，则拒绝交易。

[0038] 在示例性交易网络 100 内，施加至交易信息的密码保护为用户的重要信息提供保护，使其不会被任何恶意方和 / 或商户得到。具体地，即使在恶意方尝试拦截交易信息、或商户端设备 104 受到损害（通过例如病毒等）的情况下，密码保护也可帮助防止交易以欺骗方式在以后重演。因此，为尽量增强用户保护，密码元件在设置于客户端设备 102 中的安全元件内受到物理上的保护，安全元件可包括安全处理器、安全文件系统以及可操作存储器。然而，相关领域中的普通技术人员应当认识到，维持客户端设备内存储的密码材料的安全性是困难的。例如，一个此类问题是初始配置、部署以及维护。客户端设备由设备制造商（其可能不受信任）制造。另外，某些商业模型可取决于第三方参与者（其可能不受信任）市场。

[0039] 理想的是，用于分发密码材料的解决方案应可在大型分发网络上伸缩。此外，分发方案必须保护密码材料（凭据）免于被任何中介实体（例如，设备制造商、第三方中介等）得到。在一些实施例中，密码材料应当是唯一的（即，单个资产实例每次仅可在单个安全元件中使用）。最后，解决方案应使对实时交互的需要降到最低程度。

[0040] 现在参考图 2，示出了一种示例性调配网络 200。如图所示，调配系统 200 包括 :客户端设备 300、资产代理器 400、资产中介器 500 和资产锁定器 600。如前所述，在 VME 操作的上下文内，VME 安全性还可细分成多级别，包括 :级别 1(L1)、级别 2(L2) 以及级别 3(L3)。每个级别可由调配系统 200 的元件来促成。

[0041] 资产锁定器 600 可用于根据级别 1(L1) 安全性来执行 VME 保护。如本文所用，级别 1 安全性一般且非限制性地指被配置为保护 VME 中包含的机密和 / 或密码材料（例如，安全密钥、密码材料、用户历史等）的安全机制。此外，术语“安全性”一般是指数据和 / 或软件的保护。例如，密码安全性保护与访问 VME 相关联的数据和 / 或软件免受未经授权的活动和 / 或恶意第三方盗窃、滥用、损坏、公开和 / 或篡改。

[0042] 资产代理器 400 可用于根据级别 2(L2) 安全性来执行 VME 保护。如本文所用，级别 2 安全性一般且非限制性地指阻止 VME 的意外和 / 或恶意复制（强制保全）的安全机制。此外，术语“保全”是指不能被轻微增加或减小的元件（物理的或虚拟的）。例如，在正常操作期间不能拷贝或复制所保全的 VME。此外，如本文使用的，应用于元件（物理的或虚拟的）的术语“唯一性”是指使元件是具有特定属性和 / 或特性的独一无二元件的属性。例如，唯一 VME 不能具有副本 VME。

[0043] 资产中介器 500 可用于根据级别 3(L3) 安全性来执行 VME 保护。如本文所用，级别 3 安全性一般且非限制性地指将 VME 安全地递送给与预期用户（例如，个人、企业、机器客户端等）相关联的设备（例如，客户端设备、POS 等）的安全机制。此外，如本文所用，术语“用户授权”一般是指指定用户对资源的访问权限。利用常见的交换媒介（信用卡、借记卡、现金），交易可以要求对媒介的实质占有，并且实体卡受用户保护。例如，在使用实体信用卡时，假设该卡是由用户所有（并由用户隐形授权）。在 VME 操作的上下文内，需要类似

功能来对 VME 转移进行用户授权。具体地讲，VME（以及调配系统 200）的“所有人”需要确保 VME 仅被转移至一个或多个合法设备。

[0044] 出于下文将明确的原因，每个级别的安全性与一组有限功能 / 职责相关联；因此，提供级别 2 安全性的设备可自由地执行与级别 2 相关联的动作，但同样必须满足能够影响 VME 的级别 1 元件的级别 1 安全性。例如，资产代理器（下文将更详细描述）防止 VME 被克隆；然而，资产代理器不一定具有改变 VME 内包含的密码材料的能力，也不是负责检测受损密码材料的资产代理器。

[0045] 前述对 VME 安全性级别的定义仅是说明性的，而非意图限制本文中的描述。事实上，应当理解，前述术语应当被认为是相关领域内的“通俗用语”，并且从相关行业和 / 或技术的早期发展来看可能发生改变。

[0046] 应当理解，软件通常比硬件更灵活；例如，软件容易被复制、修改以及分发。此外，软件常常可被做成比硬件等价物更便宜、更有功率效率且体积更小。然而，需要特别考虑 VME 数据（例如，顾客财务信息、资产中介器密码机密等）的敏感性质。期望的是，为了实现用户保护，必须防止 VME 遭受非预期的复制和 / 或损坏。因此，VME 操作应当满足以下特性：(i) 安全性；(ii) 唯一性；以及 (iii) 保全性。

[0047] 在一个示例性实施例中，公开了一种分发基础结构，该分发基础结构使 VME 能够被递送给安全元件。安全元件可设置于客户端设备和 / 或商户端设备之中。此外，本发明的基础结构的各种功能可灵活分割并且 / 或者适配，使得各方（例如，设备制造商、第三方零售商、顾客等）可拥有基础结构的相应部分；可根据各方的需求优化这些零碎解决方案。另一个示例性实施例能够提供操作冗余。

[0048] 现在参考图 3A，展示了一种示例性客户端设备 300。示例性客户端设备 300 包括：客户端 - 商户端接口 302、处理器子系统 304、非暂态计算机可读介质（存储器子系统）306 和安全元件 308。在一些变型中，安全元件 308 还包括安全处理器 308A 和安全非暂态计算机可读介质（安全存储器）308B。如本文所用，术语“客户端设备”包括但不限于被配置为交易并且 / 或者管理用户 VME 中的一个或多个的设备。客户端设备的常见示例尤其是具有无线功能的蜂窝电话、智能电话（诸如 iPhone™）、具有无线功能的个人计算机 (PC)、诸如手持计算机的移动设备、个人数字助理 (PDA)、个人媒体设备 (PMD)、无线平板电脑（诸如 iPad™），所谓的“平板手机”，或以上设备的任何组合。

[0049] 处理器子系统 304 可包括以下器件中的一个或多个：数字信号处理器、微处理器、现场可编程门阵列、或安装在一个或多个基板上的多个处理部件。处理器子系统 304 还可包括内部高速缓存存储器。处理器子系统 304 与存储器子系统 306 通信，后者包括存储器，存储器可例如包括静态随机存取存储器 (SRAM)、闪存和 / 或同步动态随机存取存储器 (SDRAM) 部件。存储器子系统 306 可实现一个或多个直接存储器存取 (DMA) 型硬件，以有利于本领域熟知的数据访问。该示例性实施例的存储器子系统 306 包含能由处理器子系统 304 执行的计算机可执行指令。

[0050] 在一个示例性实施例中，客户端设备 300 包括适于连接至商户端设备的一个或多个接口，例如，客户端 - 商户端接口 302。客户端 - 商户端接口 302 可为无线接口，或另选地为物理接口（有线）。无线接口可包括具有最多几厘米的工作范围的“触摸”或“碰撞”型接口（例如，射频识别 (RFID)、NFC 等，诸如符合国际组织标准 (ISO) 标准 14443A/B 的那些，

该标准全文以引用方式并入本文），以及更强的无线接口诸如全球移动通信系统（GSM）、码分多路访问（CDMA）、通用移动通信系统（UMTS）、长期演进（LTE）/LTE-Advanced、全球微波接入互操作性（WiMAX）、Wi-Fi、蓝牙、无线通用串行总线（USB）等。物理接口的常见示例包括例如USB（例如，USB 2.0、USB 3.0）、火线、Thunderbolt等。此外，还应理解，某些设备可以具有“卡”型形式因数，诸如用户身份模块（SIM）卡或信用卡等。这些“卡”式设备可提供与支付用读取器的现有生态系统的向后兼容性，同时仍支持本文所述的改进功能。

[0051] 在一些实施例中，客户端设备300可另外包括其他部件，诸如包括任意数目的所熟知的I/O的用户接口子系统，所述I/O包括但不限于小键盘、触摸屏（例如，多点触摸界面）、液晶显示器（LCD）、背光、扬声器和/或麦克风。应当理解，在某些应用中，用户接口可不是必需的。例如，卡型客户端实施例可以没有用户接口。

[0052] 在例示的实施例中，客户端设备300包括安全元件308。安全元件308在该实施例中包括：执行在安全存储器308B中存储的软件的安全处理器308A。安全存储器308B不可被所有其他部件访问（安全处理器308A除外）。此外，可进一步在物理上强化安全元件308以使其不被篡改（例如，封入树脂中）。

[0053] 安全元件308能够接收、发送和存储一个或多个VME。在一个实施例中，安全元件308存储与用户相关联的VME阵列或多个VME（例如，信用“卡”、借记“卡”、预付费账号或卡号、公交卡、电影票、礼券、“忠诚度”程序元件等）。在一些变型中，每个VME还可与小型文件系统相关联，小型文件系统包括计算机可读指令和相关联的数据（例如，加密密钥、完整性密钥等）。

[0054] 文件系统可支持附加的特征。例如，文件系统可包括例如安全性（例如，保护与其他实体的通信的认证程序、授权程序和密码材料）、用户管理（例如，账户余额信息、最近交易历史等）等的程序和数据。相关领域的普通技术人员将容易地理解，VME及其相关联的文件系统是唯一且保全的数据资产。

[0055] 此外，在一个实施例中，安全元件308维持所存储的VME的列表或清单以及它们相关联的文件系统。该清单可包括与所存储的VME的当前状态有关的信息；此类信息可包括例如：可用性、有效性、账户信息（例如，当前余额等）和/或先前经历过的错误。该清单可被进一步链接或关联至用户接口，以使用户能够选择可用VME进行使用。在一些情况下，用户可选择一个VME来作为用于例如所有交易、与某个商户的所有交易、某个时间范围内的所有交易等的默认VME（例如，默认的信用卡）。

[0056] 在一些变型中，安全元件308可具有一个或多个相关联的设备密码密钥。这些设备密钥用于安全交换。在一种此类变型中，密码密钥是用于加密消息发送交易的非对称的公共/私有密钥对。公共密钥可自由地分发，而不损害私有密钥的完整性。例如，可基于芮韦斯特、莎米尔和艾德曼（Rivest，Shamir and Adleman）（RSA）算法对客户端设备300进行分配；公共密钥可提供给希望与客户端设备300安全通信的任何设备。用客户端设备300的用公共密钥加密的消息仅可被客户端设备自己的私有密钥（其安全地存储于客户端设备300中）解密。在其他变型中，密码密钥是对称的（即，加密设备和解密设备具有相同密钥）。对称变型可使密码的复杂性降低，但需要加密设备和解密设备两者强力保护共享密钥。

[0057] 在其他变型中，安全元件308可具有用于验证和/或发放数字证书的密码密钥。数

字证书可被用来例如验证（证书的）发放方的身份。例如，安全元件 308 可将数字证书发放给商户端设备，使得商户端设备此后能够证明交易已经发生（通过检索客户端设备的签名证书）。类似地，安全元件 308 能够验证从商户端设备提供以证明该商户端设备可信的数字证书。

[0058] 在客户端 - 商户端交易（或客户端 / 第三方中介交易）期间，安全元件 308 执行与相关联的一个或多个 VME 的交易。简单的实施例可为账号、“代理”号或它们的子集的传输。在更复杂的变型中，传输可包括例如交易量、密码保护、证据信息（例如，交易时间 / 日期和位置）、商户 ID 信息等。

[0059] 虽然本文所描述实施例中的许多实施例都是在金融交易的上下文中描述的，但非金融交易也同等适用。例如，代金券、票证等可根据使用情况来递增和 / 或递减信用数量。在其他示例中，交易可以是有效性检验；例如，公交卡在某个时间范围（例如，几天、几周、几月、几年等）内是有效的，因此在该时间范围内的任何使用次数也都是有效的。类似地，某些类型的通行证可受到例如“限用”日期影响，在这种情况下，该通行证在限用期内是无效的。

[0060] 在一些实施例中，客户端 - 商户端（或其他）交易在公共时间于客户端设备 300 和商户端设备之间执行（即，客户端设备 300 和商户端设备两者同时经历交易）；例如，在 NFC 交易中，客户端设备 NFC 接口设置成接近（“碰撞”）商户端设备 NFC 接口，后者诸如将信号发送至客户端设备 300 上的至少部分被动 NFC IC 的询问器。

