(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201443800 A
(43)公開日： 中華民國 103 (2014) 年 11 月 16 日

(21)申請案號：103103966 (22)申請日： 中華民國 103 (2014) 年 02 月 06 日
(51)Int. Cl.： *G06Q20/40 (2012.01)* *G06Q20/36 (2012.01)*
(30)優先權：2013/02/06 美國 61/761,654
(71)申請人：蘋果公司 (美國) APPLE INC. (US)
美國
(72)發明人：哈葛提 大衛T HAGGERTY, DAVID T. (US)；可汗 艾哈默A KHAN, AHMER A. (US)；夏普 克里斯多弗 SHARP, CHRISTOPHER (US)；浩克 傑諾德 凡 HAUCK, JERROLD VON (US)；林狄 喬金 LINDE, JOAKIM (SE)；麥克勞林 凱文P MCLAUGHLIN, KEVIN P. (US)；柴特 麥地 ZIAT, MEHDI (DZ)；維德 尤瑟夫H VAID, YOUSUF H. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：20 項 圖式數：13 共 59 頁

(54)名稱

用於資產之安全元件交易及管理之裝置及方法

APPARATUS AND METHODS FOR SECURE ELEMENT TRANSACTIONS AND MANAGEMENT OF ASSETS

(57)摘要

本發明揭示用於配置財務票據及其他資產之方法及裝置。在一實施例中，揭示保證始終安全地加密某一資產，只存在該資產之唯一複本且該資產被遞送至一經鑑認及/或經授權客戶之一安全軟體協定。另外，揭示尤其能夠處置大訊務叢發(諸如在器件之所謂的「上市日」可發生者)的佈建系統之例示性實施例。

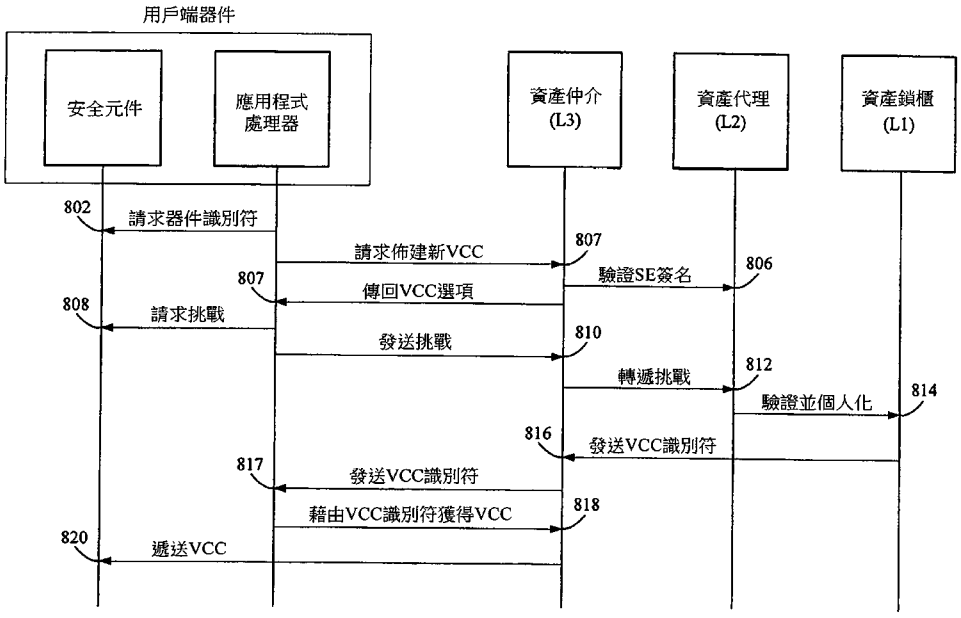

圖8

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201443800 A
(43)公開日： 中華民國 103 (2014) 年 11 月 16 日

(21)申請案號：103103966 (22)申請日： 中華民國 103 (2014) 年 02 月 06 日
(51)Int. Cl.： *G06Q20/40 (2012.01)* *G06Q20/36 (2012.01)*
(30)優先權：2013/02/06 美國 61/761,654
(71)申請人：蘋果公司 (美國) APPLE INC. (US)
美國
(72)發明人：哈葛提 大衛T HAGGERTY, DAVID T. (US)；可汗 艾哈默A KHAN, AHMER A. (US)；夏普 克里斯多弗 SHARP, CHRISTOPHER (US)；浩克 傑諾德 凡 HAUCK, JERROLD VON (US)；林狄 喬金 LINDE, JOAKIM (SE)；麥克勞林 凱文P MCLAUGHLIN, KEVIN P. (US)；柴特 麥地 ZIAT, MEHDI (DZ)；維德 尤瑟夫H VAID, YOUSUF H. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：20 項 圖式數：13 共 59 頁

(54)名稱

用於資產之安全元件交易及管理之裝置及方法

APPARATUS AND METHODS FOR SECURE ELEMENT TRANSACTIONS AND MANAGEMENT OF ASSETS

(57)摘要

本發明揭示用於配置財務票據及其他資產之方法及裝置。在一實施例中，揭示保證始終安全地加密某一資產，只存在該資產之唯一複本且該資產被遞送至一經鑑認及/或經授權客戶之一安全軟體協定。另外，揭示尤其能夠處置大訊務叢發(諸如在器件之所謂的「上市日」可發生者)的佈建系統之例示性實施例。

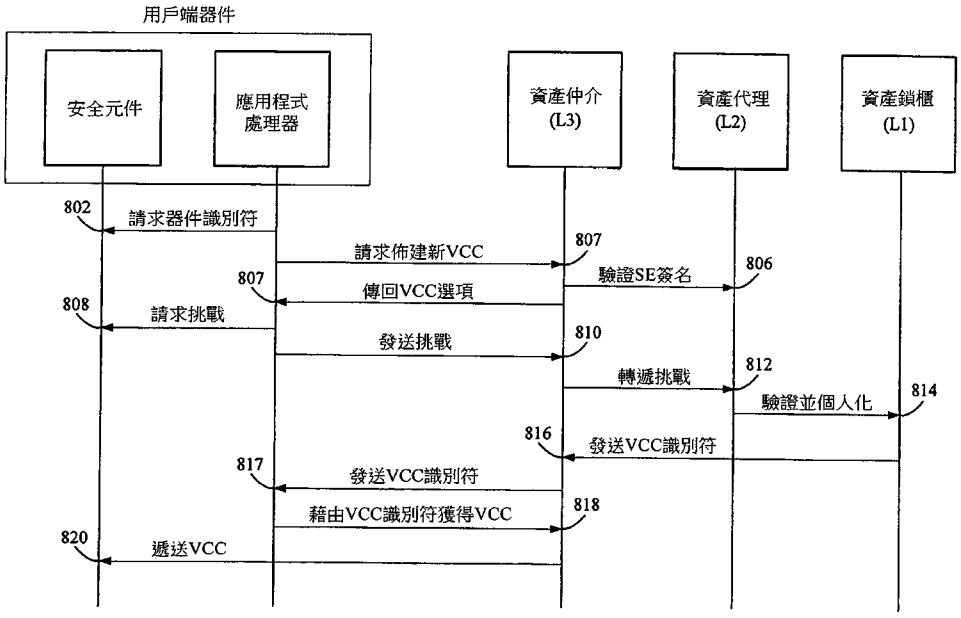

圖8

201443800

發明摘要

※ 申請案號：103103966

※ 申請日： 103.2.6 ※IPC 分類：G06Q 20/40 (2012.01)

G06Q 20/36 (2012.01)

【發明名稱】

用於資產之安全元件交易及管理之裝置及方法

APPARATUS AND METHODS FOR SECURE ELEMENT TRANSACTIONS AND MANAGEMENT OF ASSETS

【中文】

本發明揭示用於配置財務票據及其他資產之方法及裝置。在一實施例中，揭示保證始終安全地加密某一資產，只存在該資產之唯一複本且該資產被遞送至一經鑑認及/或經授權客戶之一安全軟體協定。另外，揭示尤其能夠處置大訊務叢發(諸如在器件之所謂的「上市日」可發生者)的佈建系統之例示性實施例。

【英文】

Methods and apparatus for the deployment of financial instruments and other assets are disclosed. In one embodiment, a security software protocol is disclosed that guarantees that the asset is always securely encrypted, that one and only one copy of an asset exists, and the asset is delivered to an authenticated and/or authorized customer. Additionally, exemplary embodiments of provisioning systems are disclosed that are capable of, among other things, handling large bursts of traffic (such as can occur on a so-called "launch day" of a device).

【代表圖】

【本案指定代表圖】：第（8）圖。

【本代表圖之符號簡單說明】：

無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】

用於資產之安全元件交易及管理之裝置及方法

APPARATUS AND METHODS FOR SECURE ELEMENT TRANSACTIONS AND MANAGEMENT OF ASSETS

【技術領域】

本發明大體上係關於安全器件交易之領域，且更特定言之，在一例示性實施例中係關於財務工具及其他資產之配置。

【先前技術】

客戶及商家大體上需要用於執行財務及其他相關交易之便利且安全構件。諸如信用卡、轉帳卡、預付卡、禮品卡、優待券等之資產皆為貨幣之愈發「虛擬化」本質的實例。具體而言，藉由(例如)帳號或「代理(proxy)」帳號(例如，一人出於處理銷售點處之交易的目的所產生，但並非實際收款帳號或付款帳號)執行交易，且以電子方式收款/付款基金，而非實際上交換實體貨幣或貨物及/或服務之實體優待券。

不幸的是，由於本文中所詳細描述之原因，用於散發此等資產之現存解決方案效率低下且易於失效。舉例而言，虛擬錢包範例可係基於預先存在之帳戶；且為了執行貨幣化交易，用戶端器件之使用者必須具有具錢包服務(例如，提供與錢包相關聯之帳戶處理資料庫的可信實體)之預先存在帳戶，或已預付錢包服務。另外，現存資產並非「可替代的」，且當其產生時，其專用於特定用途。

由於客戶及商家已不斷地演變交易複雜性及/或便利性(包括行動器件之愈發普遍使用)，因此需要用於散發資產之新的經改良方案。

理想地，此等解決方案應在不破壞資產之靈活性的情況下為客戶、商家及發佈實體提供合理且便利之管理能力。

【發明內容】

本發明藉由提供(尤其)用於資產之安全元件交易及管理之裝置及方法而處理前述需要。

在一實施例中，揭示一種用於將一資產散發至一用戶端器件的方法。可藉由自該用戶端器件接收將該資產佈建至一帳戶的一請求而進行該方法。佈建該資產之該請求可伴隨有唯一地識別該用戶端器件之一器件識別符。然後，鑑認佈建該資產之該請求。在一種狀況下，在驗證該用戶端器件是否與該帳戶相關聯時使用該器件識別符鑑認佈建該資產之該請求。在鑑認該請求之後，將該資產佈建至該帳戶並將該資產指派至該用戶端器件。然後，自諸如一資產鎖櫃(asset locker)之一遠端器件接收唯一地識別該經指派資產之一資產識別符。接著將該資產識別符發送至該用戶端器件。隨後，該用戶端器件可使用該資產識別符請求該經指派資產。在自該用戶端器件接收對該經指派資產及該資產識別符之一請求之後，將該經指派資產遞送至該用戶端器件。

在另一實施例中，揭示一種用於將一資產散發至一用戶端器件的方法。該用戶端器件與唯一地識別該用戶端器件之一器件識別符相關聯。藉由為該用戶端器件預組態該資產而進行該方法。該預組態程序可包括(i)藉由基於該器件識別符之一唯一密鑰加密該資產，(ii)將挑戰資料嵌入該資產中，及/或(iii)將該資產與一使用者帳戶相關聯。因此，為該用戶端器件組態或「個人化」該資產。然後，將該經預組態資產與一資產識別符相關聯。在該實施例之一態樣中，在預組態該資產之前將該資產識別符提供至該用戶端器件。該用戶端器件可接著請求該經預組態資產。該請求可包括該資產識別符。在接收該請求之

後，可將該經預組態資產遞送至該用戶端器件。

在又一實施例中，揭示一種電腦可讀儲存媒體。該電腦可讀儲存媒體儲存當由一用戶端器件之一處理器執行時導致該用戶端器件發送將一資產佈建至一帳戶之一請求的指令。可將該請求發送至一遠端器件。該帳戶可與該用戶端器件之一使用者相關聯。該用戶端器件可發送唯一地識別該用戶端器件之一器件識別符以及該請求。在該實施例之一態樣中，將該器件識別符儲存於安置於該用戶端器件中之一安全元件上。此外，亦可將一或多個挑戰儲存於該安全元件上。該等指令進一步導致該用戶端器件將一挑戰傳輸至該遠端器件。該用戶端器件可接著自該遠端器件接收該資產。該所接收資產可包括該安全元件可使用，以驗證該所接收資產是否有效之挑戰資料。該挑戰資料可基於該所傳輸挑戰。

僅僅出於總結一些實例實施例之目的而提供此總結，以便提供對本文中所描述之標的物的一些態樣之基本理解。因此，將瞭解，上文所描述之特徵僅為實例，且不應視為以任何方式縮小本文中所描述之標的物的範疇或精神。自以下詳細描述、圖式及申請專利範圍，本文中所描述之標的物的其他特徵、態樣及優勢將變得顯而易見。

本發明之其他態樣及優勢自以下結合隨附圖式之詳細描述將變得顯而易見，該等隨附圖式藉由實例說明所描述之實施例的原理。

【圖式簡單說明】

參考如下描述及隨附圖式，可較好地理解所描述之實施例。另外，參考如下描述及隨附圖式，可較好地理解所描述之實施例的優勢。

圖1為根據本發明的交易網路之一例示性組態的圖形表示。

圖2為根據本發明的佈建系統之一例示性組態的圖形表示。

圖3A為根據本發明的用戶端器件之一例示性實施例的邏輯區塊

圖式。

圖3B為根據本發明的商家器件之一例示性實施例的邏輯區塊圖式。

圖4為根據本發明的資產代理(asset agent)之一例示性實施例的邏輯區塊圖式。

圖5為根據本發明的資產仲介(asset broker)之帳戶伺服器的一例示性實施例之邏輯區塊圖式。

圖6為根據本發明的資產鎖櫃之一例示性實施例的邏輯區塊圖式。

圖7為根據本發明的用於散發資產之一般化方法的一實施例之邏輯流程圖。

圖8為根據本發明的表示例示性佈建交易之邏輯梯形圖。

圖9A及圖9B展示根據本發明的用於散發資產之一般化方法的另一實施例之邏輯流程圖。

圖10A及圖10B展示根據本發明的用於散發資產之一般化方法的另一實施例之邏輯流程圖。

圖11為根據本發明的用於散發資產之一般化方法的另一實施例之邏輯流程圖。

圖12為根據本發明的用於散發資產之一般化方法的另一實施例之邏輯流程圖。

圖13A、圖13B及圖13C展示根據本發明的用於散發資產之一般化方法的另一實施例之邏輯流程圖。

【實施方式】

根據本申請案之方法及裝置的代表性應用描述於此部分中。此等實例僅係為了添加內容脈絡及輔助理解所描述之實施例之目的而提供。因此，對熟習此項技術者而言，可在無此等具體細節中之一些或

全部的情況下實踐所描述之實施例係顯而易見的。在其他情況下，未詳細描述熟知之程序步驟以便避免不必要地混淆所描述之實施例。其他應用係可能的，使得不應將以下實例視為係限制性的。

在以下之詳細描述中，參看形成該描述之部分且藉由說明展示根據所描述之實施例的具體實施例的隨附圖式。儘管以充分細節描述此等實施例以使得熟習此項技術者能夠實踐所描述之實施例，但應理解此等實例並非係限制性的，使得可使用其他實施例，且在不脫離所描述之實施例的精神及範疇的情況下可作出改變。

虛擬化「錢包」可為客戶、商家及財務機制提供大量益處。虛擬化錢包之虛擬「內容」可包括一或多個資產。任何實體(例如，使用者、商家、財務機制等)可在適當致能且安全之器件之間自由地傳送此等資產；此外，可靈活地儲存、備份等此等資產。現存之解決方案提供某些基本交易，例如，經由網際網路協定(IP)網路進行散發、更新、修補等。然而，歸因於財務交易及資訊之敏感本質，需要大量安全措施以防止竊取、誤用、惡意行為等。