[0061] 然而，应当理解，在另选场景中，客户端 - 商户端交易能够以时移方式执行。例如，客户端设备或商户端设备可在第一时间发起交易，并且对端设备稍后确认交易。一旦双方设备都确认了交易，则交易就可完成（例如，转移适量资金等）。例如，客户端和商户端在没有连通性的农贸市场执行交易。稍后当商户端设备连接至资产中介器时，交易被发起。此后，客户端设备同步其交易记录，完成交易。在一些情况下，资产中介器还可在发生未付款项时通知客户端设备。

[0062] 现在参考图 3B，展示了一种示例性商户端设备 350。示例性商户端设备 350 包括：商户端 - 客户端接口 352、处理器子系统 354、非暂态计算机可读介质（存储器子系统）356 和网络接口 358。如本文所用，术语“商户端设备”包括但不限于被配置为交易和 / 或查询对应于 VME 的服务器（例如，后端服务器 106)（例如，以确定交易是否应被允许等）的设备。应当理解，术语“商户端”的使用决不意在将其定义限制为购买或销售任何事物的实体所拥有或操作的设备。相反，期望该术语更广义地包括但不限于被配置用于或实现交易的装置，无论该交易是否针对商品、服务、虚拟报酬、获得或积累资金或信用、礼券兑现等。常见的商户端设备示例包括但不限于：信息亭、出纳机（例如，ATM)、“现金”出纳机、移动结账读取器（例如，基于 RFID 或条形码的读取器）、移动无线平板电脑甚至智能电话。此外，虽然商户端设备过去是专用型设备，但应理解，消费电子设备现在越来越为普遍，因此可使其能够促进小型业务（例如，具有无线功能的蜂窝电话、智能电话、个人计算机 (PC)、手持计算机、PDA、个人媒体设备 (PMD)、无线平板电脑、“平板手机”等），无论在制造时还是此后由第三方或设备用户本身调配时都是如此。

[0063] 处理器子系统 354 可包括以下器件中的一个或多个：数字信号处理器、微处理器、现场可编程门阵列、或安装在一个或多个基板上的多个处理部件。处理器子系统 354 还可

包括内部高速缓存存储器。处理器子系统 354 与存储器子系统 356 通信，后者包括存储器，存储器可例如包括 SRAM、闪存和 / 或 SDRAM 部件。存储器子系统 356 可实现一个或多个 DMA 型硬件，以有利于本领域熟知的数据访问。该示例性实施例的存储器子系统 356 包含能由处理器子系统 354 执行的计算机可执行指令。

[0064] 在一个示例性实施例中，商户端设备 350 包括适于连接至客户端设备的一个或多个接口，例如，商户端 - 客户端接口 352。商户端 - 客户端接口 352 可为无线接口，或另选地为物理接口（有线）。无线接口可包括具有最多几厘米的操作范围的“触摸”型接口（例如，RFID、NFC 等），以及更强的无线接口诸如 GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、Wi-Fi、蓝牙、无线 USB 等，或前述接口的任何组合。例如，商户端设备 350 可包括近距离 NFC 接口以及长距离 Wi-Fi 接口，甚至 WiMAX、卫星或蜂窝接口。常见的物理接口示例包括例如 USB、火线、Thunderbolt 等。在一些变型中，商户端 - 客户端接口 352 可作为读卡器或智能卡插卡器（例如，以维持与现有传统卡等的相容性）实施。

[0065] 在一些实施例中，商户端设备 350 还可包括其他部件，诸如包括任意数目的所熟知的 I/O 的用户接口子系统，所述 I/O 包括但不限于小键盘、触摸屏（例如，多点触摸界面）、LCD、背光、扬声器和 / 或麦克风。应当理解，在某些应用中，用户接口可以不是必需的。例如，简单的读卡器商户端设备可没有用户接口。

[0066] 在例示的实施例中，商户端设备 350 包括网络接口 358，该网络接口被配置为向资产中介器安全地报告与一个或多个 VME 的交易。在一些变型中，每个交易可另外存储在安全文件系统内，以供未来进行参阅 / 记账。常见的网络接口示例包括但不限于 :以太网、数字用户线路 (DSL)、电缆、光纤同轴电缆混合、无线局域网 (WLAN)、蜂窝数据连接等。

[0067] 在一些实施例中，商户端设备 350 可具有相关联的设备密码密钥或其他密码功能，诸如但不限于高级加密标准 (AES)/ 数据加密标准 (DES) 加密、互联网协议安全性 (IPSec)、多媒体互联网密钥管理 (MIKEY)、安全套接层 (SSL)/ 传输层安全性 (TLS)。这些设备密钥（和 / 或其他特征）可被用于安全交换。在一种此类变型中，密码密钥是非对称的公共 / 私有密钥对。在其他变型中，密码密钥是对称的密钥对。在其他变型中，商户端设备 350 可具有用于验证和 / 或发放数字证书的密码密钥。此外，可对 NFC 接口（在使用时）施加加密，诸如加密在传输过程中敏感的用户或付款信息。

[0068] 在示例性客户端 - 商户端交易期间，商户端设备 350 执行与相关联的一个或多个 VME 的交易。例如，商户端设备 350 可在交换商品 / 服务的过程中，接收（或请求）客户端设备的虚拟信用。所接收的信息可另外地包括例如交易量、有效性检验信息、密码保护、证据信息（例如，交易时间 / 日期和位置）、商户 ID 等。在其他实施例中，如果交易成功，商户端设备 350 可反过来向客户端设备报告，例如报告交易量、所使用的支付来源、商户 ID 等。

[0069] 在示例性商户端设备 - 资产中介器交易过程中，商户端设备 350 向资产中介器报告交易情况。这可包括报告与客户端设备的 VME 相关联的信息、要贷记 / 借记等的商户账户，以及交易量。作为响应，资产中介器确认该量已成功（不成功）从客户端设备的对应账户转移至商户端设备的账户。

[0070] 现在参考图 4，展示了一种示例性资产代理器 400。示例性资产代理器 400 包括 : 客户端设备接口 402、处理器子系统 404、非暂态计算机可读介质（存储器子系统）406 以及网络接口 408。如本文所用，术语“资产代理器”包括但不限于被配置成分发 VME 的实体。

常见的 VME 示例包括但不限于 :设备制造商、第三方经销商等。

[0071] 处理器子系统 404 可包括以下器件中的一个或多个 :数字信号处理器、微处理器、现场可编程门阵列、或安装在一个或多个基板上的多个处理部件。处理器子系统 404 还可包括内部高速缓存存储器。处理器子系统 404 与存储器子系统 406 通信,后者包括存储器,存储器可例如包括 SRAM、闪存和 / 或 SDRAM 部件。存储器子系统 406 可实现一个或多个 DMA 型硬件,以有利于本领域熟知的数据访问。该示例性实施例的存储器子系统 406 包含能由处理器子系统 404 执行的计算机可执行指令。

[0072] 在一个示例性实施例中,资产代理器 400 包括适于连接至客户端设备的一个或多个接口,例如,客户端设备接口 402。客户端设备接口 402 可为无线接口,或另选地为物理接口 (有线)。无线接口可包括例如 GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、Wi-Fi、蓝牙、无线 USB 等。常见的物理接口示例包括例如 USB、火线、Thunderbolt 等。

[0073] 在例示的实施例中,资产代理器 400 包括网络接口 408,该网络接口被配置为安全地报告利用资产中介器的一个或多个 VME 的分发。网络接口的常见的示例包括但不限于 :以太网、DSL、电缆、光纤同轴电缆混合、WLAN、蜂窝数据连接等。

[0074] 在一些实施例中,资产代理器 400 可具有相关联的设备密码密钥。这些设备密钥可用于安全交换。在一种此类变型中,密码密钥是非对称的公共 / 私有密钥对。在其他变型中,密码密钥是对称的密钥对。在其他变型中,资产代理器 400 可具有用于验证和 / 或发放数字证书的密码密钥。

[0075] 在一个示例性实施例中,资产代理器 400 具有并非是与安全元件先验关联的 (即,并非是与具有安全元件的设备相关联的) VME 的数据库。如下文更详细所述,VME 可由资产代理器根据 L2 安全层与安全元件相关联。L2 安全层防止 VME 在递送时被“克隆”。

[0076] 例如,在一个具体实施中,客户端设备请求并预先加载多个“质询”;每个质询用于验证请求的有效性和现时性 (例如,不是从先前请求重放)。更具体地,每个质询是一次性使用的质询,该质询是对于客户端设备的安全元件而言唯一有效的质询,即,一旦该质询被用掉,只有下一个质询才对安全元件有效。当用户对各账户签名时,VME 由资产代理器 400 调配。当客户端设备已耗尽所储备的质询时,用户可指示客户端设备请求一组新的质询。在一些变型中,VME 的转移在安全链路上执行,例如经由服务信息亭、通过虚拟专用网络 (VPN) 连接经由个人计算机 (PC) 等。

[0077] 现在参考图 5,展示了资产中介器 500 的一个示例性账户服务器 501。示例性账户服务器 501 包括 :网络接口 502、处理器子系统 504、非暂态计算机可读介质 (存储器子系统)506 以及账户数据库 508。如本文所用,术语“资产中介器”包括但不限于被配置为对与 VME 相关联的账户进行适当借记、贷记和 / 或验证的系统和网络。所述系统可包括一个或多个账户服务器,例如,账户服务器 501。因此,应当理解,提及到“资产中介器”也可指代资产中介器的一个或多个账户服务器,反之亦然。

[0078] 处理器子系统 504 可包括以下器件中的一个或多个 :数字信号处理器、微处理器、现场可编程门阵列、或安装在一个或多个基板上的多个处理部件。处理器子系统 504 还可包括内部高速缓存存储器。处理器子系统 504 与存储器子系统 506 通信,后者包括存储器,存储器可例如包括 SRAM、闪存和 / 或 SDRAM 部件。存储器子系统 506 可实现一个或多个 DMA 型硬件,以有利于本领域熟知的数据访问。该示例性实施例的存储器子系统 506 包含能由

处理器子系统 504 执行的计算机可执行指令。

[0079] 在一个示例性实施例中，账户服务器 501 包括适于建立与客户端设备和商户端设备的网络连接的网络接口 502。常见的网络接口示例包括但不限于：以太网、DSL、电缆 / 光纤同轴电缆混合、WLAN、无线城域网 (WMAN)、蜂窝数据连接、毫米波等。

[0080] 在一些实施例中，账户服务器 501 可具有相关联的密码密钥。这些密钥可用于安全信息交换。在一种此类变型中，密码密钥是非对称的公共 / 私有密钥对。在其他变型中，密码密钥是对称的密钥对。在其他变型中，账户服务器 501 可具有用于例如验证和 / 或发放数字证书的密码密钥。

[0081] 在一个示例性实施例中，账户服务器 501 被配置为对顾客账户认证并授权 VME。VME 由账户服务器 501 根据 L3 安全层来相关联。L3 安全层验证顾客账户 VME 组合是真实且经授权的（即，非欺骗性或滥用的）。

[0082] 现在参考图 6，展示了一种示例性资产锁定器 600。示例性资产锁定器可包括：网络接口 602、处理器子系统 604、非暂态计算机可读介质（存储器子系统）606 以及安全数据库 608。如本文所用，术语“资产锁定器”包括但不限于被配置成存储、加密和生成 VME 的设备。例如，资产锁定器 600 可为可信安全模块 (TSM)。

[0083] 处理器子系统 604 可包括以下器件中的一个或多个：数字信号处理器、微处理器、现场可编程门阵列、或安装在一个或多个基板上的多个处理部件。处理器子系统 604 还可包括内部高速缓存存储器。处理器子系统 604 与存储器子系统 606 通信，后者包括存储器，存储器可例如包括 SRAM、闪存和 / 或 SDRAM 部件。存储器子系统 606 可实现一个或多个 DMA 型硬件，以有利于本领域熟知的数据访问。存储器子系统 606 包含计算机可执行指令，这些指令可由处理器子系统 604 执行，但也可以使用其他类型的计算机化逻辑（例如，硬件和软件 / 固件的组合）。

[0084] 在一个示例性实施例中，资产锁定器 600 包括适于建立与一个或多个账户服务器的网络连接的网络接口 602。常见的网络接口示例包括但不限于：以太网、DSL、电缆、光纤同轴电缆混合、WLAN、蜂窝数据连接等。

[0085] 在一些实施例中，资产锁定器 600 可具有相关联的密码密钥。这些密钥可用于安全信息交换。在一种此类变型中，密码密钥是非对称的公共 / 私有密钥对。在其他变型中，密码密钥是对称的密钥对。在其他变型中，资产锁定器 600 可具有用于验证和 / 或发放数字证书的密码密钥。

[0086] 资产锁定器 600 还被配置为提供以及 / 或者生成一个或多个 VME。在一个示例性实施例中，按照特定标准（例如，美国国家标准学会 (ANSI) 标准 X4.13-1983（全文以引用方式并入本文））生成 VME，并将 VME 存储于安全数据库 608 内。另选地，可根据例如专有或特定用途的格式来构建 VME。阅读本发明的内容之后，相关领域的普通技术人员将容易地理解更多可能的格式。

[0087] 在一个示例性实施例中，资产锁定器 600 被配置成为客户端设备的安全元件加密 VME。资产锁定器 600 促使每个资产只有在被加密时根据 L1 安全层进行转移。L1 安全层促使 VME 仅存在于资产锁定器 600 或客户端设备的安全元件内的明文（未加密的）中。

[0088] 现在参考图 7，公开了用于在系统内分发 VME 的一般化方法 700 的一个实施例。在步骤 702 处，根据第一可信关系来保护一个或多个 VME 的内容。在一个示例性实施例中，第

一可信关系被配置为保护 VME 中包含的机密和 / 或密码材料（例如，安全密钥、密码材料、用户历史等）。例如，第一可信关系基于安全模块（实施于硬件或软件内），该安全模块被配置为根据唯一设备密钥或签注证书加密或解密 VME。具体地讲，安全模块被配置为加密用以递送至符合第一可信关系的期望目标设备（例如，客户端设备或商户端设备）的 VME，或解密从符合第一可信关系的源设备接收的访问控制客户端。在一个示例性实施例中，所有 VME 必须在设备之间转移时被加密（即，VME 无法以未加密形式被转移至任何其他设备）。处于第一可信关系级别的每个设备被给于唯一设备密钥和签注证书，所述唯一设备密钥和签注证书可被用于安全转移 VME。

[0089] 第一标准可信关系的各种具体实施还可受到物理和 / 或逻辑保护。例如，第一标准可信关系可包括硬件安全模块 (HSM) 内的保护，该 HSM 被配置为在被强制打开 / 访问的情况下自毁。更一般地，第一标准可信关系的示例性实施例以最低程度保护可信边界。常见的可信边界示例包括物理边界（例如，物理隔离等）和 / 或逻辑边界（例如，加密通信等）两者。

[0090] 在步骤 704 处，根据第二可信关系控制 VME 的副本数量。在一个示例性实施例中，第二可信关系被配置为防止意外和 / 或恶意复制 VME（强制保全）。例如，第二标准可信关系可由被配置成为其本身或另一个设备加密 VME 的安全模块管理。类似地，安全模块可对 VME 加密，使 VME 可仅被另一个特定设备解码（例如，基于非对称的密码密钥）。在一些实施例中，安全模块加密方案可以基于非对称密钥对；或另选地，安全模块加密方案可使用对称密钥对。

[0091] 如前所述，公共 / 私有密钥对是基于机密私有密钥、以及可公开的公共密钥。公共 / 私有密钥方案被认为是“非对称的”，因为用于加密和解密的密钥不相同，因此加密器和解密器不共享相同密钥。相比之下，“对称”密钥方案为加密和解密两者使用相同密钥（或一般转换的密钥）。RSA 算法是相关领域内常用的一种公共 / 私有密钥对密码术，但应理解，本文所描述的实施例决不限于 RSA 算法（或就此而言，决不限于非对称或对称密钥对）。

[0092] 公共 / 私有密码方案可用来将消息加密，并且 / 或者生成签名。具体地讲，可利用私有密钥将消息加密，并利用公共密钥将其解密，由此确保消息在传输中不被更改。类似地，可利用公共密钥验证利用私有密钥生成的签名，从而确保生成该签名的实体是合法的。在这两种使用情况下，私有密钥保持被隐藏，而公共密钥被自由地分发。

[0093] 在步骤 706 处，根据第三可信关系将 VME 分发给目标设备以供使用。第三可信关系需要实体认证和授权。更直接地，第三可信关系确保 VME 仅被发送至能够认证其身份并针对 VME 获得授权的实体。

[0094] 由于分发模型的灵活性，设想了许多不同方案，并且普通技术人员在阅读本发明时将会认识到这些方案。下文更详细公开了若干 VME 分发方案，它们是对根据本发明的各个方面的适于操作的各种各样方案的例示。

[0095] 现在参考图 8，示出了表示调配交易的一个示例性实施例的逻辑梯形图。该调配交易可由客户端设备、资产中介器、资产代理器以及资产锁定器进行。客户端设备包括安全元件 (SE) 和应用处理器 (AP)（例如，处理器子系统 304）。SE 可存储软件，软件包括有利于根据本发明的交易的所谓软件层“堆栈”。每个软件层负责一组分级功能，与其对应的对等软件层协商该功能。还应理解，在一些情况下，AP 可受到损害（例如，“已越狱”等）；因此，可

信关系仅存在于 SE 与对应的逻辑层实体之间；即，AP 不受信任。

[0096] 安全软件协议包括 L1 层、L2 层和 L3 层。L1 安全性对 VME 数据执行加密和解密。L1 操作限于安全的执行环境（例如 SE 或 TSM）。在 L1 内，VME 数据可以明文（即，未加密的）存储于逻辑 L1 边界内；在逻辑 L1 边界以外，VME 数据被安全地加密。L2 安全性防止 VME 数据被复制。L2 边界确保 VME 有且仅有一个副本在 L2 边界外。在 L2 边界内，可以存在多个副本。此外，L2 安全性还可将质询嵌入加密的 VME 数据中。在安装 VME 前，客户端设备可将 VME 中嵌入的质询与客户端设备上存储的质询进行比较，以便验证 VME 是否过期（即，该 VME 是当前的唯一 VME）。L3 安全性负责建立拥有 VME 的用户的信任、所有权和验证。对于每个 VME，SE 可以存储信息以指示与 VME 相关联的所有权。

[0097] 在一个示例性实施例中，资产锁定器是 TSM，其被配置为生成 VME 的数据组件并大批量地存储 VME。资产锁定器根据 L1 安全性执行 VME 操作，并且确保只有加密的 VME 被发送（即，VME 不会在资产锁定器外以未加密的形式发送）。为了向顾客调配 VME，资产代理器从资产锁定器接收加密 VME，并且存储 VME 以便根据需要向客户端设备调配 VME。资产代理器根据 L2 安全性执行 VME 操作，并且确保加密 VME 只有一个副本被调配给客户端设备。最后，资产中介器的示例性实施例根据 L3 安全性执行 VME 操作，并促进仅向具有已认证并被授权的 SE 的客户端设备发送加密 VME。一旦 VME 已递送至客户端设备，资产中介器就将 VME 与同客户端设备相关联的账户和 / 或同客户端设备的用户相关联的账户相关联。

[0098] 在一个实施例中，存储于客户端设备中的软件应用程序请求向用户的账户调配新的虚拟信用卡 (VCC) 以供使用。利用 AP 执行该软件应用程序。在 802 处，AP 从 SE 处请求唯一识别客户端设备或 SE 的信息。例如，该信息可包括设备标识符。在 804 处，在对新 VCC 的请求中，AP 向资产中介器发送设备标识符。资产中介器认证对将 VCC 调配至用户账户的请求。认证基于设备标识符。在该实施例的一个方面，资产中介器通过确定 SE/ 客户端设备与用户账户相关联而认证该请求。

[0099] SE 可利用数字签名对设备标识符进行加密，使得该设备标识符从客户端设备安全地发送至资产中介器。一旦资产中介器认证 / 授权了新 VCC，资产中介器就向资产代理器转发 SE 数字签名。在 806 处，资产代理器验证 SE 数字签名，由此针对 VCC 唯一地识别目标 SE。在 807 处，向客户端设备提供另外的 VCC 选项。

[0100] 简而言之，所谓的“质询”是用于将特定 VME 与 SE 相关联的关键资源。具体地讲，每个 SE 维持某个数量的质询，从而维持 L2 安全性。通过验证质询是有效的，SE 可以确保 VME 不是“过期”的 VME（即，无效或者无用的复制）。当接收到具有匹配的质询数据的 VME 时，SE 删除质询。考虑以下具体实施，SE 创建（或被给予）多个质询，这些质询为与资产代理器所共享。此后，资产代理器可将当前质询嵌入已经为 SE 调配的 VME 中。当 SE 接收 VME 时，SE 可验证所接收的 VME 包含适当质询并且没有过期。

[0101] 上述方案的一个可能的缺点是，固定数量的质询可能容易受到拒绝服务 (DOS) 攻击的影响。在 DOS 攻击中，连续触发 SE 以生成质询，直到耗尽其所有质询资源。为此，SE 的示例性实施例另外执行与资产中介器 / 资产代理器的会话握手，然后处理将触发 SE 消耗质询的请求。另外，在资源被耗尽且 SE 无法创建新质询的罕见情况下，SE 可以存储一组单独的保留质询，该组质询被专门指定以便释放另一组质询。在一些情况下，SE 还可包括原始设备制造商 (OEM) 凭据，OEM 可以使用此凭据进一步控制质询操作。

[0102] 在 808 处，AP 请求 SE 提供质询来与 VCC 相关联。一旦 SE 提供质询，就在 810 处向资产中介器发送质询，并且随后在 812 处转发给资产代理器。在 814 处，资产代理器验证质询，并且随后将个性化信息提供给资产锁定器。在 816 处，资产锁定器为 SE 个性化新的 VCC，并且将相关联的 VCC 标识符提供给资产中介器。接着，在 817 处，资产中介器将 VCC 标识符提供给 AP。在 818 处，AP 一旦接收到 VCC 标识符，就可请求递送 VCC。此后，在 820 处，资产中介器可向客户端设备的 SE 提供 VCC。

[0103] 相关网络领域的普通技术人员将认识到，在运营大规模分发网络期间会出现很多实际问题。具体地讲，大规模分发网络必须可缩放，以应对大量突发性流量（诸如可在客户端设备的所谓“首发日”发生的情况）。用于减少总体网络流量的一个方案是延期递送 VME（如果可能的话）。

[0104] 现在参考图 9A 和图 9B，公开了用于在系统内分发 VME 的一般化方法 900 的一个实施例。在预个性化操作过程中，具有 SE 的所谓“预个性化”客户端设备被预先分配有 VME，然后才会发运（即，当用户在商店购买设备时、在线订购设备等时）。在 902 处，在向用户递送客户端设备前，扫描设置在与客户端设备相关联的箱盒上的标贴、标签或其他标记。例如，箱盒可为包封客户端设备的零售包装。标贴包含唯一识别客户端设备并可与 VME 相关联的信息（例如，设备标识符）。可为客户端设备预先配置 VME，方式为例如 :(i) 在 904 处，利用特定于 SE(L1) 的密钥（从标贴确定）加密 VME ;(ii) 在 906 处，将指定的初始质询嵌入 VME(L2) 中 ;并且 (iii) 在 908 处，将 VME 与用户的认证 / 授权信息 (L3)（在购买时确定）相关联。随后，在 910 处，将 VME 分配给唯一识别 VME 的标示符，例如，VME 标识符。此后，在 912 处，客户端设备可使用 VME 标识符来请求 VME。在 914 处，一旦接收到请求和 VME 标识符，VME 就可以其完全配置状态被递送给客户端设备。

[0105] 前述方案基于从客户端设备（和 / 或与客户端设备相关联的箱盒）收集的信息以及在购买时来自用户的信息，有效地预先配置 VME。在设备处于运输状态（例如，装运、送货上门等）时，尽力配置 VME（即，配置在资源可用时发生）。此后，在不需要实时流量的情况下，可将 VME 从缓存位置无缝加载到客户端设备中。为了尽可能提高系统可靠性，所述预先配置的 VME 还可以冗余方式缓存于多个地理位置 ;即，使在不同地理位置的多个数据中心具有重复的 VME(L2 安全性提供初始质询方案，使得在检索到 VME 的首个副本时，复制品失效）。

[0106] 更直接地，不同于常规的制造方案，客户端设备的示例性实施例并未用利 VME 制造和预先配置。VME 的配置和递送可被“延期”，直到客户端设备已制造并且 / 或者部署后才进行。例如，如果多个 VME 可受该客户端设备支持，那么在用户激活账户后，该客户端设备可具有稍后可配置有所选 VME 的通用软件。在一些具体实施中，该通用软件可包括通用或默认 VME。在该具体实施中，用户在购买客户端设备时，可被允许（或被要求）提供与默认 VME 一起使用的信用卡账户（或类似物）。此后，一旦客户端设备被激活，默认 VME 就在激活序列中被自动加载。

[0107] 现在参考图 10A 和图 10B，公开了用于在系统内分发 VME 的一般化方法 1000 的另一个实施例。在这个变型中，在 1002 处，在具有 SE 的客户端设备被装运时（即，在用户在商店处购买设备、在线订购设备等时）从 VME 池向其分配 VME，即，特定 VME 不与客户端设备相关联。此时，在 1004 处，用户能够提供认证 / 授权信息。在 1006 处将客户端设备递送给