應注意，出於此論述之上下文的目的，貫穿本發明之實施例描述呈虛擬化交易媒介(VME)之形式的資產。虛擬化交易媒介之共用實例包括(但不限於)：信用「卡」編號、轉帳「卡」編號、預付「卡」編號、帳戶資訊及虛擬化貨幣等。更大體而言，虛擬化交易媒介亦涵蓋無實際價值之票據，例如，電子優待券、電子憑單、電子票證、電子通行證等。應理解，本描述並非限制性的，且所描述之實施例可用於散發任何有用及/或有價值之事物。此外，VME可實施於複雜性變化之廣泛多種資料結構內(例如，字串、陣列、物件、密碼編譯元件等)；例如，簡單實施可為簡單之帳號，較複雜之實施可併有帳戶資訊及/或檢查值。在一些狀況下，VME可提供額外特徵，諸如，密碼編譯保護、問責(亦即，交易歷史)、匿名、詐騙偵測等。

所描述之實施例係關於用於VME之安全交易及管理之方法及裝置。在一實施例中，佈建系統將VME散發至用戶端器件。佈建系統包括一或多個實體，其管理VME並根據具有三個等級(其可被稱作L1、L2及L3)之安全協定，將VME散發至用戶端器件。在L1處，安全地產生、儲存並加密VME。可藉由一或多個資產鎖櫃促進L1。L2控制並管理VME之有效複本的數目。L2可防止無意及/或惡意之複製VME。在實施例之一態樣中，一旦已散發VME之第一複本，L2可使用一或多個挑戰以失效VME之重複複本。可藉由一或多個資產代理促進L2。L3進行鑑認並授權將資產散發至預期用戶端器件。在實施例之一態樣中，L3可在鑑認程序期間使用自安置於用戶端器件中之安全元件所獲得的識別符。L3亦可在鑑認程序期間使用與使用者之帳戶相關聯的資訊。可藉由一或多個資產仲介促進L3。

在一實施例中，揭示一種用戶端器件與佈建佈建之間的佈建交易。佈建系統包括資產仲介、資產代理及資產鎖櫃。用戶端器件包括與用戶端器件相關聯之器件識別符。可將識別符儲存並加密於安置於用戶端器件中之安全元件中。當使用者(亦即，客戶)購買用戶端器件時，可產生使用者帳戶。替代性地，當購買用戶端器件時，使用者帳戶可為由使用者所識別之預先存在帳戶。用戶端器件向資產仲介請求VME，並提供識別資訊，例如，器件識別符。資產仲介鑑認識別資訊，並判定SE/用戶端器件與使用者帳戶相關聯。在鑑認之後，資產仲介可將SE之簽名轉遞至資產代理。資產代理驗證安全元件之識別碼，並識別用於該安全元件之VME。然後，安全元件將挑戰提供至佈建系統。可由資產代理將基於所提供之挑戰的挑戰資料嵌入VME中。因此，挑戰資料可用於防止發佈VME之重複複本。資產鎖櫃可接著為用戶端器件之安全元件提供與VME相關聯之識別符(例如，VME識別符)。在接收VME識別符之後，用戶端器件可隨後使用VME

識別符，向資產仲介請求遞送VME。

在另一實施例中，可推遲VME之組態及遞送，直至使用者購買具有安全元件之用戶端器件為止。以此方式，並不藉由VME製造或預程式化用戶端器件。實情為，「預個人化」用戶端器件，使得在將用戶端器件遞送至使用者之前，其預指派有VME。「預個人化」程序可包括使儲存於佈建系統中之VME相關聯於與用戶端器件相關聯之識別符。在購買時，使用者提供鑑認資訊。在傳輸時(例如，當使用者購買用戶端器件與當使用者請求VME之間的時間，及/或將用戶端器件運輸至使用者所花費之時間)，可針對用戶端器件預組態VME。預組態VME可包括(i)藉由特定於安全元件之密鑰加密VME，(ii)將挑戰資料嵌入VME中，及(iii)使VME與鑑認資訊相關聯。接著，使VME與VME識別符相關聯。然後，用戶端器件可使用VME識別符請求VME。隨後，佈建系統可將VME遞送至經預組態之用戶端器件。以此方式，當請求VME時，可將VME順暢地載入至用戶端器件上而不要求即時訊務。

在又一實施例中，在自用戶端器件接收請求VME之前，為用戶端器件分配來自VME集區之VME (例如，VME集區中之每一VME最初並不與特定用戶端器件相關聯)。當購買用戶端器件時，使用者提供鑑認資訊。可將用戶端器件提供至使用者。除用戶端器件以外，亦將可用於鑑認用戶端器件之識別資訊(例如，唯一地識別用戶端器件之器件識別符)提供至使用者。舉例而言，可自安置於封裝用戶端器件之箱子上的貼紙搜集器件識別符。接著當請求激活VME時，用戶端器件可在使用者之指令下將器件識別符提供至佈建系統。

下文參考圖1至圖13C論述此等及其他實施例；然而，熟習此項技術者將容易地瞭解，本文中關於此等圖式給定之詳細描述僅出於解釋性目的，且不應將其視為限制性的。

現參看圖1，說明一例示性交易網路100。例示性交易網路100包括一或多個用戶端器件102、一或多個商家器件(亦被稱作「銷售點」(POS)) 104及一或多個後端伺服器106。一般熟習此項技術者將容易地瞭解，前述交易網路100僅僅說明可能之網路佈局及功能的較寬陣列。此外，應認識到，各種實施可組合及/或進一步劃分圖1中所說明之各種實體。

當用戶端器件102以密碼編譯方式加密交易資訊並將其發送至商家器件104時，執行一交易。在一實例中，用戶端器件102可包括經組態以藉由(例如)刷過適當讀取器(諸如，近場通信(NFC)等)、視覺檢查來自圖形使用者介面(GUI)的交易識別符(例如，條碼、編號等)等而執行與商家器件104的交易之一虛擬「錢包」。在另一實例中，用戶端器件102可包括一全球定位系統(GPS)接收器，或用於向商家器件104 (例如，收銀機、行動平板電腦等)警告存在用戶端器件102之其他位置資訊(例如，WiFi存在等)，且進行對用戶端器件102之使用者的後續確認(例如，諸如其面部之照片的生物測定)，以便授權對已知使用者帳戶計費。交易資訊可包括如下各者之組合：(i)一別名、(ii)一遞增計數器、(iii)一隨機數、(iv)一商家識別符、(v)其他交易誤符(errata)(例如，交易量、時間戳記、位置戳記等)。

商家器件104將受保護交易資訊提供至後端伺服器106。其後，後端伺服器106可解密受保護交易資訊、驗證交易，並適當地處理交易。舉例而言，將一別名值映射至一信用卡編號，且若經加密資訊係正確的，則後端伺服器106利用映射至該別名值之信用卡編號而處理該交易。否則，若交易資訊遭損毀或表現為有詐騙性，則拒絕該交易。

在例示性交易網路100內，應用於交易資訊之密碼編譯保護使使用者之有價值資訊免於受到任何惡意方及/或商家侵害。具體而言，

即使惡意方將嘗試攔截交易資訊或商家器件104已被破壞(例如，藉由病毒等)，密碼編譯保護仍可幫助防止稍後以詐騙方式再次進行交易。因此，為了最大化使用者保護，實體地將密碼編譯元件保護於安置於用戶端器件102中之安全元件內，該器件可包括一安全處理器、一安全檔案系統及操作記憶體。然而，一般熟習此項技術者將認識到，難以保持儲存於用戶端器件內之密碼編譯材料的安全性。舉例而言，一種此問題為初始組態、配置及維護。用戶端器件由器件製造商(其可係非可信任的)製造。又，某些商業模型可取決於第三方參與者(其可係非可信任的)之市場。

理想地，用於散發密碼編譯材料之解決方案應可在較大之散發網路上擴充。此外，散發方案必須使密碼編譯材料(憑證)免受任何中間實體(例如，器件製造商、第三方仲介等)侵害。在一些實施例中，密碼編譯材料應係唯一的(亦即，單一資產執行個體一次僅可在單一安全元件中使用)。最後，解決方案應最小化對即時互動之要求。

現參看圖2，說明一例示性佈建系統200。如所展示，佈建系統200包括：用戶端器件300、資產代理400、資產仲介500及資產鎖櫃600。如先前所描述，在VME操作之內容脈絡內，可將VME安全性進一步再分成包括如下各者之等級：等級1 (L1)、等級2 (L2)及等級3 (L3)。每一等級可由佈建系統200之元件促進。

資產鎖櫃600可用於實行根據等級1 (L1)安全性的VME安全性。如本文中所使用，等級1安全性大體上係指(且並非限制性地)經組態以保護VME內所含有之秘密及/或密碼編譯材料(例如，安全密鑰、密碼編譯材料、使用者歷史等)的安全機制。此外，術語「安全性」大體上係指對資料及/或軟體的保護。舉例而言，密碼編譯安全性使與VME相關聯之資料及/或軟體免於被未授權活動及/或惡意第三方竊取、誤用、損毀、公開及/或竄改。

資產代理400可用於實行根據等級2 (L2)安全性的VME安全性。如本文中所使用，等級2安全性大體上係指(且並非限制性地)用於防止無意中及/或惡意再製(clone) VME之安全機制(強制保留(conservation enforcement))。此外，如本文中所使用之術語「保留」係指不能平凡地增加或減少之元件(實體抑或虛擬)。舉例而言，在正常操作期間不能複製或複寫所保留VME。另外，如本文中所使用，如應用於元件(實體抑或虛擬)之術語「唯一性」係指該元件為具有特定性質及/或特性之唯一元件的性質。舉例而言，唯一之VME不能具有重複之VME。

資產仲介500可用於實行根據等級3 (L3)安全性的VME安全性。如本文中所使用，等級3安全性大體上係指(且並非限制性地)將VME安全地遞送至與預期使用者(例如，個人、企業、機器用戶端等)相關聯之器件(例如，用戶端器件、POS等)的安全機制。此外，如本文中所使用，術語「使用者授權」大體上係指指定使用者對資源之存取。在交易媒介(信用卡、轉帳卡、現金)流行的情況下，交易可需要實體地所有媒介；且由使用者保護該實體卡。舉例而言，當使用實體信用卡時，假定卡為使用者所有(且隱含地，由使用者授權)。在VME操作之內容脈絡內，使用者需要類似能力以用於授權VME傳送。詳言之，VME之「所有者」(以及佈建系統200)需要保證僅將VME傳送至一或多個器件。

出於下文中將明確說明之原因，每一安全等級皆與受限集合之能力/責任相關聯；因此，提供等級2安全性之器件可自由地執行與等級2相關聯之動作，但必須亦能夠提供等級1安全性以影響VME之等級1元件。舉例而言，資產代理(下文中較詳細地描述)防止複製VME；然而，資產代理未必具有改變VME內所含有之密碼編譯材料的能力，負責偵測損毀之密碼編譯材料的資產代理亦未必具有該能

力。

前述之VME安全等級定義僅僅係說明性的，且並不意欲限制本文中之描述。實際上，應瞭解，應將前述術語認為係相關技術內之「口語語言」，且鑒於相關工業及/或技術之初期演進，其可能發生改變。

應瞭解，軟體常常比硬體具有較多靈活性；例如，軟體易於進行複製、修改及散發。另外，可常常將軟體製成較便宜、較具功耗效率(power efficiency)，並實體地小於硬體等效物。然而，VME資料(例如，客戶財務資訊、資產仲介密碼編譯秘密等)之敏感本質要求特別考慮。預期為了使用者保護之利益，必須避免並不意欲之重複及/或毀壞VME。因此，VME操作應符合如下性質：(i)安全性、(ii)唯一性及(iii)保留性。

在一例示性實施例中，揭示使得能夠將VME遞送至安全元件之散發基礎建設。安全元件可安置於用戶端器件及/或商家器件中。此外，可靈活地分割及/或調適所揭示之基礎建設的各種功能，使得個別合作對象(例如，器件製造商、第三方零售商、客戶等)可代管基礎建設之部分；可針對個別合作對象之需要最佳化此分段式解決方案。再此外，例示性實施例可提供操作冗餘。

現參看圖3A，呈現一例示性用戶端器件300。例示性用戶端器件300包括：用戶端商家介面302、處理器子系統304、非暫時性電腦可讀媒體(記憶體子系統) 306及安全元件308。在一些變化形式中，安全元件308進一步包括安全處理器308A及安全非暫時性電腦可讀媒體(安全記憶體) 308B。如本文所使用，術語「用戶端器件」包括(但不限於)經組態以交易及/或管理使用者之VME中之一或多者的器件。用戶端器件之共用實例尤其為具有無線功能之蜂巢式電話、智慧型電話(諸如，iPhone™)、具有無線功能之個人電腦(PC)、諸如手持式電腦

之行動器件、個人數位助理(PDA)、個人媒體器件(PMD)、無線平板電腦(諸如，iPad™)、所謂的「平板手機」或前述各者之任何組合。

處理器子系統304可包括數位信號處理器、微處理器、場可程式化閘陣列中之一或多者，或安裝於一或多個基板上之複數個處理組件。處理器子系統304亦可包括內部快取記憶體。處理器子系統304與記憶體子系統306通信，記憶體子系統306包括記憶體，該記憶體可(例如)包括靜態隨機存取記憶體(SRAM)、快閃記憶體及/或同步動態隨機存取記憶體(SDRAM)組件。如在此項領域中所熟知，記憶體子系統306可實施直接記憶體存取(DMA)型硬體中之一或多者，以便促進資料存取。例示性實施例之記憶體子系統306含有可由處理器子系統304執行之電腦可執行指令。

在一例示性實施例中，用戶端器件300包含一或多個介面，例如，適於連接至商家器件之用戶端商家介面302。用戶端商家介面302可為無線介面，或替代地為實體介面(有線)。無線介面可包括具有至多若干公分之操作範圍的「觸摸」或「碰觸」型介面(例如，射頻識別(RFID)、NFC等，諸如遵守國際標準化組織(ISO)標準14443A/B之彼等，該標準之全文以引用的方式併入本文中)，至較強大之無線介面，諸如，全球行動通信系統(GSM)、分碼多重存取(CDMA)、通用行動電信系統(UMTS)、長期演進(LTE)/LTE進階、微波存取全球互通(WiMAX)、WiFi、藍芽、無線通用串列匯流排(USB)等。實體介面之共用實例包括(例如) USB (例如，USB 2.0、USB 3.0)、FireWire、Thunderbolt等。此外，應進一步瞭解，某些器件可具有「卡」型外觀尺寸，諸如，用戶識別模組(SIM)卡或信用卡等。此等「卡」器件可為支付讀取器之現存生態系統提供回溯相容性，同時仍支援本文中所描述之經改良功能性。

在一些實施例中，用戶端器件300可另外包括其他組件，諸如，

包括任何數目之熟知I/O的使用者介面子系統，I/O包括(但不限於)小鍵盤、觸控螢幕(例如，多點觸控介面)、液晶顯示器(LCD)、背光、揚聲器及/或麥克風。應認識到，在某些應用中，使用者介面可係不必要的。舉例而言，卡型用戶端實施例可缺乏使用者介面。

在所說明之實施例中，用戶端器件300包括安全元件308。在此實施例中，安全元件308包括：執行安全記憶體308B中所儲存之軟體的安全處理器308A。所有其他組件(除了安全處理器308A)皆不可存取安全記憶體308B。此外，可進一步以物理方式硬化安全元件308以防止發生竄改(例如，封入樹脂中)。

安全元件308能夠接收、傳送及儲存一或多個VME。在一實施例中，安全元件308儲存與使用者相關聯之陣列VME或複數個VME (例如，信用「卡」、轉帳「卡」、預付帳號或卡編號、公交通行證、電影票憑單、優待券、「忠誠」程式元件等)。在一些變化形式中，每一VME可進一步與包括電腦可讀指令之較小檔案系統，及相關聯資料(例如，密碼密鑰、完整性密鑰等)相關聯。

檔案系統可支援額外特徵。舉例而言，檔案系統可包括用於(例如)安全之程式及資料(例如：用以保護與其他實體之通信的鑑認程式、授權程式及密碼編譯材料)、用於使用者管理之程式及資料(例如，帳戶平衡資訊、最近交易歷史等)等。一般熟習此項技術者將容易地瞭解，具有其相關聯檔案系統之VME係唯一且所保留之資料資產。