用户后，通过例如销售商点、在家中的用户等来输入唯一识别客户端设备的信息。可从设置在与客户端设备相关联的箱盒上的标贴、标签或其他标记取得该信息。该信息还可指示应为客户端设备分配某个 VME，但该 VME 尚未被分配。在 1008 处，响应于接收到该信息，资产中介器、资产代理器以及资产锁定器协作分配可用 VME，方式为例如：在 1010 处，利用特定于 SE(L1) 的密钥（从标贴确定）加密 VME；在 1012 处，将质询数据嵌入 VME(L2) 中；并且在 1014 处，将 VME 与用户的认证 / 授权信息 (L3)（在购买时确定）相关联。在 1016 处，新创建且加密的 VME 以其完全配置状态被递送给客户端设备。

[0108] 前述方案根据需要有效地配置 VME。此类具体实施允许资产中介器和 / 或资产代理器智能地管理 VME 池。由于 VME 池中的每个 VME 未被分配给特定的客户端设备（即，专用于特定用途）并且按需来被分配，因此资产中介器和 / 或资产代理器不必跟踪尚未激活的库存（例如，一些设备可能先被购买，而后在激活之前被退货，这就减少了不必要的 VME “流失”）。在 VME 是有限资源的情况下，这可能是有用的。相关领域中的普通技术人员将容易地了解，账号是有限的资源（并因此就其稀缺性而言是珍贵的）；例如，ANSI 标准 X4.13-1983（先前全文以引用方式并入本文）是大多数国家信用卡系统使用的账户编号系统。根据十六 (16) 位信用卡号的 ANSI 标准 X4.13-1983，在这十六位中只有部分位表示实际账号（例如，八 (8) 位可仅用于表示多达 1 千万个唯一账号）；其他位被认为有其他用途（例如，识别发卡机构、提供“校验”值、识别卡号等）。

[0109] 现在参考图 11，公开了用于在系统内分发 VME 的一般化方法 1100 的另一个实施例。在该实施例中，VME 的配置可被完全延期，直到发生了初始具有之后才进行配置。在系统与客户端设备之间将发生多个具有（例如，周期性具有）的情况下，该实施例可为有用的。例如，用户可选择购买例如多个电影通行证 (movie pass)、公交月卡等。在 1102 处，用户向系统提供付款信息，例如，信用卡信息。在 1104 处，将识别客户端设备的信息（例如客户端设备标识符）提供给系统。可根据任何前述实施例来提供设备标识符（例如，“预个性化”过程、由用户输入、由 AP 提供等）。初始具有通常可在 1106 处执行。同时，使用设备标识符、所提供的付款信息和 / 或质询数据为客户端设备配置 VME；在 1108 处配置 VME 后，在 1110 处，向客户端设备递送 VME 以供后续使用。在一些情况下，递送可以基于就绪、自动下载、或手动下载时的推送通知。

[0110] 现在参考图 12，公开了用于在系统内分发 VME 的一般化方法 1200 的另一个实施例。可利用与具有 SE 的客户端设备、资产代理器和资产锁定器通信的资产中介器来执行方法 1200。在 1202 处，资产中介器从客户端设备接收用来将 VME 调配给用户账户以供使用的请求。该账户可与客户端设备的用户相关联（即，账户为该用户所拥有）。该请求可包括唯一地与客户端设备相关联的身份信息，例如，设备标识符。在该实施例的一个方面，该请求还可包括发送识别该账户的信息。接着，在 1204 处，资产中介器认证该请求。资产中介器能够通过验证设备标识符所识别的客户端设备与账户相关联来认证该请求。随后，资产中介器与资产代理器和资产锁定器协作，根据本文所描述实施例来为账户调配 VME 并为客户端设备配置 VME。在 1206 处，资产中介器从资产锁定器接收 VME 标识符。VME 标识符识别为客户端设备配置的 VME。随后，在 1208 处，资产中介器向客户端设备发送 VME 标识符。客户端设备能够存储 VME 标识符，并且随后在从资产中介器请求所配置的 VME 时使用 VME 标识符。一旦在 1210 处从客户端设备接收对 VME 的请求，资产中介器就可在 1212 处向客户

端设备发送所配置的 VME。

[0111] 现在参考图 13A 至图 13C，公开了用于在系统内分发 VME 的一般化方法 1300 的另一个实施例。可由与能够包括资产代理器、资产中介器和资产锁定器的调配系统通信的客户端设备来执行方法 1300。该客户端设备可包括 SE 和 AP。应当注意，为了清楚和方便起见，下文描述在客户端设备和资产中介器之间执行的方法 1300。应当了解，方法 1300 的步骤还可在客户端设备和调配系统的一个或多个实体（例如，资产代理器、资产中介器）之间执行。

[0112] 在 1302 处，客户端设备接收输入，该输入指示将 VME 调配给用户账户以供使用的期望。该输入可由用户使用客户端设备上的 I/O 接口（例如，按钮、小键盘、触摸屏、语音命令等）输入。在 1304 处，客户端设备可从 SE 请求身份信息。该身份信息唯一地与客户端设备相关联，例如，设备标识符。可从 SE 获得身份信息。在另选实施例中，可从客户端设备外部的来源获得身份信息。例如，用户可从客户端设备的箱盒上的标贴获得身份信息，并使用客户端设备的 I/O 设备输入该身份信息。

[0113] 在 1306 处，一旦从 SE 接收设备标识符，客户端设备就可向资产中介器发送对调配 VME 的请求。除了请求之外，在 1308 处，客户端设备还向资产中介器发送设备标识符。在 1310 处，客户端设备从资产中介器接收对质询的请求。质询可用来根据如本文所述的 L2 安全性验证 VME。在 1312 处，响应于从资产中介器接收到请求，AP 可从 SE 请求质询。在 1314 处，一旦从 SE 接收到质询，客户端设备就可向资产中介器发送质询。调配系统可认证该请求，并为客户端设备配置 VME。接着，在 1316 处，客户端设备可从资产中介器接收 VME 标识符。VME 标识符可唯一地识别配置用于客户端设备的 VME。随后，在 1318 处，客户端设备可向资产中介器发送对所配置的 VME 的请求。除了请求之外，在 1320 处，客户端设备发送 VME 标识符。在 1322 处，响应于接收到请求和 VME 标识符，资产中继器可向客户端设备递送所配置的 VME。在 1324 处，SE 可通过验证所接收的 VME 被嵌入有有效质询数据，来验证所接收的 VME 是有效的（即，所接收的 VME 没有过期）。

[0114] 应当理解，虽然在方法的步骤的具体顺序的方面描述了某些特征，但是这些描述仅仅例示本文公开的更广泛方法，并且可根据特定应用的需求而修改。在某些情况下，某些步骤可呈现为不必要的或可选的。此外，可将某些步骤或功能性添加至所公开的实施例，或者可对两个或多个步骤的执行次序加以排列。所有此类变型被认为包含在本文的公开和权利要求内。

[0115] 此外，可单独地或以任何组合方式来使用所述实施例的各方面、实施例、具体实施或特征。可由软件、硬件或硬件与软件的组合来实现所述实施例的各个方面。所述实施例还可体现为计算机可读介质上的计算机可读代码。计算机可读介质为可存储数据的任何数据存储设备，所述数据其后可由计算机系统读取。计算机可读介质的示例包括只读存储器、随机存取存储器、CD-ROM、HDD、DVD、磁带和光学数据存储设备。计算机可读介质还可分布在网络耦接的计算机系统中，以使得计算机可读代码以分布式方式来存储和执行。

[0116] 在上述描述中，为了进行解释，所使用的特定命名提供对所述实施例的彻底理解。然而，对于本领域的技术人员而言将显而易见的是，实践所述实施例不需要这些具体细节。因此，对特定实施例的上述描述是出于举例说明和描述的目的而呈现的。这些描述不旨在被认为是穷举性的或将所述的实施例限制为所公开的精确形式。对于本领域的普通技术人

员而言将显而易见的是，根据上述教导内容，许多修改和变型是可能的。

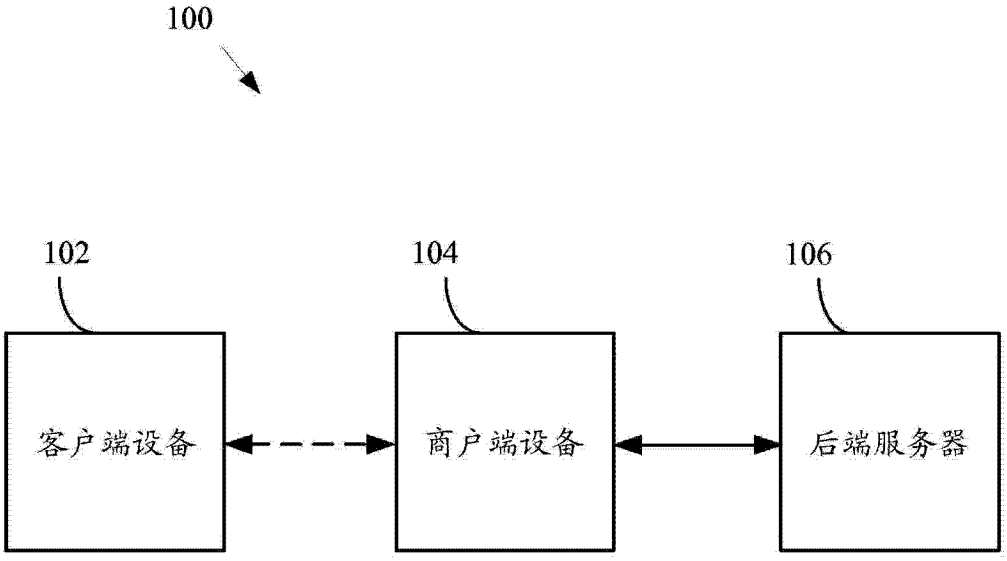


图 1

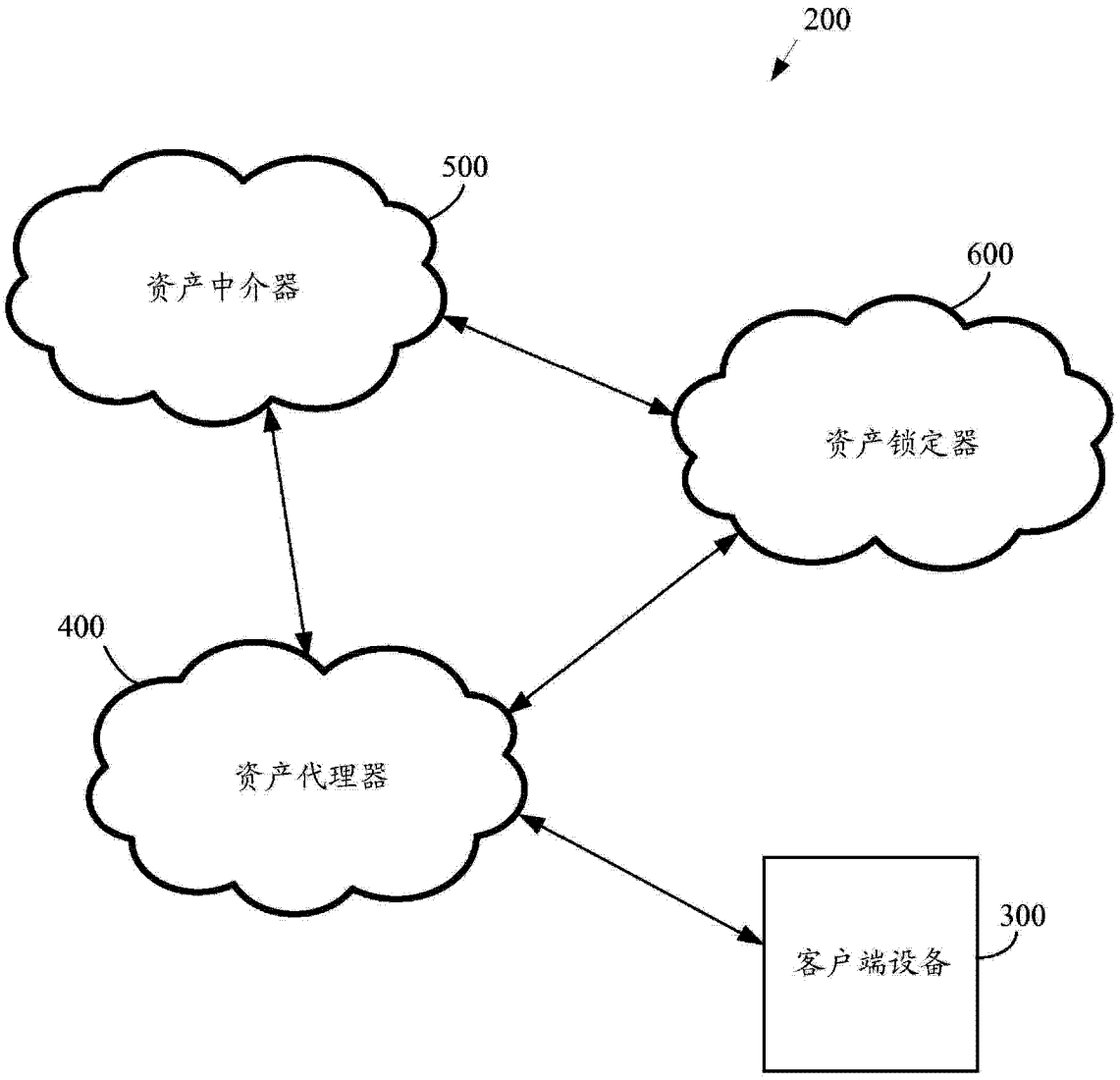


图 2

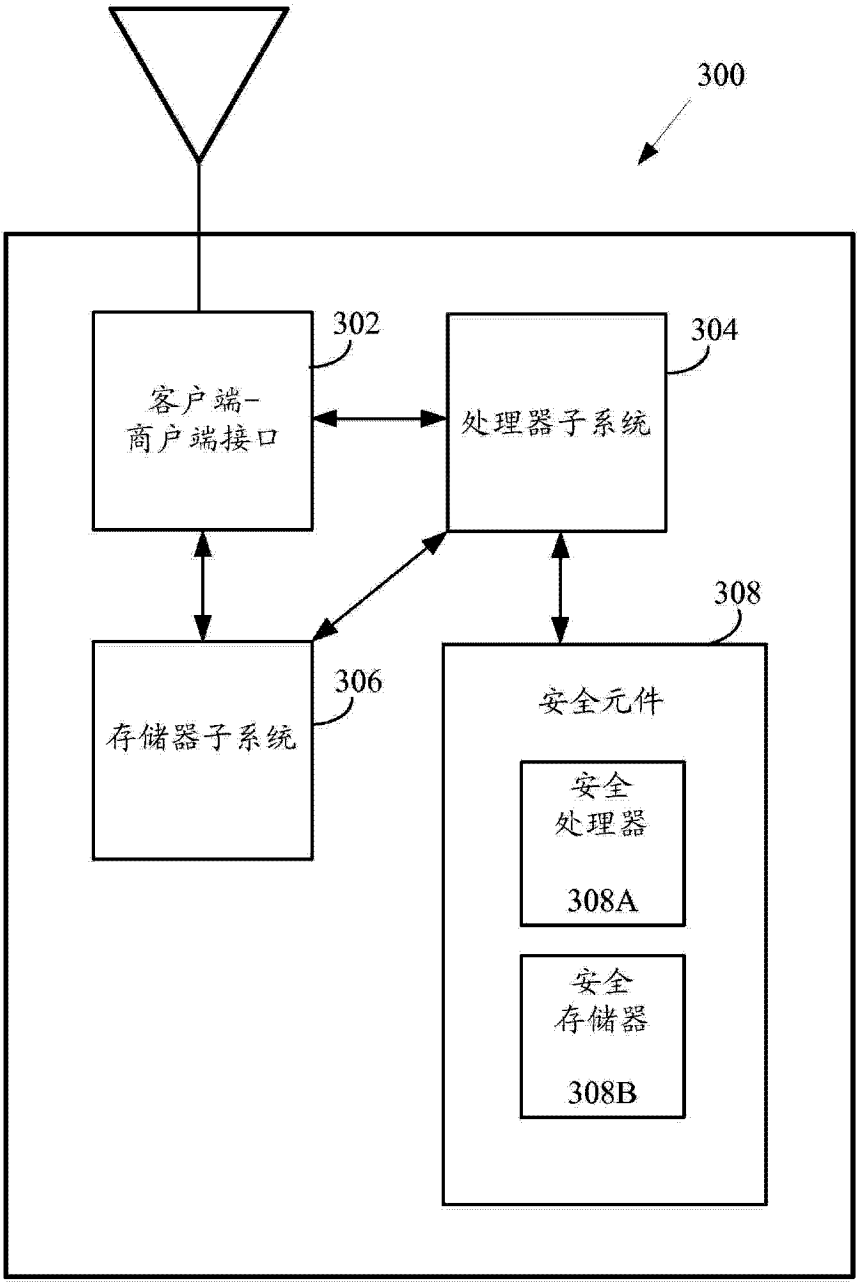

300
302
客户端-
商户端接口
304
处理器子系统
306
存储器子系统
308
安全元件
安全
处理器
308A
安全
存储器
308B

图 3A

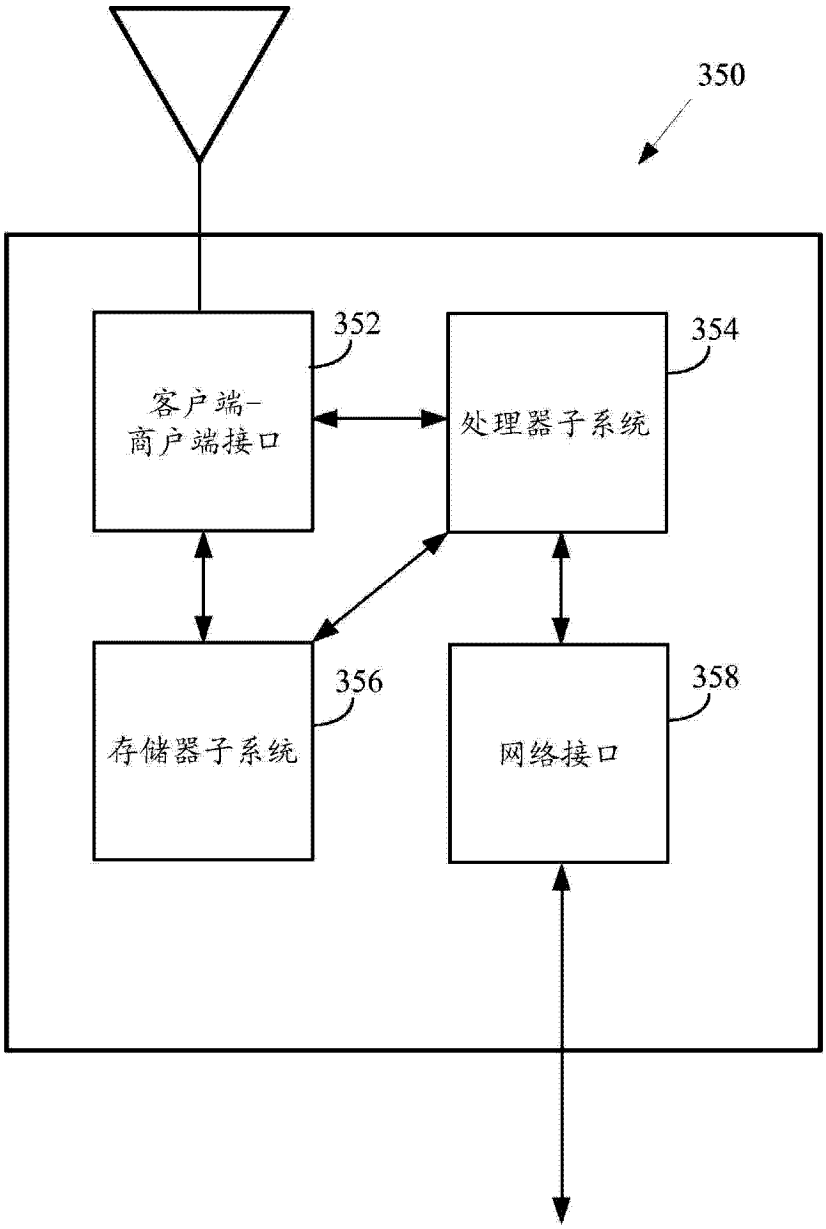


图 3B

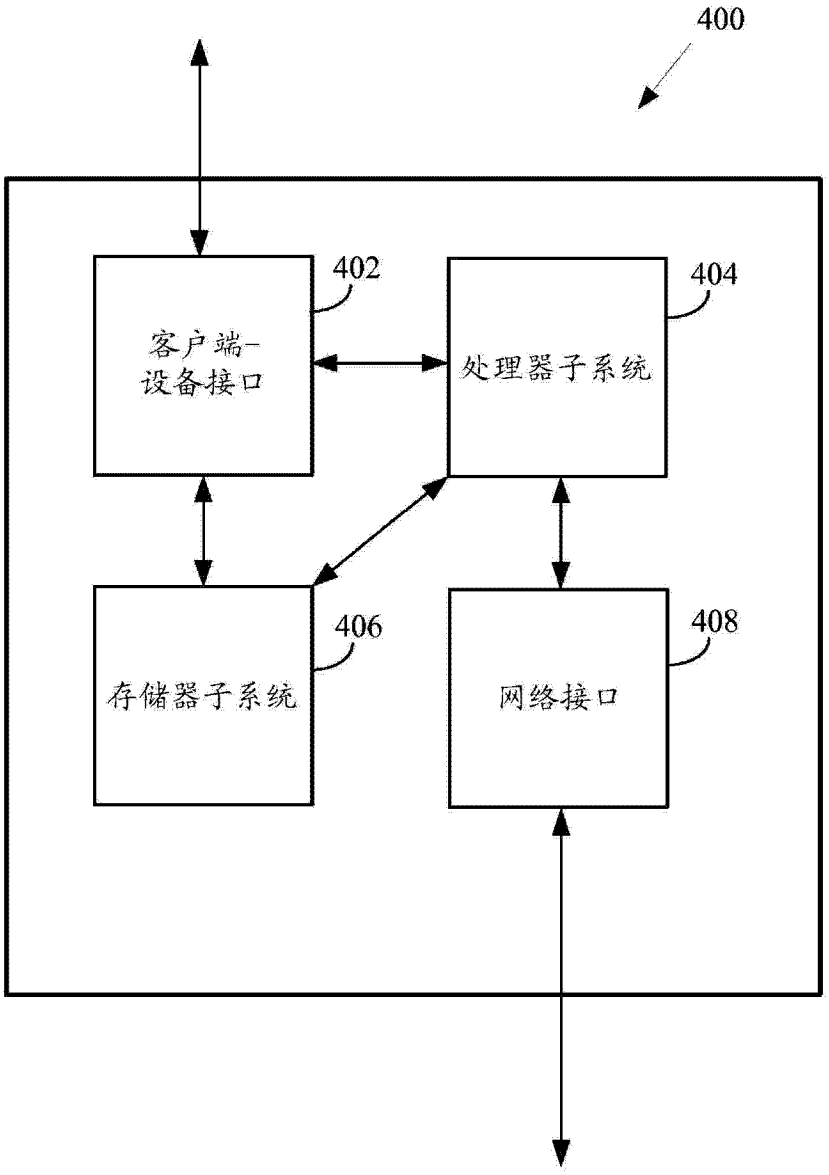


图 4

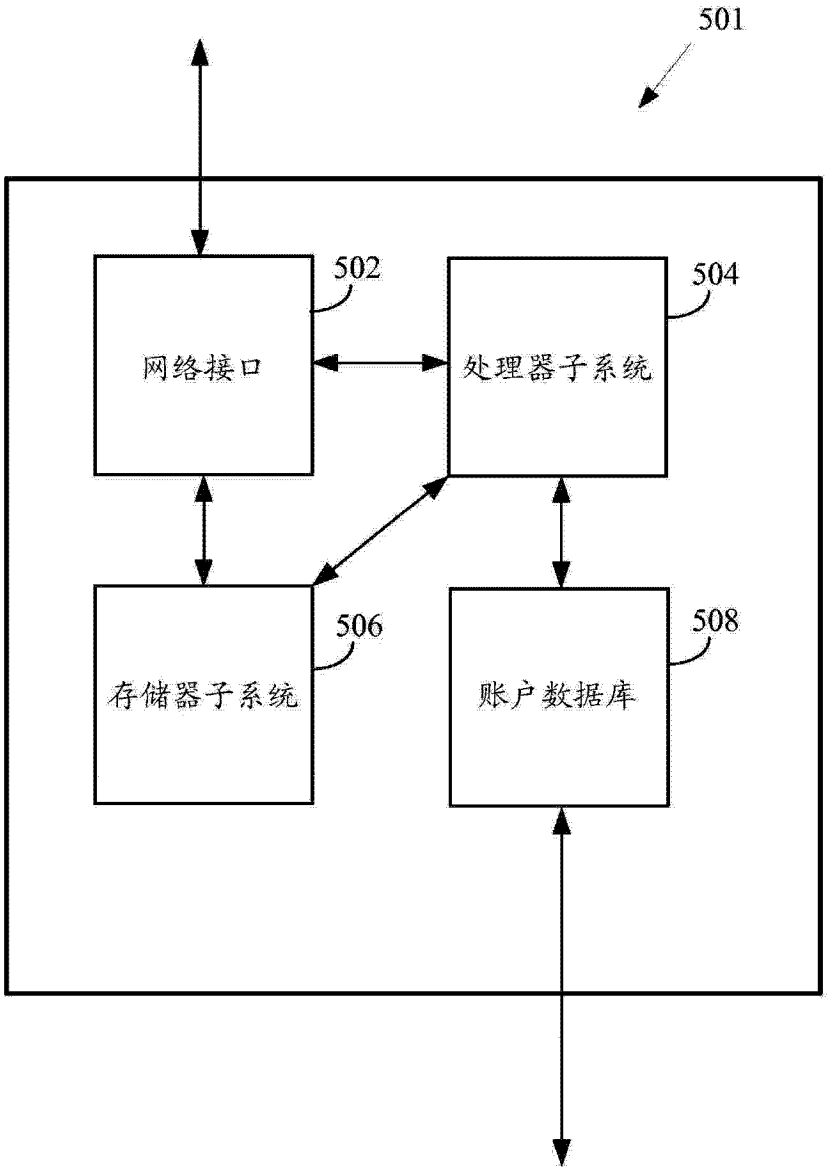


图 5