此外，在一實施例中，安全元件308維持所儲存之VME及其相關聯檔案系統之列表或顯示。顯示可包括關於所儲存之VME的當前狀況之資訊；此資訊可包括(例如)：使用可用性、有效性、帳戶資訊(例如，當前平衡等)及/或之前所經歷之誤差。可進一步將顯示連結或耦接至使用者介面，以便使得使用者能夠選擇用於使用之可用VME。

在一些狀況下，使用者可將一VME選擇為用於(例如)所有交易、與商家之所有交易、時間範圍內之所有交易等的預設(例如，預設信用卡)。

在一些變化形式中，安全元件308可具有一或多個相關聯器件密碼編譯密鑰。此等器件密鑰用於確保安全之交換。在一此變化形式中，密碼編譯密鑰為用於加密傳訊交易之不對稱公用/專用密鑰對。可在不破壞專用密鑰之完整性的情況下自由地散發公用密鑰。舉例而言，可基於瑞斯特(Rivest)、沙米爾(Shamir)及艾德曼(Adleman)(RSA)演算法將公用/專用密鑰指派給用戶端器件300 (或其內部產生該密鑰)；希望與用戶端器件300安全地通信之任何器件可用該公用密鑰。可僅由用戶端器件自身之專用密鑰(其安全地儲存於用戶端器件300中)解密藉由用戶端器件300之公用密鑰加密的訊息。在其他變化形式中，密碼編譯密鑰係對稱的(亦即，加密器件及解密器件具有相同之密鑰)。對稱之變化形式可提供減少之密碼編譯複雜性，但要求加密器件及解密器件兩者皆強有力地保護共用密鑰。

在其他變化形式中，安全元件308可具有用於驗證及/或發佈數位證書的密碼編譯密鑰。A數位證書可用於(例如)驗證(證書)發佈者的識別碼。舉例而言，安全元件308可將數位證書發佈至商家器件，使得商家器件可稍後(藉由擷取用戶端器件之經簽署證書)而證明已發生交易。類似地，安全元件308可驗證自商家器件所提供的證明該商家器件可信之數位證書。

在用戶商家交易(或用戶/第三方中間交易)期間，安全元件308與相關聯一或多個VME執行交易。簡單之實施例可為傳輸帳號、「代理」編號或其子集。在較複雜之變化形式中，傳輸可併有(例如)交易量、密碼編譯保護、認證資訊(例如，交易時間/日期及位置)、商家ID資訊等。

雖然本文中所描述之許多實施例係在財務交易之內容脈絡中描述，但非財務交易同樣合適。舉例而言，可根據使用遞增及/或遞減憑單、票證等之數個信用。在其他實例中，交易可為有效性檢查；例如，公交通行證歷時一時間範圍(例如，數天、數週、數月、數年等)有效，因此在彼時間範圍內進行任何數目之使用係有效的。類似地，某些類型之通行證可經受通行證歷時封鎖週期無效之(例如)「封鎖」日期。

在一些實施例中，於共用時間處在用戶端器件300與商家器件之間執行用戶商家(或其他)交易(亦即，用戶端器件300及商家器件兩者同時經歷交易)；例如，在NFC交易中，用戶端器件NFC介面安置成接近(「碰觸」)商家器件NFC介面，諸如將信號傳輸至用戶端器件300上之至少部分被動NFC IC的詢問機。

然而，應瞭解，在替代性情境中，可以時間轉換方式執行用戶商家交易。舉例而言，用戶端器件或商家器件可在第一時間處起始交易，而對應器件在稍後時間處認可交易。一旦該等器件兩者皆已認可交易，接著可完成該交易(例如，傳送適當基金等)。舉例而言，用戶及商家在(例如)不存在連接性之農貿市場處執行交易。稍後當商家器件連接至資產仲介時，起始該交易。隨後，用戶端器件同步其完成該交易之交易記錄。在一些狀況下，當產生未支付費用時，資產仲介可進一步通知用戶端器件。

現參看圖3B，呈現一例示性商家器件350。例示性商家器件350包括：商家用戶端介面352、處理器子系統354、非暫時性電腦可讀媒體(記憶體子系統) 356及網路介面358。如本文中所使用，術語「商家器件」包括(但不限於)經組態以交易及/或詢問對應於VME之伺服器(例如，後端伺服器106)(例如，以判定是否應允許交易等)的器件。將瞭解，術語「商家」之使用決不意欲將此定義限制為由購買或出售任

何事物之實體所有或所操作的器件。實情為，此術語較廣泛地意欲包括(但不限於)經組態或經致能以用於交易處理之裝置，無論彼交易係用於貨物、服務、虛擬考慮、獲得或儲放基金或信用、兌換優待券等。商家器件之共用實例包括(但不限於)：查詢一體機、櫃員機(例如，ATM)、「現金」收銀機、行動檢測讀取器(例如，RFID或基於條形碼)、行動無線平板電腦及甚至智慧型電話。此外，雖然商家器件在歷史上為專用型器件，但應瞭解，現在愈來愈多之客戶電子器件群體皆能夠無論在製造時間處，抑或之後由(例如)第三方或器件自身之使用者的佈建時間處，促進小企業問題(例如，具有無線功能之蜂巢式電話、智慧型電話、個人電腦(PC)、手持式電腦、PDA、個人媒體器件(PMD)、無線平板電腦、「平板手機」等)。

處理器子系統354可包括數位信號處理器、微處理器、場可程式化閘陣列中之一或多者，或安裝於一或多個基板上之複數個處理組件。處理器子系統354亦可包括內部快取記憶體。處理器子系統354與記憶體子系統356通信，記憶體子系統356包括記憶體，該記憶體可(例如)包含SRAM、快閃記憶體及/或SDRAM組件。如在此項領域中所熟知，記憶體子系統356可實施DMA型硬體中之一或多者，以便促進資料存取。例示性實施例之記憶體子系統356含有可由處理器子系統354執行之電腦可執行指令。

在一例示性實施例中，商家器件350包括適於連接至用戶端器件之一或多個介面，例如，商家用戶端介面352。商家用戶端介面352可為無線介面，或替代地為實體介面(有線)。無線介面可包括具有至多若干公分之操作範圍的「觸摸」型介面(例如，RFID、NFC等)，至較強大之無線介面，諸如GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、WiFi、藍芽、無線USB等或前述各者之任何組合。舉例而言，商家器件350可包括短程NFC介面，以及遠程WiFi介面，及甚至

WiMAX、衛星或蜂巢式介面。實體介面之共用實例包括(例如)USB、FireWire、Thunderbolt等。在一些變化形式中，可將商家用戶端介面352實施為讀卡器或智慧型卡座(例如，以維持與現存舊版卡等之相容性)。

在一些實施例中，商家器件350亦可包括其他組件，諸如包括任何數目之熟知I/O的使用者介面子系統，I/O包括(但不限於)小鍵盤、觸控螢幕(例如，多點觸控介面)、LCD、背光、揚聲器及/或麥克風。應認識到，在某些應用中，使用者介面可係不必要的。舉例而言，單一讀卡器之商家器件可缺乏使用者介面。

在所說明之實施例中，商家器件350包括經組態以向資產仲介安全地報告與一或多個VME之交易的網路介面358。在一些變化形式中，可另外將每一交易儲存於用於未來參考/簿記之安全檔案系統內。網路介面之共用實例包括(但不限於)：乙太網路、數位用戶線(DSL)、纜線、混合同軸光纖、無線區域網路(WLAN)、蜂巢式資料連接等。

在一些實施例中，商家器件350可具有相關聯器件密碼編譯密鑰或其他密碼編譯能力，諸如(非限制性地)高級加密標準(AES)/資料加密標準(DES)加密、網際網路協定安全(IPSec)、多媒體網際網路密鑰管理(MIKEY)、安全插座層(SSL)/安全運輸層(TLS)。此等器件密鑰(及/或其他特徵)可用於確保安全之交換。在一此變化形式中，密碼編譯密鑰為不對稱公用/專用密鑰對。在又一其他變化形式中，密碼編譯密鑰為對稱密鑰對。在其他變化形式中，商家器件350可具有用於驗證及/或發佈數位證書的密碼編譯密鑰。此外，NFC介面(在使用時)可具有施加至其上之加密，以便在傳輸期間加密敏感使用者或支付資訊。

在例示性用戶商家交易期間，商家器件350執行與相關聯一或多

個VME之交易。舉例而言，商家器件350可在交換貨物/服務時接收(或請求)用戶端器件之虛擬信用卡。所接收之資訊可另外併有(例如)待交易量、有效性檢查資訊、密碼編譯保護、認證資訊(例如，交易時間/日期及位置)、商家ID等。在其他實施例中，若交易係成功的，則商家器件350可將(例如)交易量、所使用之支付源、商家ID等報告回至用戶端器件。

在例示性商家器件-資產仲介交易期間，商家器件350向資產仲介報導交易。此情況可包括報告與用戶端器件之VME相關聯的資訊、用以收款/付款之商家帳戶等及交易量。作為回應，資產仲介認可已成功地(或不成功地)自用戶端器件之對應帳戶將該量傳送至商家器件之帳戶。

現參看圖4，呈現一例示性資產代理400。例示性資產代理400包括：用戶端器件介面402、處理器子系統404、非暫時性電腦可讀媒體(記憶體子系統) 406及網路介面408。如本文所使用，術語「資產代理」包括(但不限於)經組態以散發VME之實體。VME之共用實例包括(但不限於)：器件製造商、第三方經銷商等。

處理器子系統404可包括數位信號處理器、微處理器、場可程式化閘陣列中之一或多者，或安裝於一或多個基板上之複數個處理組件。處理器子系統404亦可包括內部快取記憶體。處理器子系統404與記憶體子系統406通信，記憶體子系統406包括記憶體，該記憶體可(例如)包括SRAM、快閃記憶體及/或SDRAM組件。如在此項領域中所熟知，記憶體子系統406可實施DMA型硬體中之一或多者，以便促進資料存取。例示性實施例之記憶體子系統406含有可由處理器子系統404執行之電腦可執行指令。

在一例示性實施例中，資產代理400包括適於連接至用戶端器件之一或多個介面，例如，用戶端器件介面402。用戶端器件介面402可

為無線介面，或替代地為實體介面(有線)。無線介面可包括(例如)GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、WiFi、藍芽、無線USB等。實體介面之共用實例包括(例如) USB、FireWire、Thunderbolt等。

在所說明之實施例中，資產代理400包括經組態以安全地報告與資產仲介散發一或多個VME之網路介面408。網路介面之共用實例包括(但不限於)：乙太網路、DSL、纜線、混合同軸光纖、WLAN、蜂巢式資料連接等。

在一些實施例中，資產代理400可具有相關聯器件密碼編譯密鑰。此等器件密鑰可用於確保安全之交換。在一此變化形式中，密碼編譯密鑰為不對稱公用/專用密鑰對。在又一其他變化形式中，密碼編譯密鑰為對稱密鑰對。在其他變化形式中，資產代理400可具有用於驗證及/或發佈數位證書的密碼編譯密鑰。

在一例示性實施例中，資產代理400具有並不優先與安全元件等相關聯(亦即，與具有安全元件之用戶端器件相關聯)的VME資料庫。如下文中較詳細地描述，可由資產代理根據L2安全層將VME與安全元件相關聯。L2安全層防止在遞送VME時「複製」VME。

舉例而言，在一實施中，用戶端器件請求「挑戰」並預載有數個「挑戰」；使用每一挑戰以驗證請求有效且係當前的(例如，並非重新執行先前請求)。更特定言之，每一挑戰為用於用戶端器件之安全元件的唯一有效挑戰之一次使用挑戰；亦即，一旦耗用挑戰，則對於安全元件而言，僅下一挑戰係有效的。隨著使用者簽署使用各種帳戶，由資產代理400佈建VME。當用戶端器件已用完預備挑戰時，使用者可指示用戶端器件請求新集合之挑戰。在一些變化形式中，經由安全鏈路(例如，經由服務查詢一體機、經由虛擬專用網路(VPN)連接上之個人電腦(PC)等)執行VME之傳送。

現參看圖5，呈現資產仲介500之一例示性帳戶伺服器501。例示性帳戶伺服器501包括：網路介面502、處理器子系統504、非暫時性電腦可讀媒體(記憶體子系統) 506及帳戶資料庫508。如本文中所使用，術語「資產仲介」包括(但不限於)經組態以適當地付款、收款及/或確認與VME相關聯之帳戶的系統及網路。該等系統可包括一或多個帳戶伺服器，例如，帳戶伺服器501。因此，應理解，對「資產仲介」之參考亦可係指資產仲介之一或多個帳戶伺服器，且反之亦然。

處理器子系統504可包括數位信號處理器、微處理器、場可程式化閘陣列中之一或多者，或安裝於一或多個基板上之複數個處理組件。處理器子系統504亦可包括內部快取記憶體。處理器子系統504與記憶體子系統506通信，記憶體子系統506包括記憶體，該記憶體可(例如)包括SRAM、快閃記憶體及/或SDRAM組件。如在此項領域中所熟知，記憶體子系統506可實施DMA型硬體中之一或多者，以便促進資料存取。例示性實施例之記憶體子系統506含有可由處理器子系統504執行之電腦可執行指令。

在一例示性實施例中，帳戶伺服器501包括適於建立至用戶端器件及商家器件之網路連接的網路介面502。網路介面之共用實例包括(但不限於)：乙太網路、DSL、纜線/混合同軸光纖、WLAN、無線都會區域網路(WMAN)、蜂巢式資料連接、毫米波等。

在一些實施例中，帳戶伺服器501可具有相關聯密碼編譯密鑰。此等密鑰可用於確保安全之傳訊交換。在一此變化形式中，密碼編譯密鑰為不對稱公用/專用密鑰對。在又一其他變化形式中，密碼編譯密鑰為對稱密鑰對。在其他變化形式中，帳戶伺服器501可具有用於(例如)驗證及/或發佈數位證書的密碼編譯密鑰。

在一例示性實施例中，帳戶伺服器501經組態以鑑認並授權客戶帳戶之VME。由帳戶伺服器501根據L3安全層相關聯VME。L3安全層

驗證客戶帳戶VME組合係可靠且經授權的(亦即，並非詐騙的或經誤用的)。

現參看圖6，呈現一例示性資產鎖櫃600。該例示性資產鎖櫃可包括：一網路介面602、一處理器子系統604、一非暫時性電腦可讀媒體(記憶體子系統) 606及一安全資料庫608。如本文所使用，術語「資產鎖櫃」包括(但不限於)經組態以儲存、加密並產生VME之器件。舉例而言，資產鎖櫃600可為一可信安全模組(TSM)。

處理器子系統604可包括數位信號處理器、微處理器、場可程式化閘陣列中之一或多者，或安裝於一或多個基板上之複數個處理組件。處理器子系統604亦可包括內部快取記憶體。處理器子系統604與記憶體子系統606通信，記憶體子系統606包括記憶體，該記憶體可(例如)包括SRAM、快閃記憶體及/或SDRAM組件。如在此項領域中所熟知，記憶體子系統606可實施DMA型硬體中之一或多者，以便促進資料存取。記憶體子系統606含有可由處理器子系統604執行之電腦可執行指令，但亦可使用其他類型之電腦化邏輯(例如，硬體及軟體/韌體之組合)。

在一例示性實施例中，資產鎖櫃600包括適於建立至一或多個帳戶伺服器之網路連接的一網路介面602。網路介面之常見實例包括(但不限於)：乙太網路、DSL、纜線、混合同軸光纖、WLAN、蜂巢式資料連接等。

在一些實施例中，資產鎖櫃600可具有相關聯密碼編譯密鑰。此等密鑰可用於確保安全之傳訊交換。在一此類變化形式中，密碼編譯密鑰為一不對稱公用/專用密鑰對。在另一其他變化形式中，密碼編譯密鑰為一對稱密鑰對。在其他變化形式中，資產鎖櫃600可具有用於驗證及/或發佈數位證書的密碼編譯密鑰。

資產鎖櫃600進一步經組態以提供及/或產生一或多個VME。在一

例示性實施例中，順應特定標準(例如，美國國家標準學會(ANSI)標準X4.13-1983 (其全文以引用的方式併入本文中))地產生VME，並將其儲存於安全資料庫608內。替代性地，可根據(例如)專屬格式或特殊使用格式建構VME。鑒於本發明之內容，一般熟習此項技術者將容易地瞭解過多可能格式。