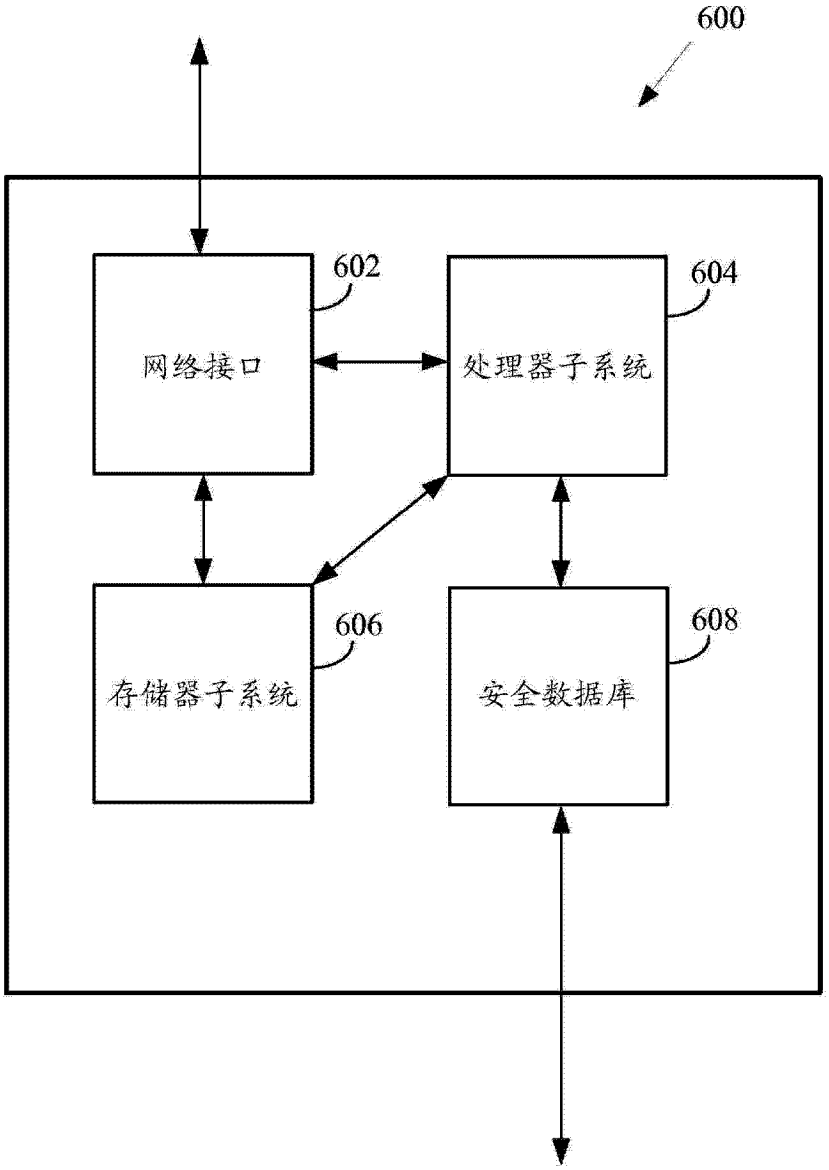


图 6

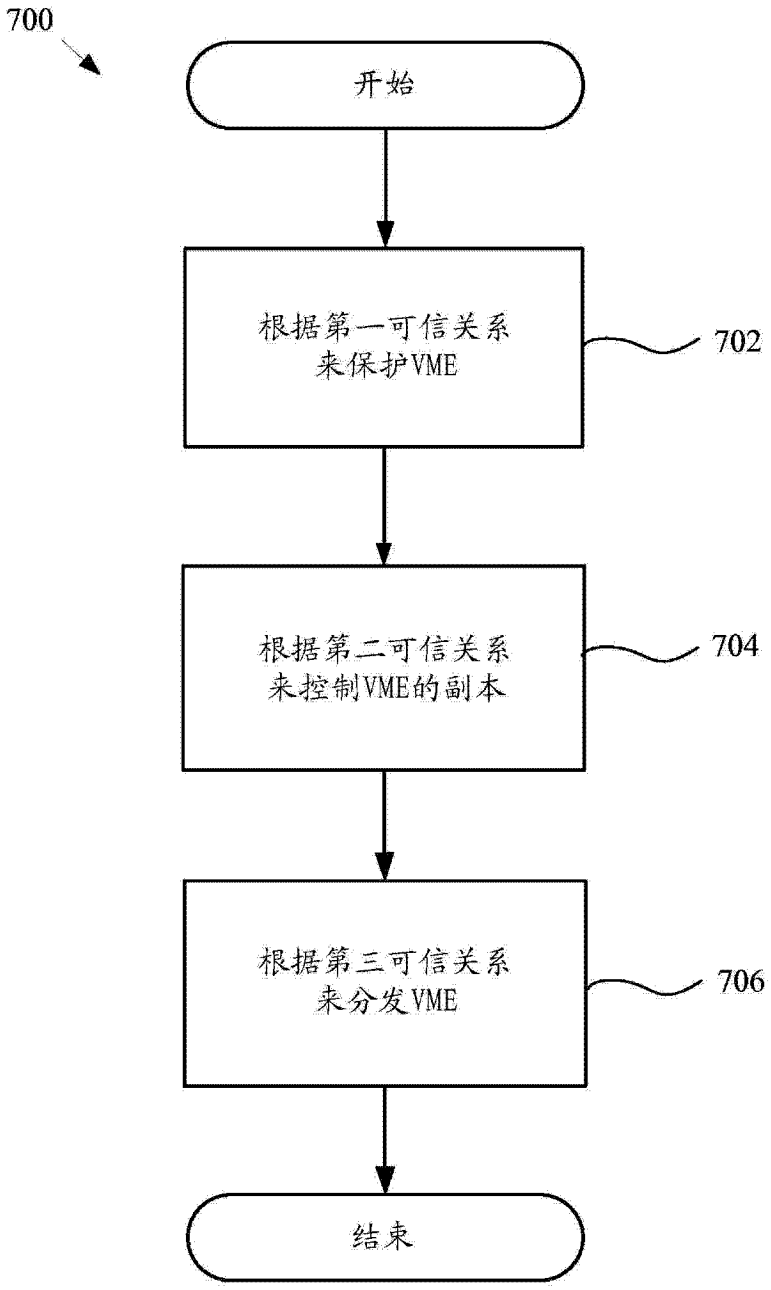

700
开始
根据第一可信关系来保护VME
702
根据第二可信关系来控制VME的副本
704
根据第三可信关系来分发VME
706
结束

图 7

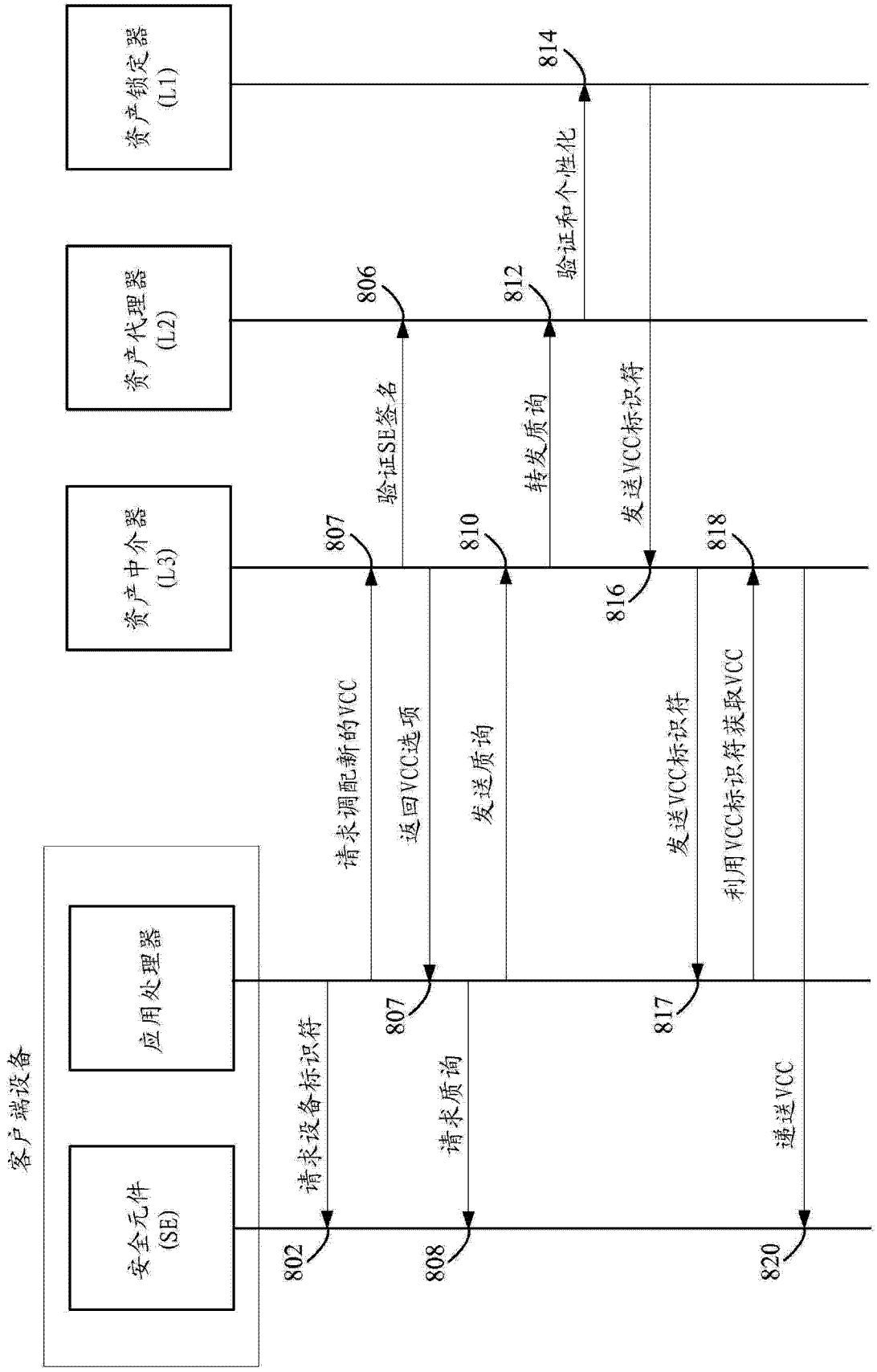

客户端设备
安全元件 (SE)
应用处理器
资产中介器 (L3)
资产代理器 (L2)
资产锁定器 (L1)
请求设备标识符
802
请求质询
808
807
返回VCC选项
请求调配新的VCC
807
发送质询
810
转发质询
812
验证SE签名
806
验证和个性化
814
816
发送VCC标识符
817
利用VCC标识符获取VCC
818
递送VCC
820