在一例示性實施例中，資產鎖櫃600經組態以加密用戶端器件之安全元件的VME。資產鎖櫃600促進僅在加密時根據L1安全層傳送每一資產。L1安全層促進VME僅存在於資產鎖櫃600抑或用戶端器件之安全元件內的純文字中(未經加密)。

現參看圖7，揭示用於在系統內散發VME之一般化方法700的一實施例。在步驟702處，根據第一標準受信任關係保護一或多個VME之內容。在一例示性實施例中，第一受信任關係經組態以保護VME內所含有之秘密及/或密碼編譯材料(例如，安全密鑰、密碼編譯材料、使用者歷史等)。舉例而言，第一受信任關係基於經組態以根據唯一器件密鑰及承認證書而加密或解密VME之安全模組(實施於硬體或軟體內)。詳言之，安全模組經組態以加密VME，以用於遞送至順應第一受信任關係之所要目的地器件(例如，用戶端器件或商家器件)，或解密自順應第一受信任關係之源器件所接收的存取控制用戶端。在一例示性實施例中，當在器件之間傳送VME時，必須加密所有VME (亦即，不能以未經加密之形式將VME傳送至任何其他器件)。第一受信任關係等級下之每一器件給定有可用於安全地傳送VME之唯一器件密鑰及承認證書。

亦可實體地及/或在邏輯上保護第一標準受信任關係之各種實施。舉例而言，第一標準受信任關係可包括若強制性地打開/存取，則經組態以摧毀其自身之硬體安全模組(HSM)內的保護。更大體而言，第一標準受信任關係之例示性實施例最低限度地保護可信邊界。

可信邊界之共用實例包括實體邊界(例如，實體隔離等)及/或邏輯邊界(例如，經加密之通信等)兩者。

在步驟704處，根據第二標準受信任關係控制VME之複本的數目。在一例示性實施例中，第二受信任關係經組態以防止無意中及/或惡意地複製VME (強制保留)。舉例而言，可由經組態以加密其自身或另一器件之VME的安全模組管理第二標準受信任關係。類似地，安全模組可加密VME，使得可僅由另一特定器件(例如，基於不對稱密碼編譯密鑰)解碼VME。在一些實施例中，安全模組加密方案可基於不對稱密鑰對；或替代性地，安全模組加密方案可使用對稱密鑰對。

如先前所提到，公用/專用密鑰對係基於秘密專用密鑰及可公開公用密鑰。認為公用/專用密鑰方案係「不對稱的」，此係由於用於加密及解密之密鑰係不同的，且因此加密程式及解密程式並不共用相同密鑰。相反地，「對稱之」密鑰方案利用用於加密及解密兩者之相同密鑰(或略微經變換之密鑰)。RSA演算法為相關技術內常用的一種類型之公用/專用密鑰對密碼術，但將認識到，本文中所描述之實施例決不限於RSA演算法(或就此而言，限於彼不對稱密鑰對或對稱密鑰對)。

公用/專用密碼術方案可用於加密訊息及/或產生簽名。具體而言，可藉由專用密鑰加密訊息，並藉由公用密鑰解密訊息，藉此確保訊息在傳輸時未發生變更。類似地，可藉由公用密鑰驗證藉由專用密鑰所產生之簽名，從而確保產生簽名之實體係合法的。在上文之兩種使用中，專用密鑰保持隱蔽，且自由地散發公用密鑰。

在步驟706處，根據第三受信任關係將VME散發至目的地器件以用於使用。第三受信任關係要求實體鑑認及授權。較為直接地，第三受信任關係確保僅將VME傳輸至可鑑認其識別碼並經授權而使用

VME之實體。

歸因於散發模式之靈活性，設想出許多不同方案，且當提供本發明時一般熟習此項技術者將認識到該等不同方案。下文中較詳細地揭示說明適於根據本發明之各種態樣而操作的廣泛多種方案之若干VME散發方案。

現參看圖8，說明表示佈建交易之一例示性實施例的邏輯梯形圖。可由用戶端器件、資產仲介、資產代理及資產鎖櫃進行佈建交易。用戶端器件包括安全元件(SE)及應用程式處理器(AP)(例如，處理器子系統304)。SE可儲存包括根據本發明而促進交易之所謂的軟體層「堆疊」之軟體。每一軟體層負責與其對應同級軟體層協商之階層式功能集合。應進一步瞭解，在一些狀況下，AP可受到破壞(例如，「越獄」(jailbroken)等)；因此，信任關係僅存在於SE與對應邏輯層實體之間；亦即，AP並非可信任。

安全軟體協定包括L1層、L2層及L3層。L1安全性執行VME資料之加密及解密。L1操作限於安全的執行環境(例如，SE或TSM)。在L1內，VME資料可儲存於邏輯L1邊界內之純文字中(亦即，未經加密)；在邏輯L1邊界外部，VME資料經安全地加密。L2安全性防止VME資料發生重複。L2邊界確保L2邊界外部存在VME之唯一複本。L2邊界內可存在多個複本。此外，L2安全性可進一步將挑戰嵌入至經加密VME資料中。在安設VME之前，用戶端器件可將嵌入VME中之挑戰與儲存於用戶端器件上之挑戰進行比較，以驗證VME並非陳舊的(亦即，VME為當前且唯一之VME)。L3安全性負責建立信任、所有權及對所有VME之客戶的驗證。對於每一VME而言，SE可儲存用以指示與VME相關聯之所有權的資訊。

在一例示性實施例中，資產鎖櫃為經組態以產生VME之資料組件並將VME儲存於成批塊體中的TSM。資產鎖櫃根據L1安全性執行

VME操作，並確保僅傳輸經加密之VME (亦即，並不在資產鎖櫃外部以未經加密之形式傳輸VME)。為了將VME佈建至客戶，資產代理自資產鎖櫃接收經加密之VME，並基於需要儲存VME以佈建至用戶端器件。資產代理根據L2安全性執行VME操作，並確保僅將經加密VME之一複本佈建至用戶端器件。最後，資產仲介之例示性實施例根據L3安全性執行VME操作，並促進僅發生至具有經鑑認及授權之SE的用戶端器件的經加密VME之傳輸。一旦已將VME遞送至用戶端器件，資產仲介可使VME與相關聯於用戶端器件之帳戶，及/或與相關聯於用戶端器件之使用者的帳戶相關聯。

在一實施例中，儲存於用戶端器件中之軟體應用程式請求將新虛擬信用卡(VCC)佈建至使用者之帳戶，以用於使用。藉由AP執行軟體應用程式。在802處，AP向唯一地識別用戶端器件或SE之SE請求資訊。舉例而言，資訊可包括器件識別符。在804處，AP在請求新VCC時將器件識別符傳輸至資產仲介。資產仲介鑑認將VCC佈建至使用者之帳戶的請求。鑑認係基於器件識別符。在實施例之一態樣中，資產仲介藉由判定SE/用戶端器件與使用者帳戶相關聯而鑑認該請求。

SE可藉由數位簽名加密器件識別符，使得將器件識別符安全地自用戶端器件傳輸至資產仲介。一旦資產仲介已鑑認/授權新VCC，資產仲介將SE之數位簽名轉遞至資產代理。在806處，資產代理驗證SE之數位簽名，因此唯一地識別VCC之目的地SE。在807處，將任何額外VCC選項提供至用戶端器件。

除簡明以外，所謂的「挑戰」為用於使特定VME與SE相關聯之關鍵資源。具體而言；每一SE維持用以維持L2安全性的某些數目之挑戰。藉由驗證挑戰係有效的，SE可確定VME並非「陳舊之」VME (亦即，其為無效或以其他方式不可用之重複)。當接收到具有匹配之挑戰資料的VME時，SE刪除挑戰。考慮如下實施，SE產生(或給定

有)與資產代理共用之數個挑戰。隨後，資產代理可將當前挑戰嵌入已佈建給SE之VME中。當SE接收到VME時，SE可驗證所接收之VME含有適當挑戰且並不陳舊。

前述方案之一潛在缺點為可容易地藉由阻斷服務(DOS)攻擊而破壞固定數目之挑戰。在DOS攻擊中，持續觸發SE以產生挑戰直至耗盡其所有挑戰資源為止。為了此等目的，在處理將觸發SE耗用挑戰之請求之前，SE之例示性實施例另外執行與資產仲介/資產代理之作業階段訊號交換。另外，在資源耗盡且SE不能產生新挑戰之不大可能狀況中，SE可儲存特別指定以用於釋放另一挑戰集合的預備挑戰之單獨集合。在一些狀況下，SE亦可包括原始設備製造商(OEM)憑證，其中OEM可用以進一步控制挑戰操作。

在808處，AP請求SE提供用於與VCC相關聯之挑戰。一旦由SE提供，在810處將該挑戰發送至資產仲介，且接著在812處將其轉遞至資產代理。在814處，資產代理驗證挑戰，且接著將個人化資訊提供至資產鎖櫃。在816處，資產鎖櫃個人化用於SE之新VCC，並將相關聯VCC識別符提供至資產仲介。然後，在817處，資產仲介將VCC識別符提供至AP。一旦AP接收到VCC識別符，AP可在818處請求遞送VCC。此後，在820處，資產仲介可將VCC提供至用戶端器件之SE。

一般熟習此項技術者將認識到，在大型散發網路操作期間產生多個實際問題。具體而言，大型散發網路必須係可調整的以處置大訊務叢發(諸如，在用戶端器件之所謂的「上市日(launch day)」上可發生者)。用於減少總網路訊務之一方案需要(當可能時)推遲遞送VME。

參看圖9A及圖9B，揭示用於在系統內散發VME之一般化的方法900的一實施例。在預個人化操作期間，在裝運之前(亦即，當使用者在商店裏購買器件、在線預訂器件等時)，將VME預指派給具有SE之

所謂的「經預個人化」用戶端器件。在902處，在將用戶端器件遞送至使用者之前，掃描安置於與用戶端器件相關聯之箱子上的貼紙、標記或其他標誌。舉例而言，箱子可為其中封閉有用戶端器件之零售封裝。此貼紙含有唯一地識別用戶端器件，且可與VME相關聯之資訊(例如，器件識別符)。可藉由進行如下操作而預組態VME以用於用戶端器件：(例如)(i)在904處藉由特定於SE之密鑰(自貼紙所判定)加密VME (L1)，(ii)在906處將指定初始挑戰嵌入VME中(L2)，及(iii)在908處將VME與使用者之鑑認/授權資訊(在購買時間處所判定)相關聯(L3)。接著，在910處，將VME指派至唯一識別VME之識別符(例如，VME識別符)。此後，在912處，用戶端器件可使用VME識別符而請求VME。在914處，在接收到請求及VME識別符之後，可將呈其完全經組態狀態之VME遞送至用戶端器件。

前述方案有效地基於自用戶端器件(及/或與用戶端器件相關聯之箱子)所搜集之資訊，及購買時來自使用者之資訊而預組態VME。在傳輸器件時(例如，裝運、帶回家等)，根據最大努力式基底(亦即，在資源可用時發生組態)組態VME。此後，可自快取位置將VME順暢地載入用戶端器件中，而不要求即時訊務。為了最大化系統可靠性，亦可以冗餘方式將經預組態VME快取於多個地理位置中；亦即，橫跨不同地理位置之多個資料中心具有重複之VME (L2安全性提供初始挑戰方案，使得一旦擷取VME之第一複本，重複之VME變得陳舊)。

較為直接地，不同於習知之製造方案，用戶端器件之例示性實施例並未經製造及預程式化有VME。可「推遲」組態及遞送VME，直至已製造及/或配置用戶端器件之後。舉例而言，若可由用戶端器件支援多個VME，則當使用者已激活帳戶時，用戶端器件可具有稍後可經組態具有所選定之VME的一般軟體。在一些實施中，一般軟體可包括一般或預設VME。在此實施中，當使用者購買用戶端器件

時，可允許(或要求)使用者提供用於與預設VME一起使用之信用卡帳戶(或類似者)。此後，一旦激活用戶端器件，預設VME自動載入為激活序列之部分。

參看圖10A及圖10B，揭示用於在系統內散發VME之一般化方法1000的另一實施例。在此變化形式中，在1002處，在裝運(亦即，當使用者在商店處購買器件、在線預訂器件等)時為具有SE之用戶端器件分配來自VME集區之VME；亦即，特定VME並不與用戶端器件相關聯。此時，使用者可在1004處提供鑑認/授權資訊。一旦在1006處將用戶端器件遞送至使用者，由(例如)銷售點之商家、在家之使用者等輸入唯一識別用戶端器件之資訊。可自安置於與用戶端器件相關聯之箱子上的貼紙、標記或其他標誌搜集資訊。資訊亦可指示應為尚未經指派之用戶端器件分配VME。回應於在1008處接收到資訊，資產仲介、資產代理及資產仲介藉由進行如下操作而協調散發可用VME：在1010處藉由特定於SE之密鑰(自貼紙所判定)加密VME(L1)，在1012處將挑戰資料嵌入VME中(L2)，及在1014處將VME與使用者之鑑認/授權資訊(購買時間處所判定)相關聯(L3)。在1016處，將呈其完全經組態狀態之新產生並經加密VME遞送至用戶端器件。

前述方案有效地基於需要組態VME。此等實施允許資產仲介及/或資產代理智能地管理VME集區。因為並未將VME集區中之每一VME指派至特定用戶端器件(亦即，專用於特定使用)，且係基於需要而指派，所以資產仲介及/或資產代理並非必須追蹤尚未起作用之存量(例如，進行激活之前可購買並傳回之一些器件，此情況減少不必要的VME「變動」)。在VME為有限資源之狀況下，此情況可係有用的。一般熟習此項技術者將容易地瞭解帳號為有限資源(且因此由於稀缺而珍貴)；例如，ANSI標準X4.13-1983 (先前其全文以引用的方式併入本文中)為由大部分國家之信用卡系統所使用的帳戶編號系統。

根據信用卡編號之十六位(16)阿拉伯數字的ANSI標準X4.13-1983，僅彼等之子集表示實際帳號(例如，僅八個(8)阿拉伯數字可用於表示至多10百萬之唯一帳號)；其他阿拉伯數字歸於其他使用(例如，識別卡發佈者、提供「檢查」值、識別卡編號等)。

現參看圖11，揭示用於在系統內散發VME之一般化方法1100的另一實施例。在此實施例中，可完全推遲組態VME直至已發生初始交易之後。在系統與用戶端器件之間將發生多個交易(例如，定期交易)之狀況下，此實施例可係有用的。舉例而言，使用者可選擇購買(例如)多個電影通行證、公交通行證月票等。在1102處，使用者為系統提供支付資訊，例如，信用卡資訊。在1104處，將識別用戶端器件之資訊(例如，器件識別符)提供至系統。可根據前述實施例(例如，「預個人化」程序、由使用者輸入、由AP提供等)中之任一者提供器件識別符。通常可在1106處執行初始交易。同時，使用器件識別符、所提供之支付資訊及/或挑戰資料為用戶端器件組態VME；一旦已在1108處組態VME，則在1110處將其遞送至用戶端器件以用於後續使用。在一些狀況下，可基於何時準備、自動下載或手動下載之推送通知進行遞送。

現參看圖12，揭示用於在系統內散發VME之一般化方法1200的另一實施例。可藉由與具有SE之用戶端器件、資產代理及資產鎖櫃通信之資產仲介進行方法1200。在1202處，資產仲介自用戶端器件接收將VME佈建至使用者帳戶以用於使用之請求。帳戶可與用戶端器件之使用者相關聯(亦即，帳戶由使用者所有)。請求可包括唯一與用戶端器件相關聯之識別碼資訊，例如，器件識別符。在實施例之一態樣中，請求亦可包括發送識別帳戶之資訊。然後，在1204處資產仲介鑑認請求。資產仲介可藉由驗證由器件識別符所識別之用戶端器件與帳戶相關聯而鑑認該請求。資產仲介接著與資產代理及資產鎖櫃協

調，以根據本文中所描述之實施例為帳戶佈建VME，並為用戶端器件組態VME。在1206處，資產仲介自資產鎖櫃接收VME識別符。VME識別符識別為用戶端器件所組態之VME。資產仲介可接著在1208處將VME識別符發送至用戶端器件。用戶端器件可儲存VME識別符，並隨後在向資產仲介請求經組態VME時使用VME識別符。在於1210處自用戶端器件接收對VME之請求後，資產仲介可在1212處將經組態VME發送至用戶端器件。

現參看圖13A至圖13C，揭示用於在系統內散發VME之一般化方法1300的另一實施例。可由與可包括資產代理、資產仲介及/或資產鎖櫃之佈建系統通信的用戶端器件進行方法1300。用戶端器件可包括SE及AP。應注意，出於清楚及簡明之目的，以下描述在用戶端器件與資產仲介之間進行的方法1300。應理解，亦可在用戶端器件與佈建系統之一或多個實體(例如，資產代理、資產仲介)之間進行方法1300之步驟。

在1302處，用戶端器件接收指示希望將VME佈建至使用者之帳戶以用於使用之輸入。可由使用者使用用戶端器件處之I/O介面(例如，按鈕、小鍵盤、觸控螢幕、語音命令等)而鍵入該輸入。在1304處，用戶端器件可向SE請求識別碼資訊。識別碼資訊唯一地與用戶端器件相關聯，例如，器件識別符。可自SE獲得識別碼資訊。在替代性實施例中，可自用戶端器件外部之源獲得識別碼資訊。舉例而言，使用者可自用戶端器件之箱子上的貼紙獲得識別碼資訊，並使用用戶端器件之I/O器件而輸入識別碼資訊。

在自SE接收器件識別符之後，用戶端器件可在1306處發送將VME佈建至資產仲介之請求。除該請求以外，用戶端器件亦在1308處將器件識別符發送至資產仲介。在1310處，用戶端器件自資產仲介接收挑戰請求。挑戰可用於根據如本文中所描述之L2安全性而驗證

VME。回應於自資產仲介接收該請求，AP可在1312處向SE請求挑戰。在自SE接收挑戰之後，用戶端器件在1314處將挑戰發送至資產仲介。佈建系統可鑑認請求並為用戶端器件組態VME。然後，在1316處，用戶端器件可自資產仲介接收VME識別符。VME識別符可唯一地識別為用戶端器件所組態之VME。隨後，在1318處，用戶端器件可將對經組態VME之請求發送至資產仲介。除該請求以外，用戶端器件在1320處發送VME識別符。回應於接收到請求及VME識別符，資產仲介可在1322處將經組態VME遞送至用戶端器件。在1324處，SE可藉由驗證所接收之VME嵌入有有效挑戰資料，而驗證所接收之VME有效(亦即，所接收之VME並不陳舊)。

將認識到，雖然按照方法之步驟的特定序列描述某些特徵，但此等描述僅說明本文中所揭示之較寬方法，且視需要可由特定應用程式進行修改。在某些情況下，某些步驟可顯現為不必要或可選的。另外，可將某些步驟或功能性添加至所揭示之實施例，或置換執行兩個或兩個以上步驟之次序。認為所有此等變化皆涵蓋於本發明內並主張於本文中。

可分別或以任何組合使用所描述之實施例的各種態樣、實施例、實施或特徵。可藉由軟體、硬體或硬體與軟體之組合實施所描述之實施例的各種態樣。所描述之實施例亦可體現為電腦可讀媒體上之電腦可讀程式碼。電腦可讀媒體為可儲存資料之任何資料儲存器件，該資料此後可由電腦系統來讀取。電腦可讀媒體之實例包括唯讀記憶體、隨機存取記憶體、CD-ROM、HDD、DVD、磁帶及光學資料儲存器件。電腦可讀媒體亦可分散於網路耦接之電腦系統上，使得電腦可讀程式碼以分散型式儲存並執行。

出於解釋之目的，前述描述使用具體術語以提供對所描述之實施例的充分理解。然而，對熟習此項技術者而言，不要求具體細節以

便實踐所描述之實施例將係顯而易見的。因此，出於說明及描述之目的而呈現具體實施例之前述說明。該描述並不意欲為係詳盡的，或將所描述之實施例限制於所揭示之精確形式。一般熟習此項技術者將顯而易見，鑒於以上教示，許多修改及變化係可能的。

【符號說明】

100	交易網路
102	用戶端器件
104	商家器件
106	後端伺服器
200	佈建系統
300	用戶端器件
302	用戶端商家介面
304	處理器子系統
306	非暫時性電腦可讀媒體/記憶體子系統
308	安全元件(SE)
308A	安全處理器
308B	安全非暫時性電腦可讀媒體/安全記憶體
350	商家器件
352	商家用戶端介面
354	處理器子系統
356	記憶體子系統
358	網路介面
400	資產代理
402	用戶端器件介面
404	處理器子系統
406	非暫時性電腦可讀媒體/記憶體子系統

408	網路介面
500	資產仲介
501	帳戶伺服器
502	網路介面
504	處理器子系統
506	非暫時性電腦可讀媒體/記憶體子系統
508	帳戶資料庫
600	資產寄物櫃
602	網路介面
604	處理器子系統
606	非暫時性電腦可讀媒體/記憶體子系統
608	安全資料庫
700	用於在系統內散發VME之一般化方法
702	步驟
704	步驟
706	步驟
900	用於在系統內散發VME之一般化的方法
1000	用於在系統內散發VME之一般化的方法
1100	用於在系統內散發VME之一般化的方法
1200	用於在系統內散發VME之一般化的方法
1300	用於在系統內散發VME之一般化的方法
L1	等級
L2	等級
L3	等級

申請專利範圍

1. 一種供包含一或多個帳戶伺服器之一資產仲介將一資產散發至包括一安全元件之一用戶端器件的方法，該方法包含該資產仲介至少進行如下操作：

自該用戶端器件接收(i)將該資產佈建至一帳戶之一請求，及(ii)唯一地識別該用戶端器件之一器件識別符；

鑑認將該資產佈建至該帳戶之該請求；

自一資產鎖櫃接收一資產識別符，其中該資產識別符唯一地識別經指派至該用戶端器件的該資產；

將該資產識別符發送至該用戶端器件；

自該用戶端器件接收對該經指派資產之一請求；

自該用戶端器件接收該資產識別符；及

將該經指派資產發送至該用戶端器件。

2. 如請求項1之方法，其進一步包含該資產仲介進行如下操作：

在自該資產鎖櫃接收該資產識別符之前：

自該用戶端器件接收與該器件識別符相關聯之一數位簽名；及

將該數位簽名發送至一資產代理，其中由該資產代理驗證該經發送數位簽名。

3. 如請求項2之方法，其進一步包含該資產仲介進行如下操作：

在將該數位簽名發送至該資產代理之後：

自該用戶端器件接收一挑戰，其中由該安全元件產生該挑戰；及

將該挑戰發送至該資產代理，其中由該資產代理驗證該經發送挑戰。

4. 如請求項1之方法，其中鑑認將該資產佈建至該帳戶之該請求包含：驗證該器件識別符與該帳戶相關聯。

5. 如請求項1之方法，其進一步包含該資產仲介進行如下操作：

將該經指派資產與該用戶端器件或該器件識別符相關聯。

6. 如請求項1之方法，其進一步包含該資產仲介進行如下操作：

在將該經指派資產發送至該用戶端器件之後，基於該經指派資產之一價值自該帳戶扣款。

7. 一種供一或多個裝置將一資產散發至包括一安全元件之一用戶端器件的方法，每一裝置包含一記憶體及一處理器，該方法包含該一或多個裝置至少進行如下操作：

藉由用基於唯一地識別該用戶端器件之一器件識別符的一唯一密鑰加密該資產，及將挑戰資料嵌入該資產中而預組態該資產；

將該經預組態資產與一資產識別符相關聯；

自該用戶端器件接收一請求，該請求包括該資產識別符；及

回應於接收到該請求，將該經預組態資產遞送至該用戶端器件。

8. 如請求項7之方法，其中該資產包含一信用卡編號。

9. 如請求項7之方法，其進一步包含該一或多個裝置進行如下操作：

在預組態該資產之前，自該用戶端器件之一使用者接收帳戶資訊，該帳戶資訊識別一使用者帳戶。

10. 如請求項9之方法，其中當該使用者購買該用戶端器件時發生自該使用者接收帳戶資訊。

11. 如請求項9之方法，其中預組態該資產進一步包含：將該資產與該使用者帳戶相關聯。

12. 如請求項7之方法，其進一步包含該一或多個裝置進行如下操作：

在預組態該資產之前，將該資產識別符提供至該用戶端器件。

13. 如請求項7之方法，其進一步包含該一或多個裝置進行如下操作：

將該經預組態資產儲存於一第一地理位置處及與該第一地理位置分開之一第二地理位置處。

14. 如請求項13之方法，其中將該經預組態資產遞送至該用戶端器件包含自該第一地理位置或自該第二地理位置遞送該經預組態資產，且其中該用戶端器件經組態以基於嵌入於該所遞送經預組態資產中之該挑戰資料而驗證該所遞送經預組態資產。

15. 如請求項7之方法，其進一步包含該一或多個裝置進行如下操作：

在預組態該資產之前，自安置於與該用戶端器件相關聯之一箱子上的一標記或標誌獲得該器件識別符。

16. 一種經組態以向一遠端伺服器請求一資產之用戶端器件，該用戶端器件包含：

一應用程式處理器；

一儲存器件，其經組態以儲存當由該應用程式處理器執行時導致該用戶端器件進行如下操作之指令：

將佈建一資產至一帳戶的一請求傳輸至該遠端伺服器，

將唯一地識別該用戶端器件之一器件識別符傳輸至該遠端伺服器，其中該所傳輸器件識別符用於鑑認佈建該資產之該請求，

自該用戶端器件之一安全元件獲得一挑戰，及

將該挑戰傳輸至該遠端伺服器；且

該安全元件包含：

一安全處理器；及

一安全記憶體，其經組態以儲存當由該安全處理器執行時導致該安全元件進行如下操作之指令：

自該遠端伺服器接收該資產，該所接收資產包括基於經傳輸至該遠端伺服器之該挑戰的挑戰資料，及

基於該挑戰資料驗證該所接收資產。

17. 如請求項16之用戶端器件，其中該安全記憶體進一步經組態以儲存當由該安全處理器執行時導致該安全元件進行如下操作之指令：在驗證該所接收資產之後，自該安全元件刪除該挑戰。

18. 如請求項17之用戶端器件，其中該安全記憶體進一步經組態以儲存當由該安全處理器執行時導致該安全元件進行如下操作之指令：

產生一新挑戰，及

將該新挑戰儲存於該安全元件上。

19. 如請求項16之用戶端器件，其中該儲存器件進一步經組態以儲存當由該應用程式處理器執行時導致該用戶端器件進行如下操作之指令：

自該遠端伺服器接收一資產識別符，及

將該所接收資產識別符發送回至該遠端伺服器。

20. 如請求項16之用戶端器件，其中該儲存器件進一步經組態以儲存當由該應用程式處理器執行時導致該用戶端器件進行如下操作之指令：在將該器件識別符傳輸至該遠端伺服器之前，自該安全元件獲得該器件識別符。