图 8

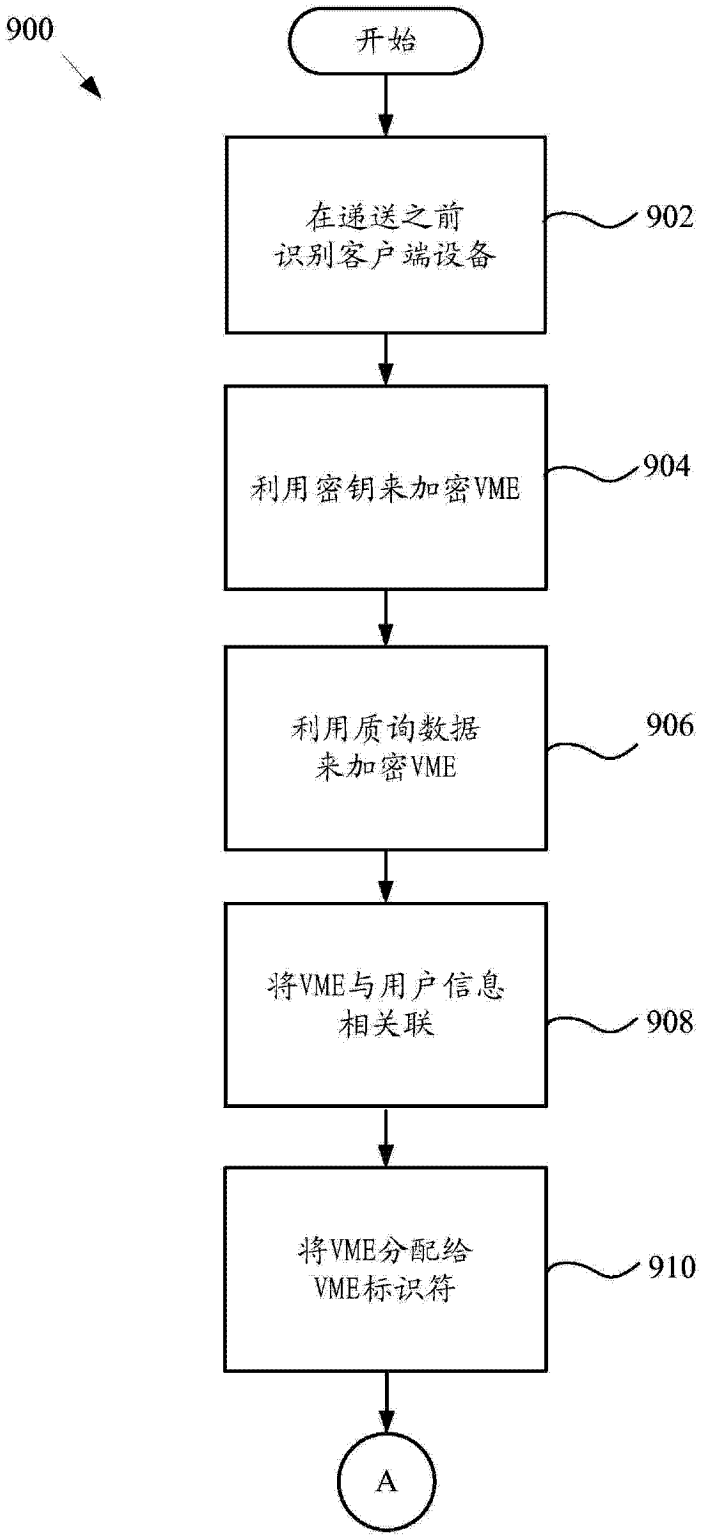

900
开始
在递送之前
识别客户端设备
902
利用密钥来加密VME
904
利用质询数据
来加密VME
906
将VME与用户信息
相关联
908
将VME分配给
VME标识符
910
A

图 9A

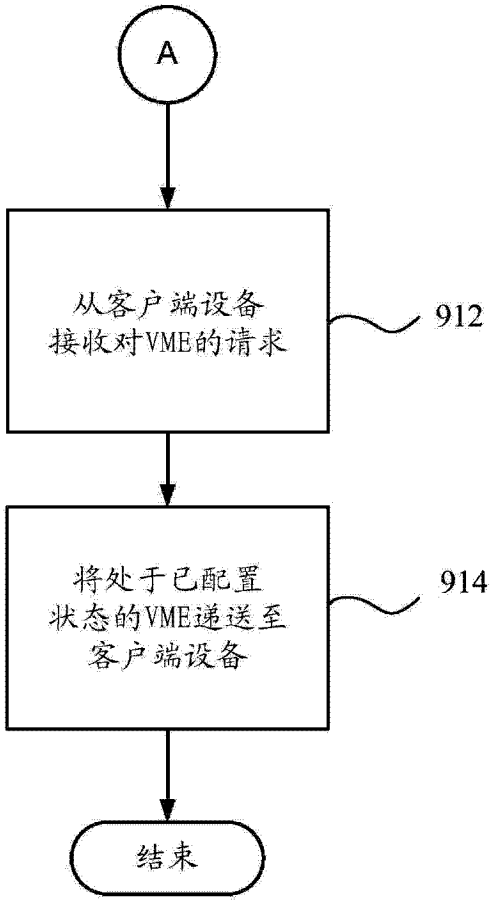

A
从客户端设备
接收对VME的请求
912
将处于已配置
状态的VME递送至
客户端设备
914
结束

图 9B

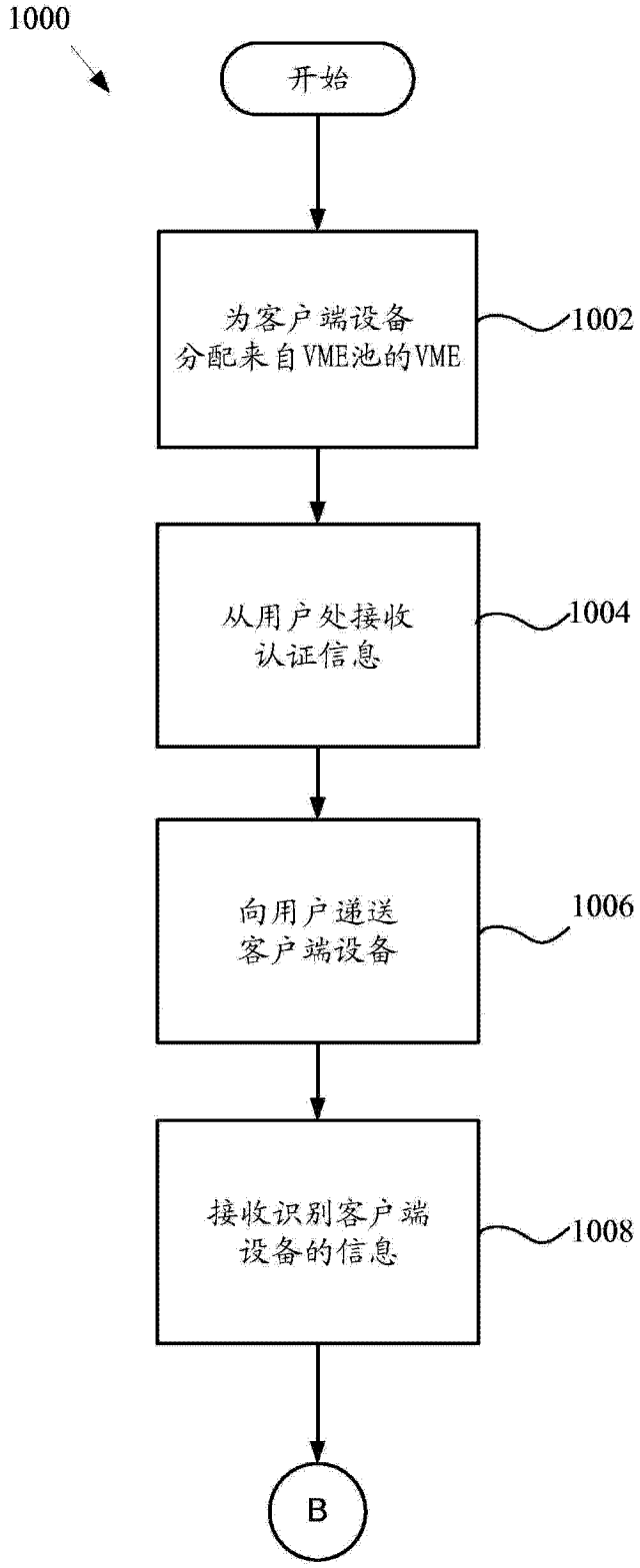

1000
开始
为客户端设备
分配来自VME池的VME
1002
从用户处接收
认证信息
1004
向用户递送
客户端设备
1006
接收识别客户端
设备的信息
1008
B

图 10A

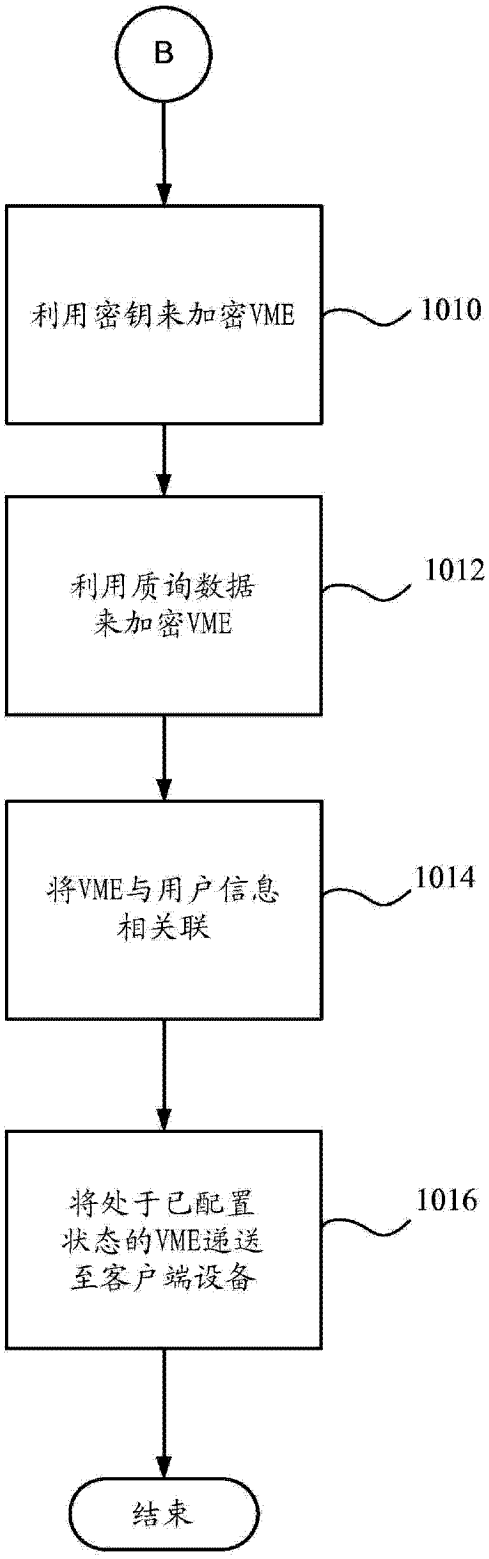

B
利用密钥来加密VME
1010
利用质询数据
来加密VME
1012
将VME与用户信息
相关联
1014
将处于已配置
状态的VME递送
至客户端设备
1016
结束

图 10B

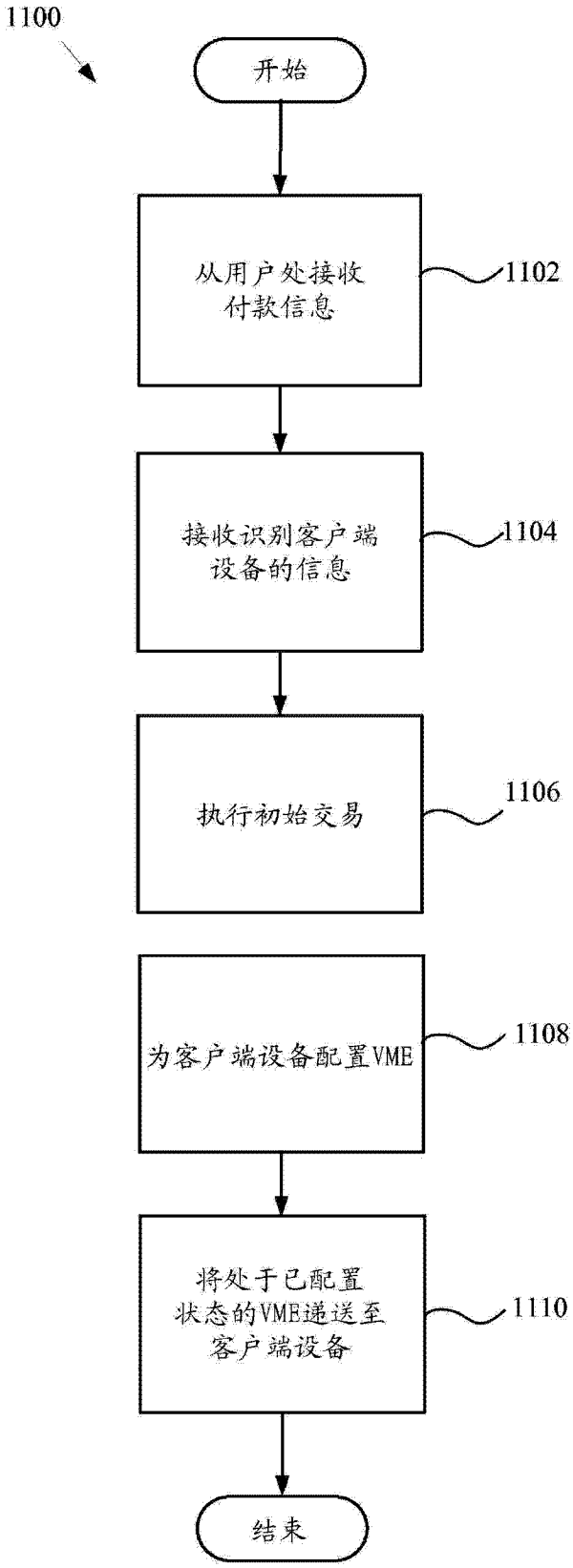

1100
开始
从用户处接收付款信息
1102
接收识别客户端设备的信息
1104
执行初始交易
1106
为客户端设备配置VME
1108
将处于已配置状态的VME递送至客户端设备
1110
结束