圖式

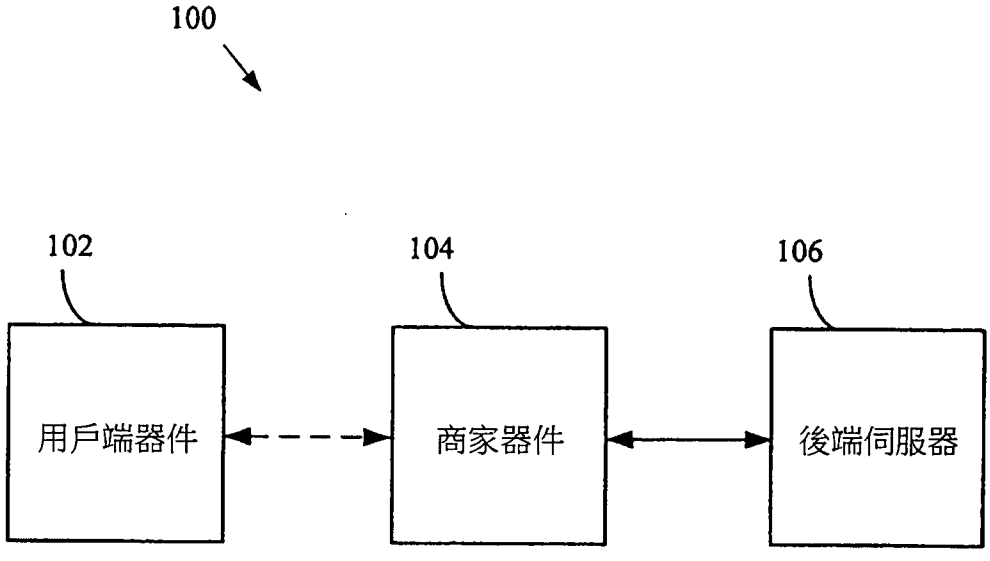

圖1

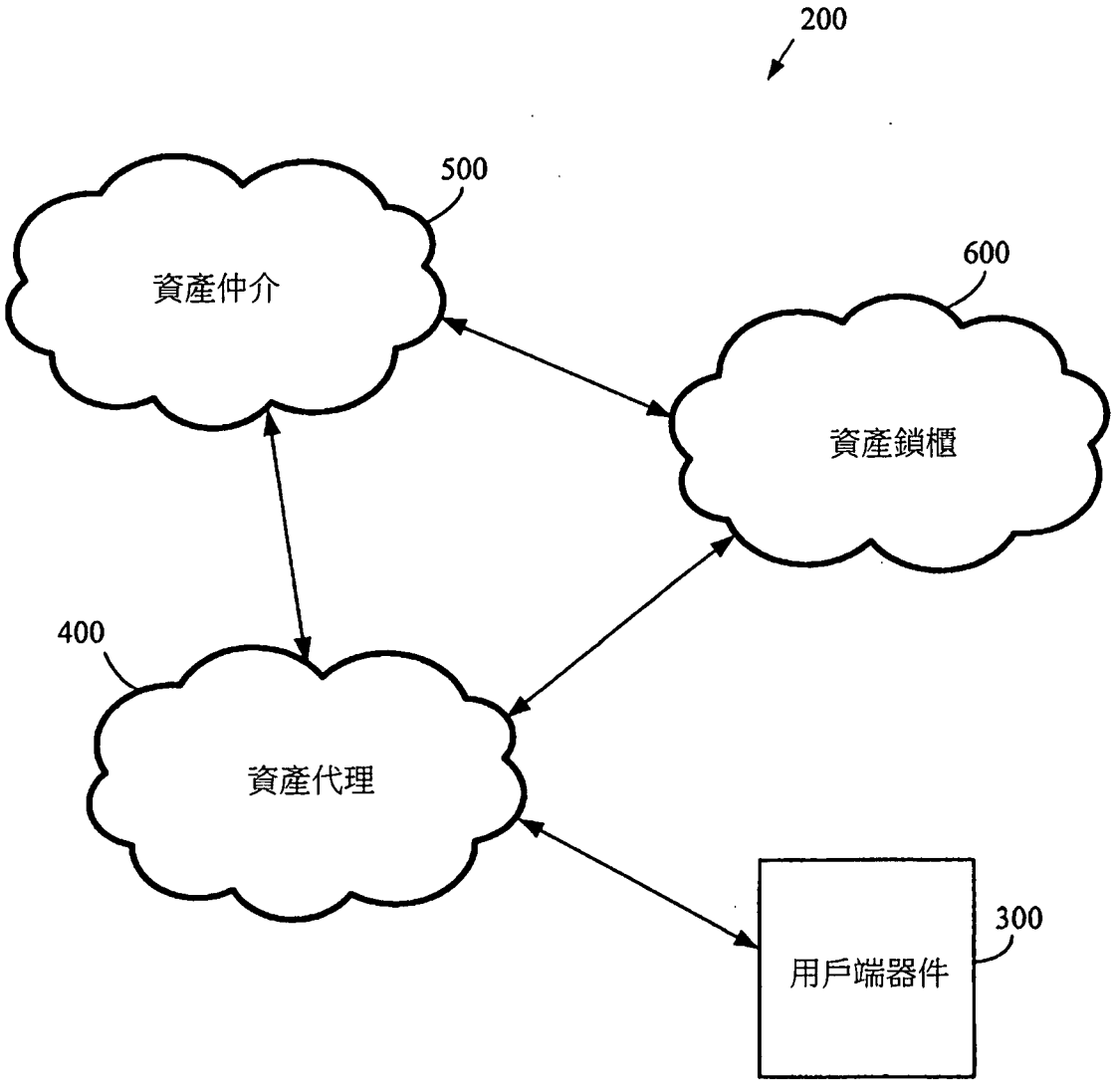

圖2

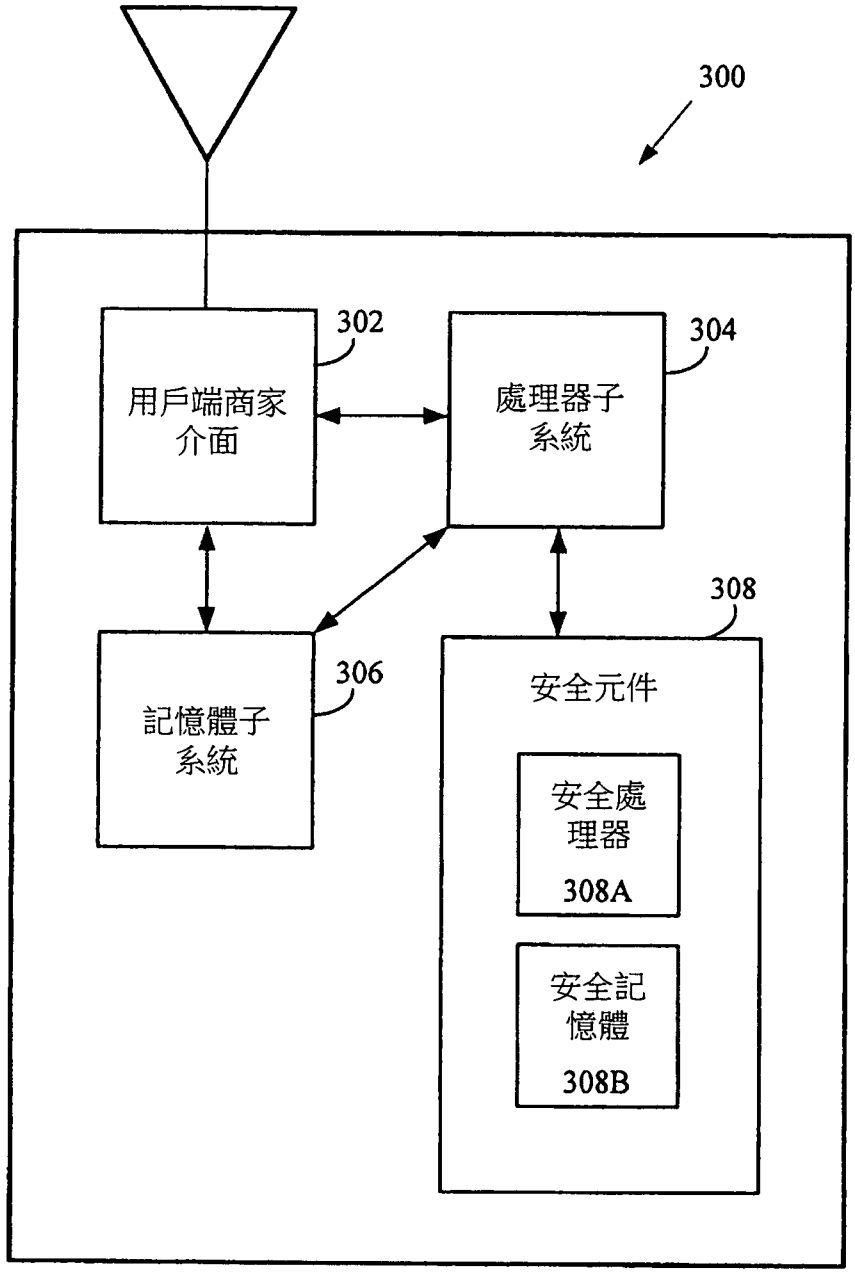
300
302
用戶端商家介面
304
處理器子系統
306
記憶體子系統
308
安全元件
安全處理器
308A
安全記憶體
308B

圖3A

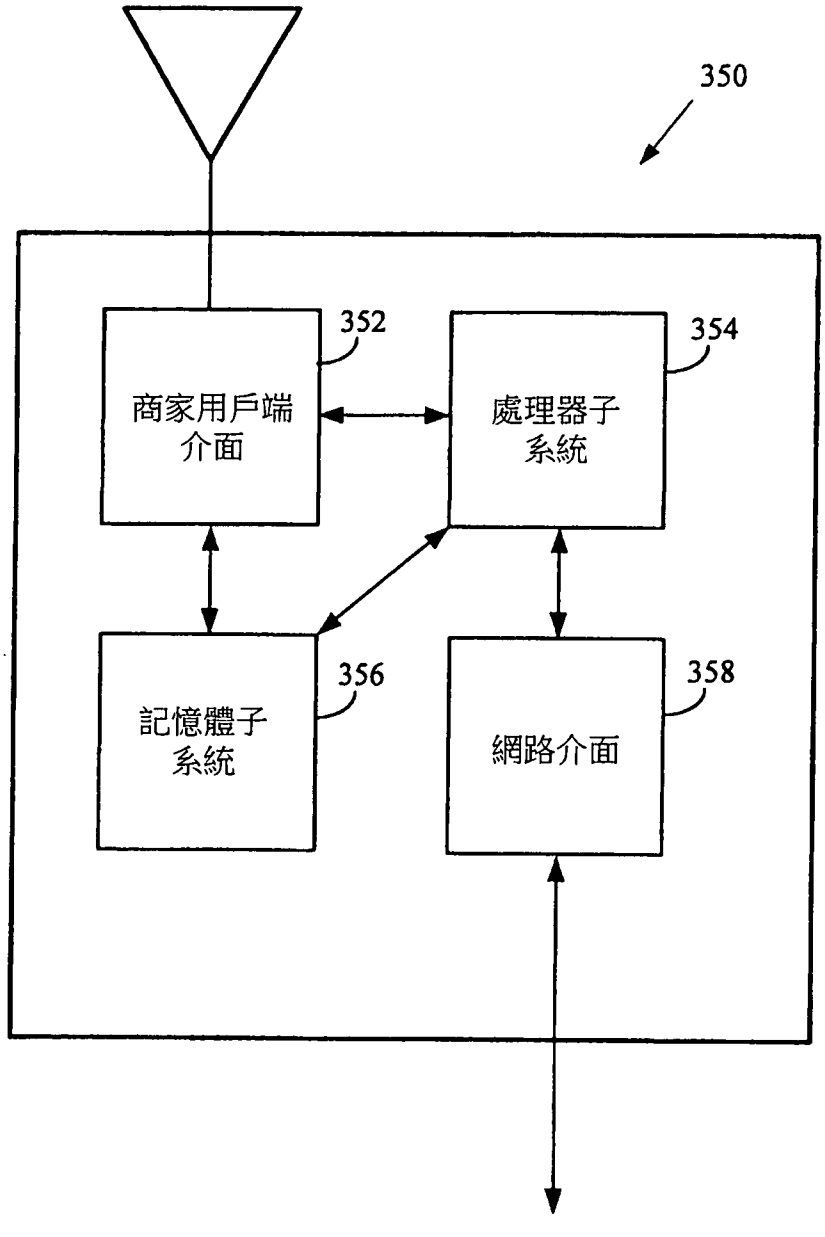

圖3B

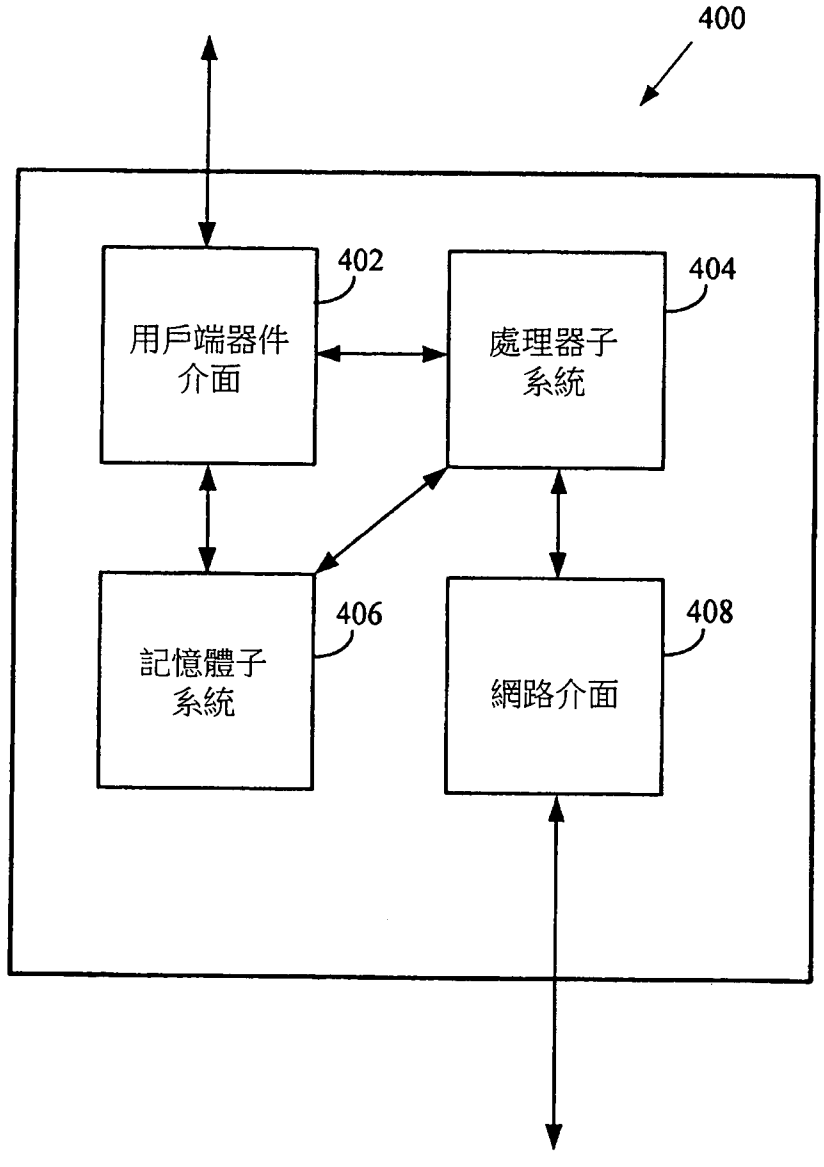

圖4

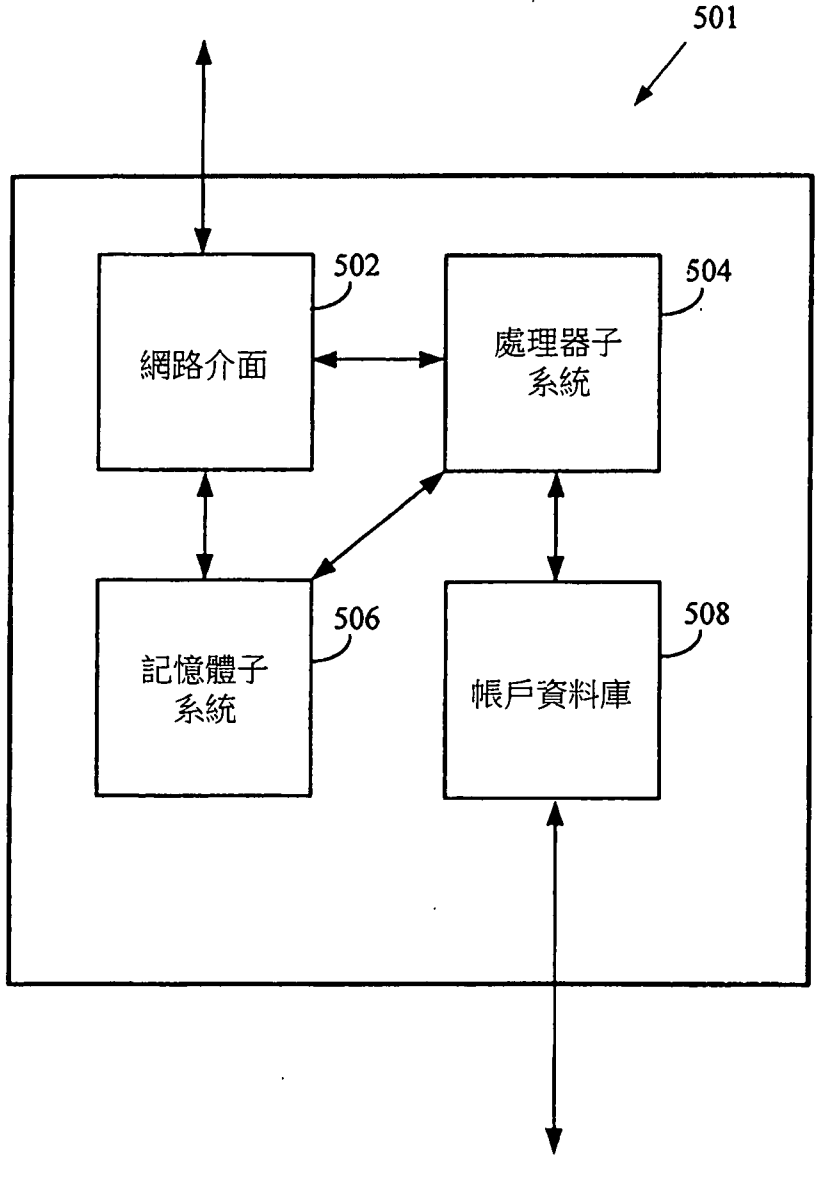

圖5

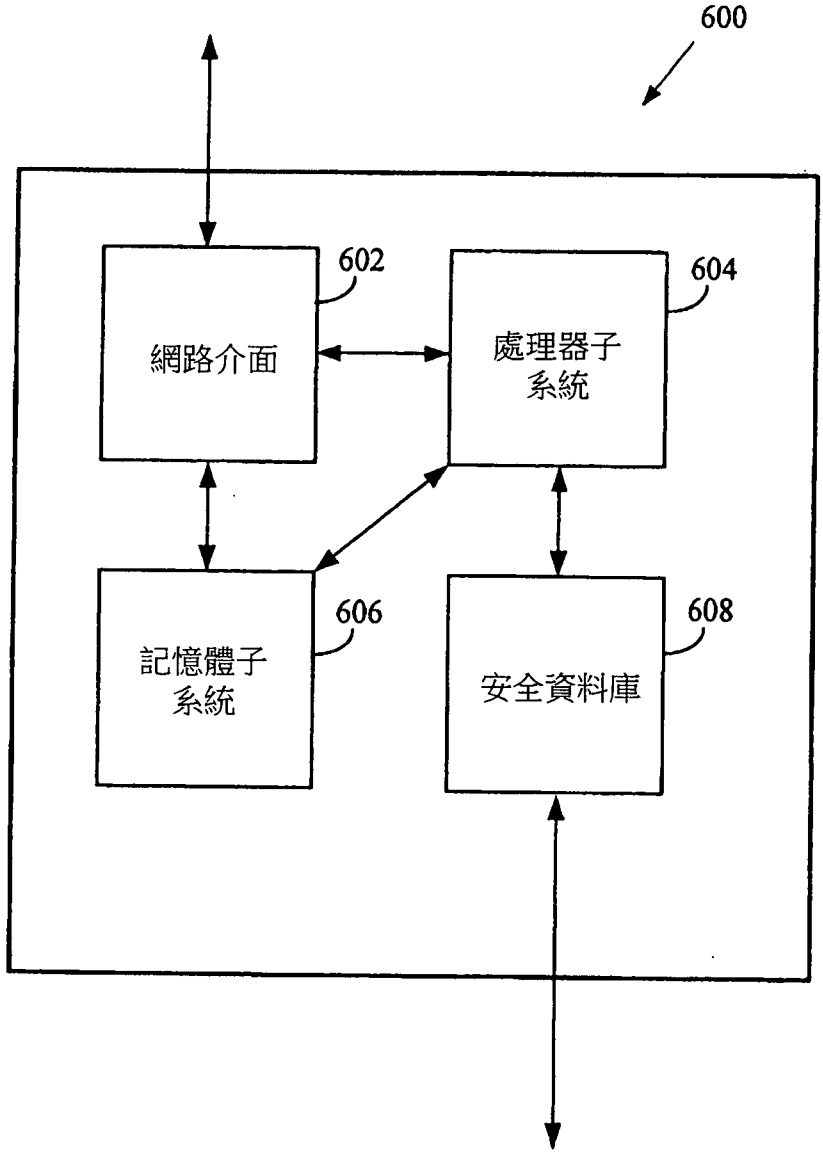

圖6

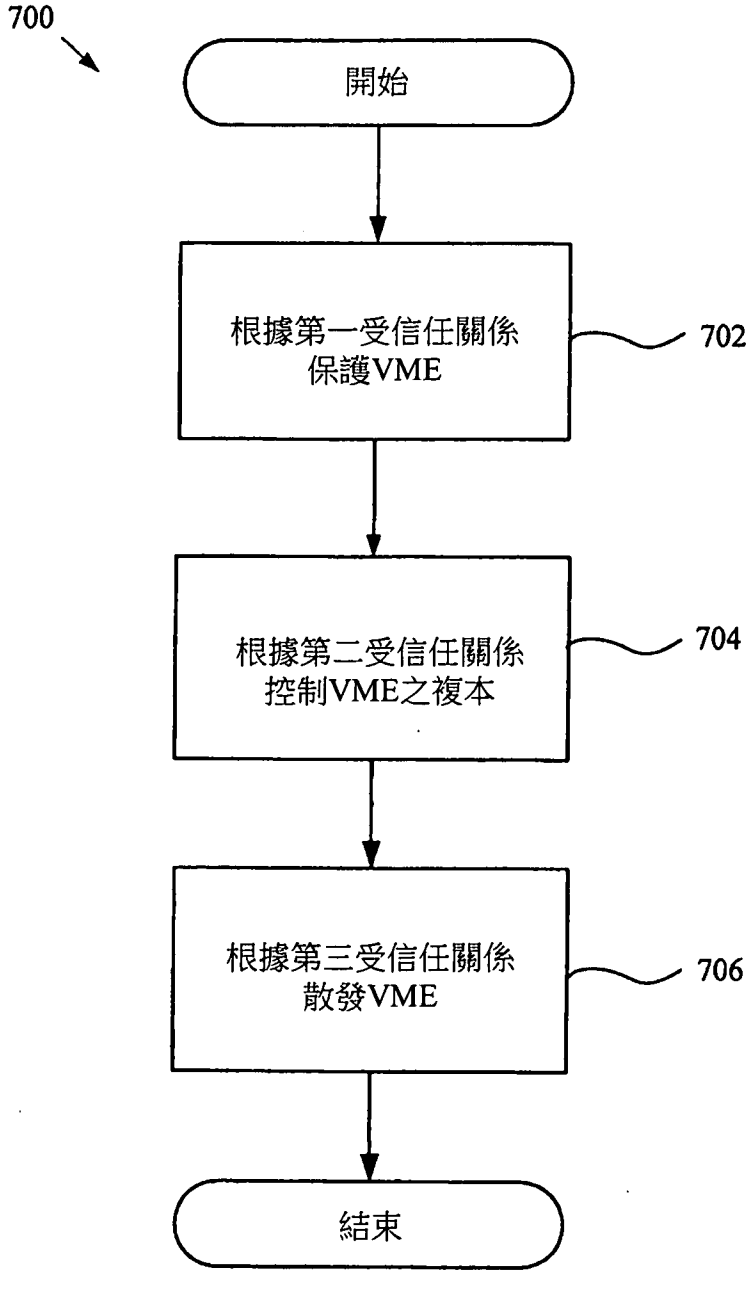
700
開始
根據第一受信任關係
保護VME
702
根據第二受信任關係
控制VME之複本
704
根據第三受信任關係
散發VME
706
結束

圖7

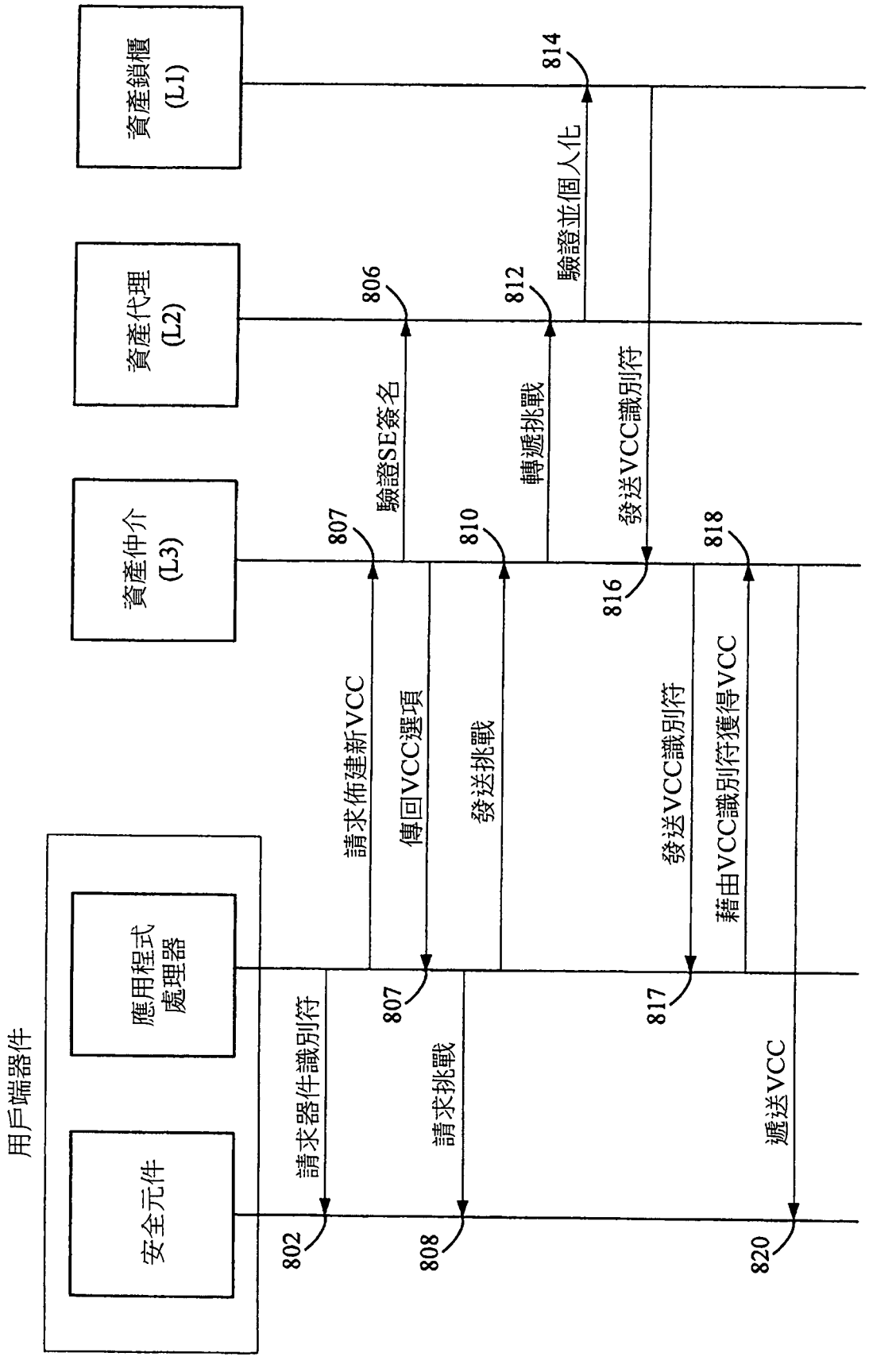
用戶端器件
安全元件
應用程式處理器
資產仲介 (L3)
資產代理 (L2)
資產鎖櫃 (L1)
請求器件識別符
802
請求佈建新VCC
807
傳回VCC選項
807
驗證SE簽名
806
發送挑戰
810
請求挑戰
808
轉遞挑戰
812
發送VCC識別符
816
驗證並個人化
814
發送VCC識別符
817
藉由VCC識別符獲得VCC
818
遞送VCC
820

圖8

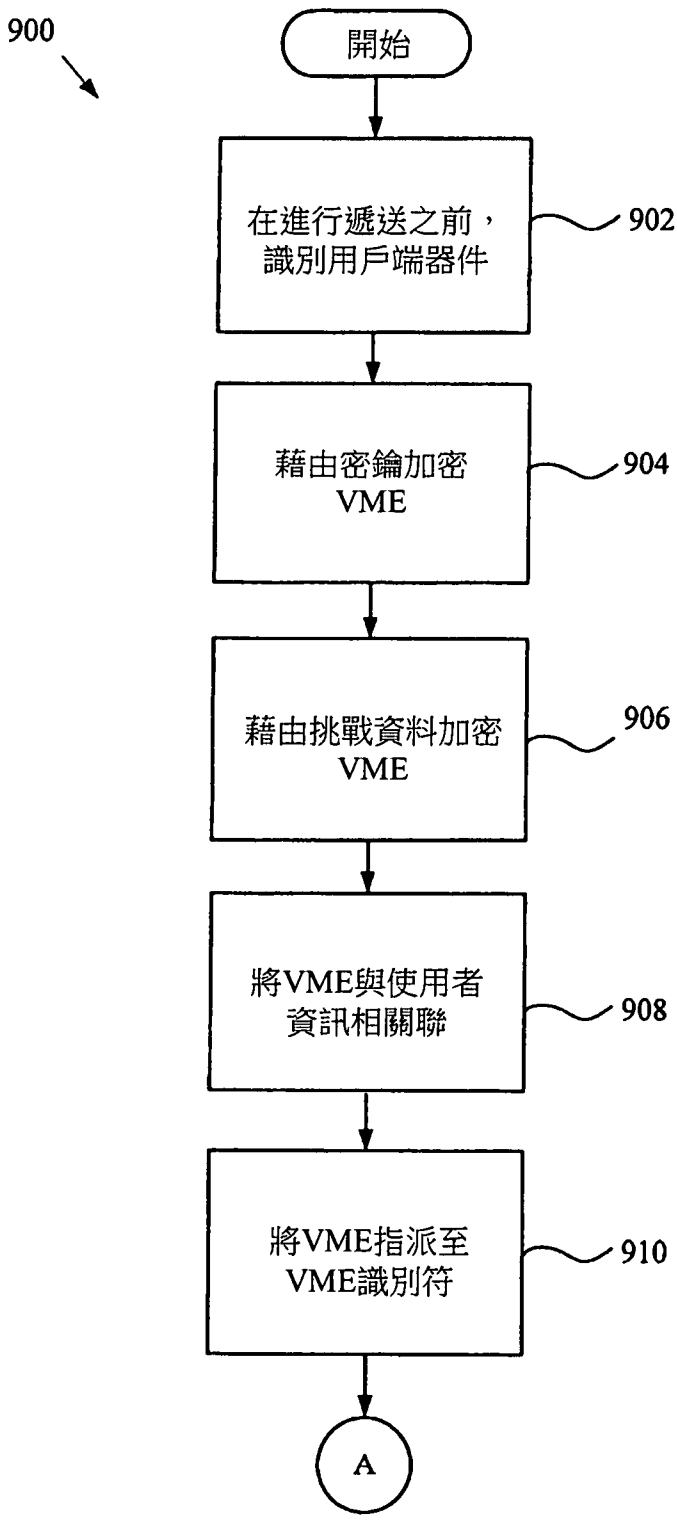
900
開始
在進行遞送之前，識別用戶端器件
902
藉由密鑰加密VME
904
藉由挑戰資料加密VME
906
將VME與使用者資訊相關聯
908
將VME指派至VME識別符
910
A

圖9A

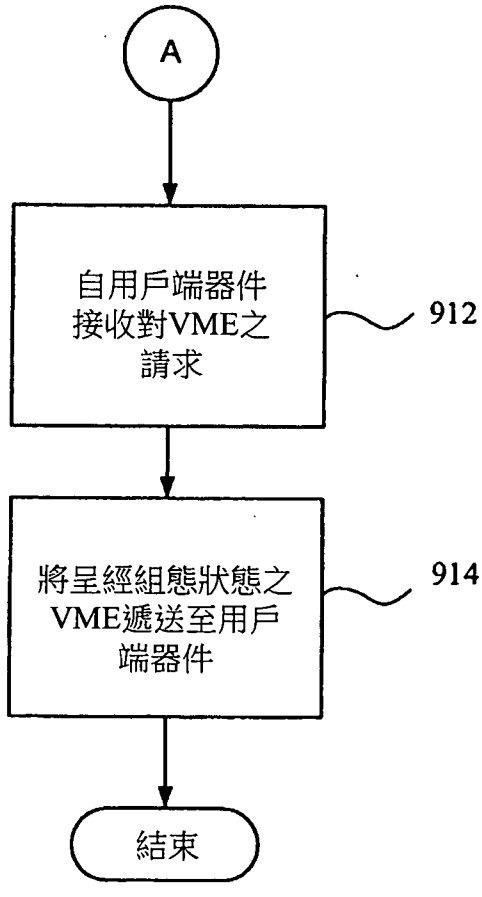

圖9B

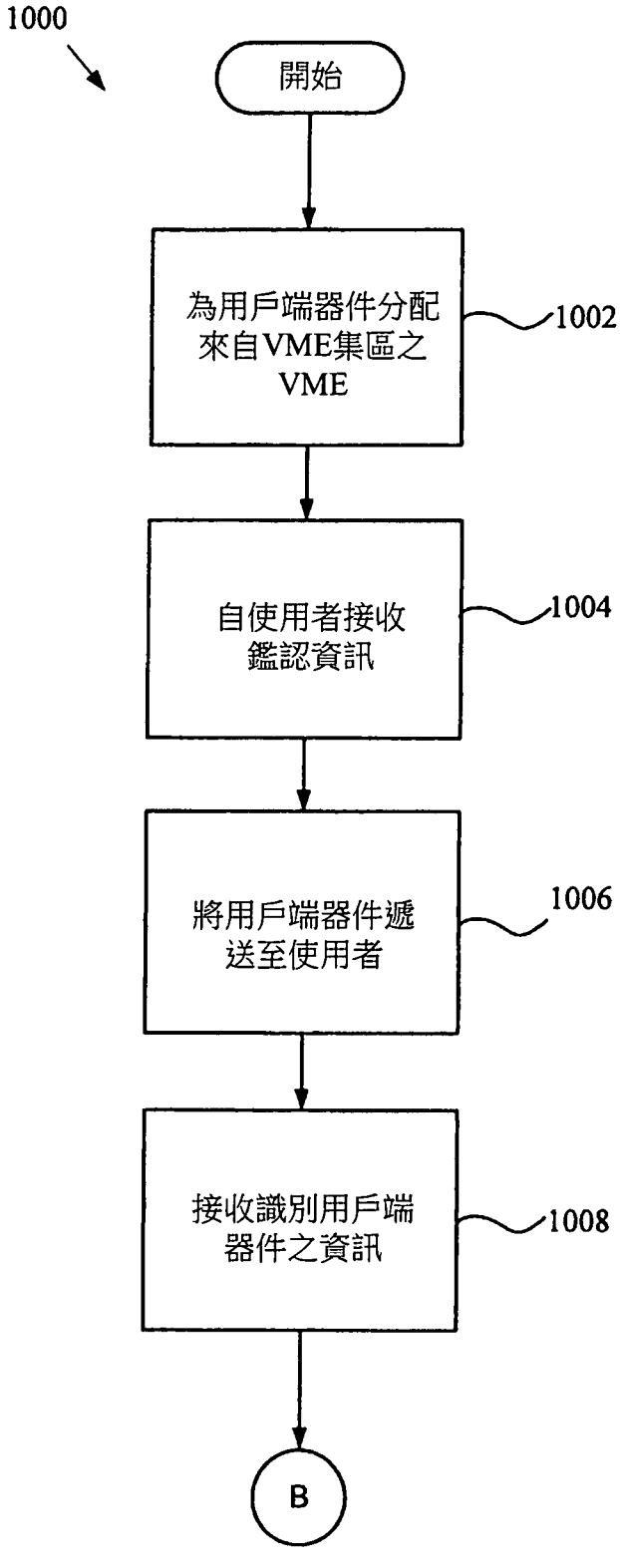
1000
開始
為用戶端器件分配來自VME集區之VME
1002
自使用者接收鑑認資訊
1004
將用戶端器件遞送至使用者
1006
接收識別用戶端器件之資訊
1008
B