图 11

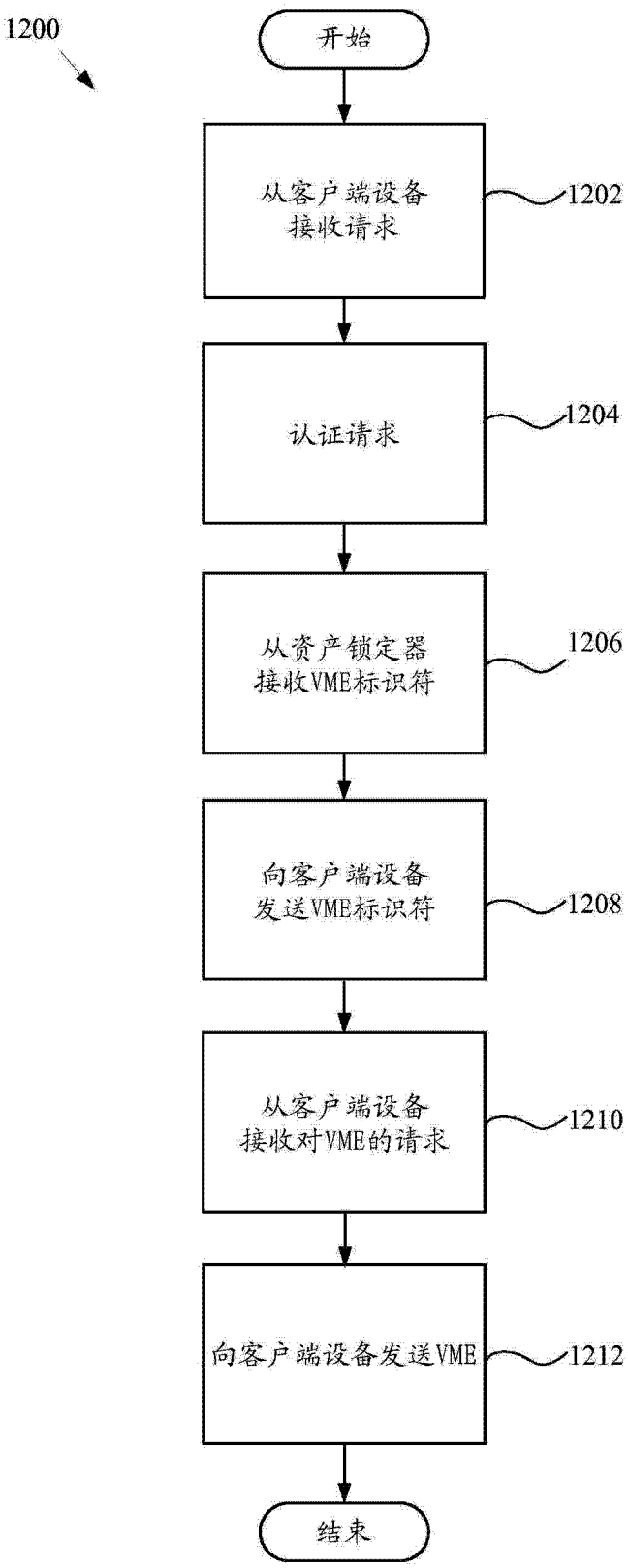

1200
开始
从客户端设备
接收请求
1202
认证请求
1204
从资产锁定器
接收VME标识符
1206
向客户端设备
发送VME标识符
1208
从客户端设备
接收对VME的请求
1210
向客户端设备发送VME
1212
结束

图 12

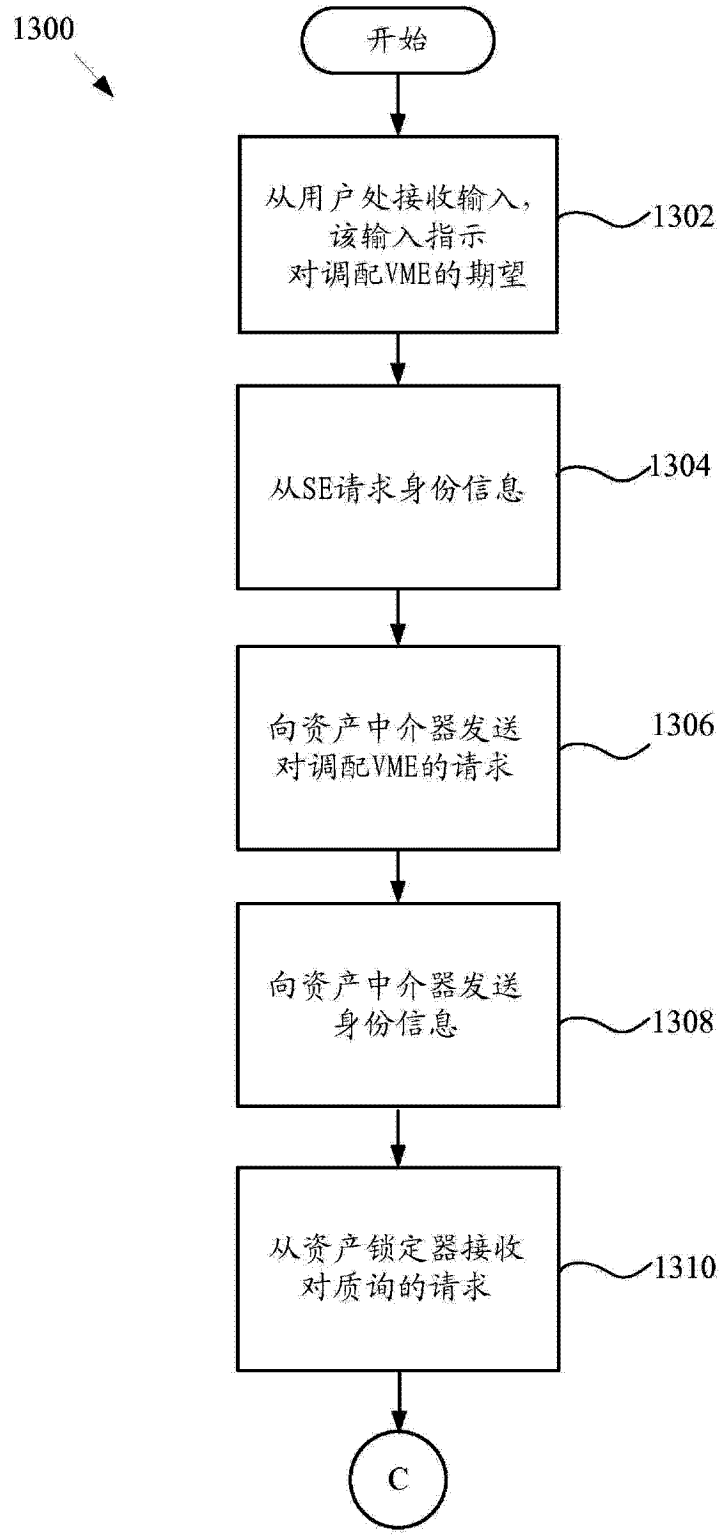

1300
开始
从用户处接收输入，该输入指示对调配VME的期望
1302
从SE请求身份信息
1304
向资产中介器发送对调配VME的请求
1306
向资产中介器发送身份信息
1308
从资产锁定器接收对质询的请求
1310
C

图 13A

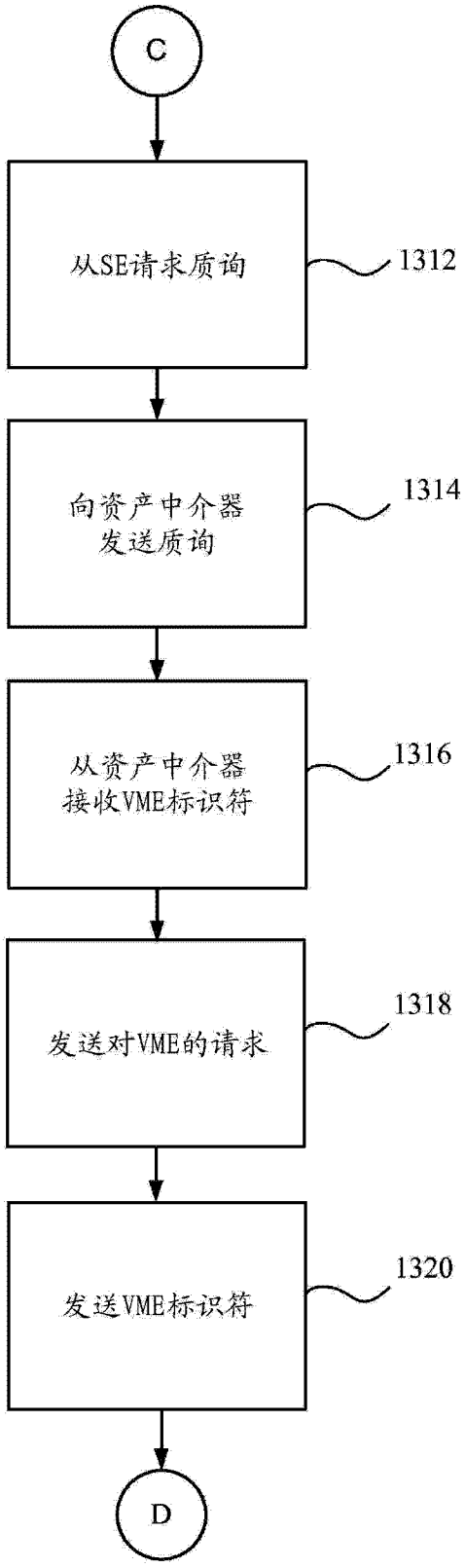

C
从SE请求质询
1312
向资产中介器发送质询
1314
从资产中介器接收VME标识符
1316
发送对VME的请求
1318
发送VME标识符
1320
D

图 13B

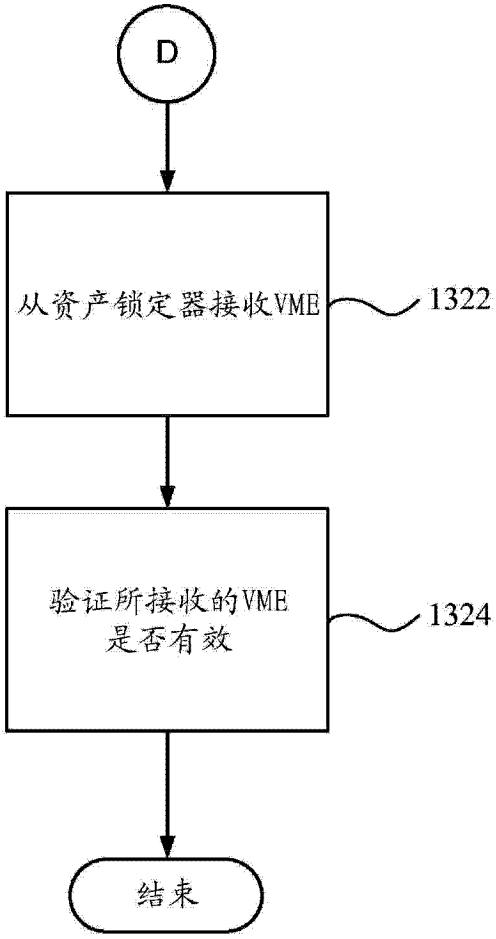


图 13C