圖10A

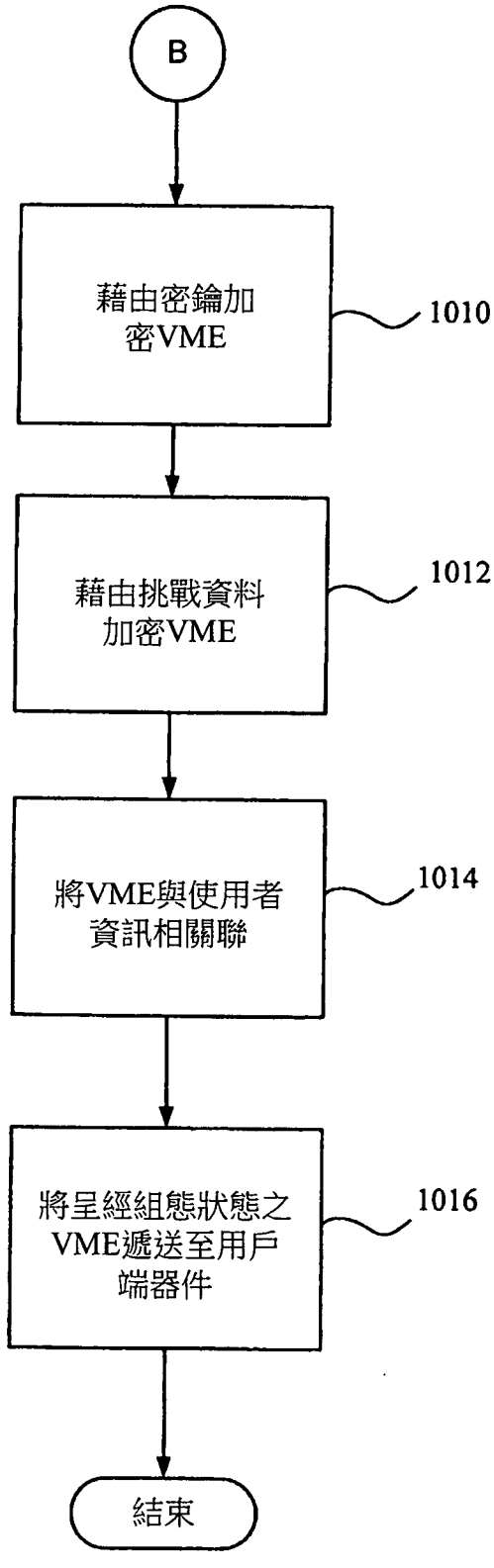
B
藉由密鑰加密VME
1010
藉由挑戰資料加密VME
1012
將VME與使用者資訊相關聯
1014
將呈經組態狀態之VME遞送至用戶端器件
1016
結束

圖10B

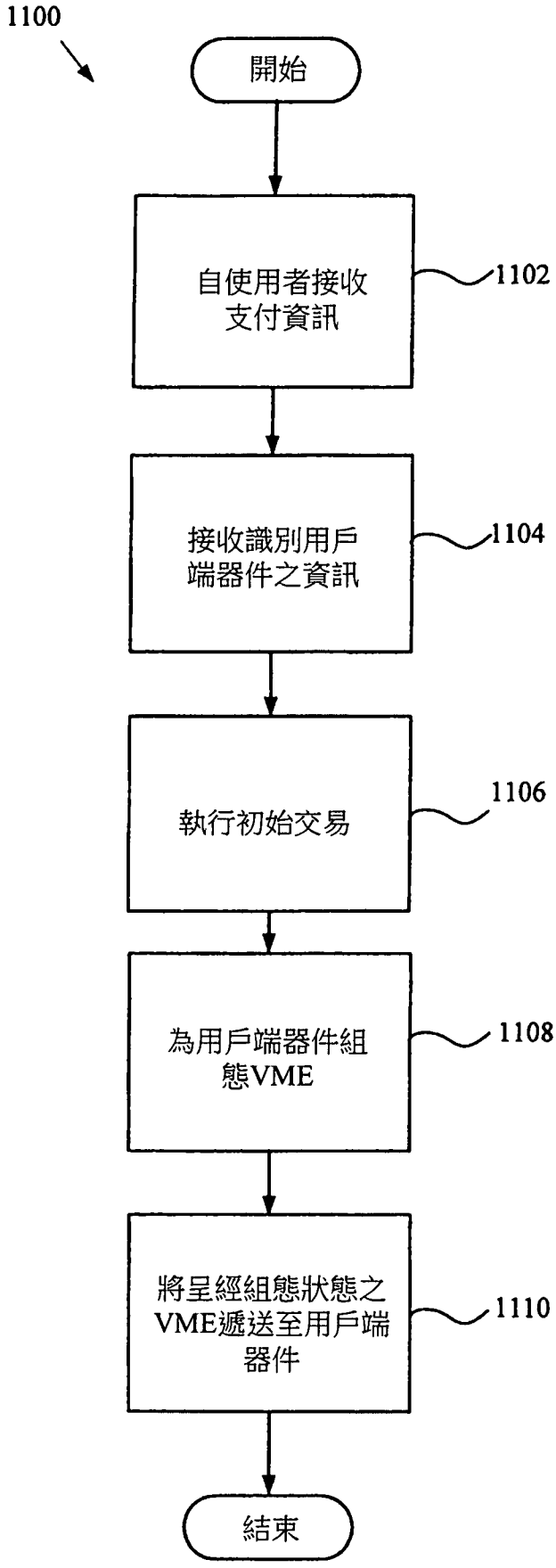
1100
開始
自使用者接收支付資訊
1102
接收識別用戶端器件之資訊
1104
執行初始交易
1106
為用戶端器件組態VME
1108
將呈經組態狀態之VME遞送至用戶端器件
1110
結束

圖11

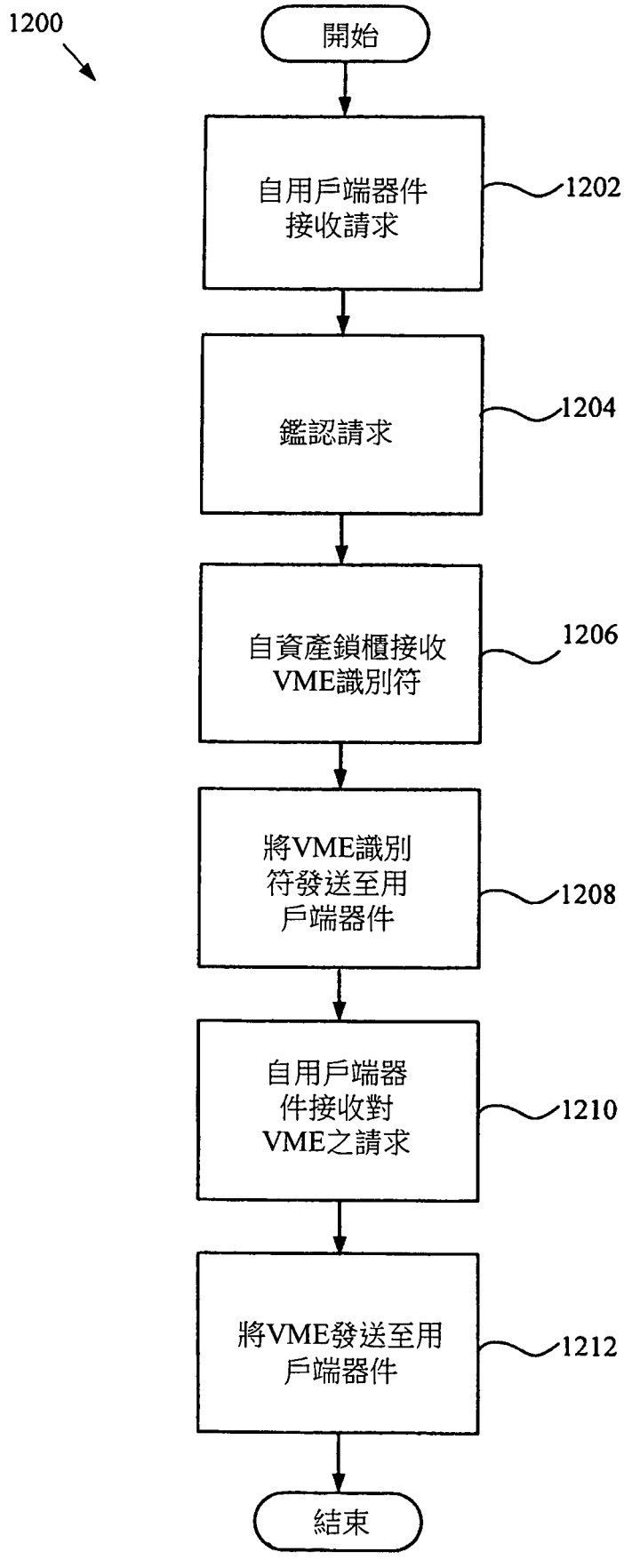
1200
開始
自用戶端器件接收請求
1202
鑑認請求
1204
自資產鎖櫃接收VME識別符
1206
將VME識別符發送至用戶端器件
1208
自用戶端器件接收對VME之請求
1210
將VME發送至用戶端器件
1212
結束

圖12

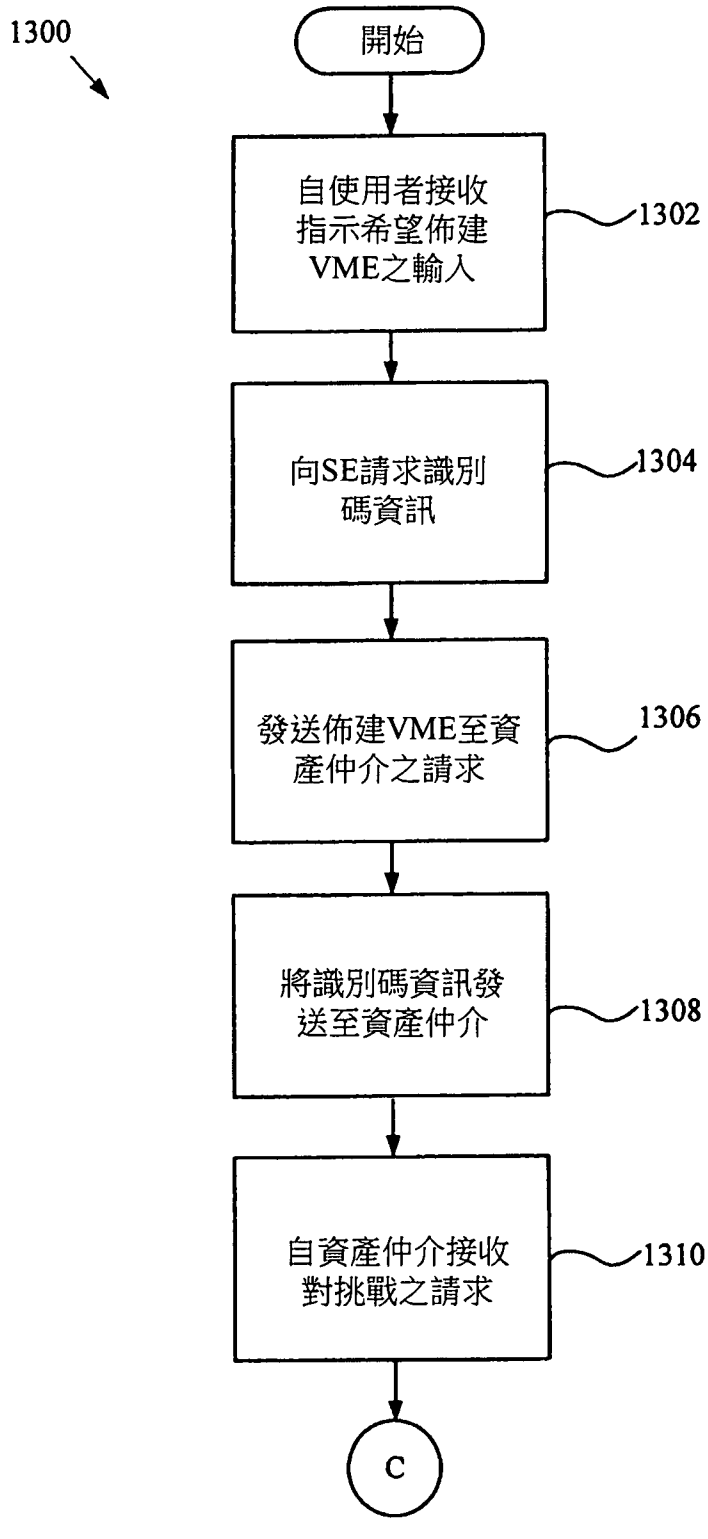
1300
開始
自使用者接收指示希望佈建VME之輸入
1302
向SE請求識別碼資訊
1304
發送佈建VME至資產仲介之請求
1306
將識別碼資訊發送至資產仲介
1308
自資產仲介接收對挑戰之請求
1310
C

圖13A

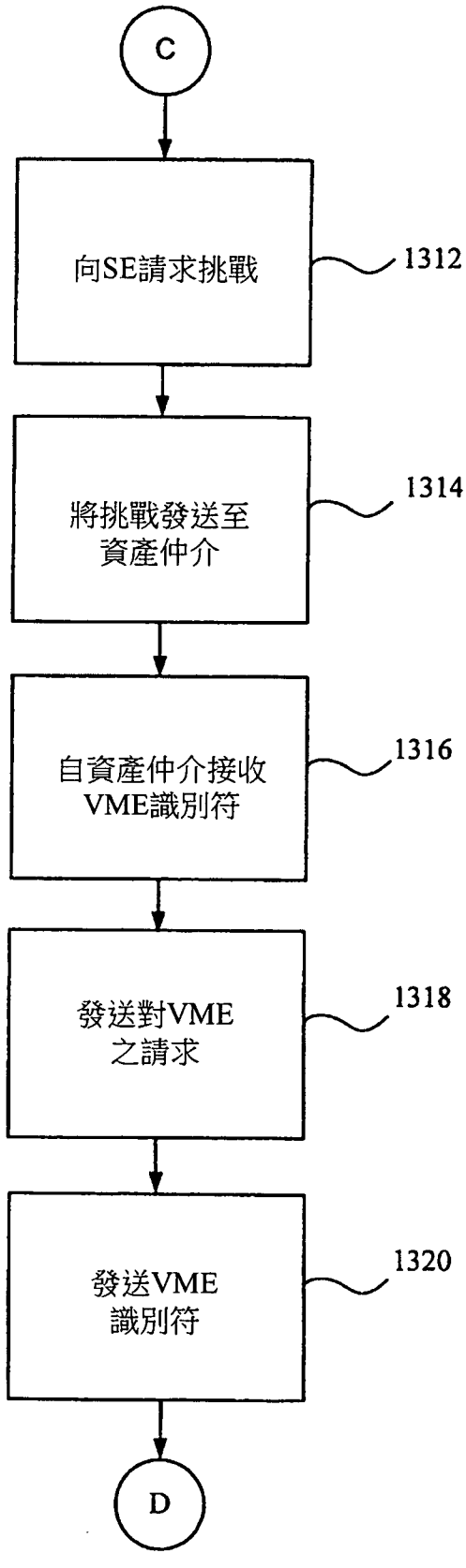
C
向SE請求挑戰
1312
將挑戰發送至
資產仲介
1314
自資產仲介接收
VME識別符
1316
發送對VME
之請求
1318
發送VME
識別符
1320
D

圖13B

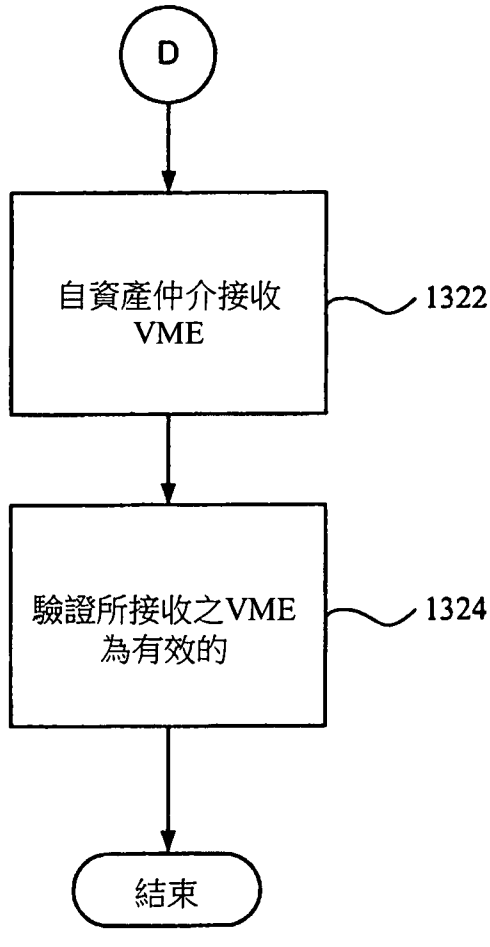

圖13C