200821931

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96138034

※ 申請日期：2007 年 10 月 11 日　　※IPC 分類：

G06F 9/44 (2006.01)

一、發明名稱：（中文/英文）

藉由一透明的第二因素之平台認證

PLATFORM AUTHENTICATION VIA TRANSPARENT SECOND FACTOR

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商・微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 6 人）

姓　名：（中文/英文）

1.湯姆史蒂芬/THOM, STEFAN

2.何特艾瑞克/HOLT, ERIK

3.伍頓大衛 R./WOOTEN, DAVID R.

4.尤瑞克湯尼/URECHE, TONY

5.史來茲丹/SLEDZ, DAN

6.麥克艾佛道格拉斯 M./MACIVER, DOUGLAS M.

國　籍：(中文/英文)

1. 德國/GERMANY
2. 美國/USA
3. 美國/USA
4. 加拿大/CANADA
5. 美國/USA
6. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

美國；2006 年 10 月 25 日；11/586,283

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

5.史來茲丹/SLEDZ, DAN

6.麥克艾佛道格拉斯 M./MACIVER, DOUGLAS M.

國　籍：(中文/英文)

1. 德國/GERMANY
2. 美國/USA
3. 美國/USA
4. 加拿大/CANADA
5. 美國/USA
6. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

美國；2006 年 10 月 25 日；11/586,283

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本技術領域概略關於電腦處理，尤指存取受保護的檔案。

【先前技術】

目前的處理系統提供了資料的保護。例如，BITLOCKER™ Drive Encryption（亦稱之為BITLOCKER™），為MICROSOFT® CORPORATION的產品，其提供可用於多種WINDOWS®作業系統之資料保護功能，BITLOCKER™可防止啟動另一作業系統或執行一軟體入侵工具的使用者來廢止檔案或系統保護，或是對於儲存在受保護磁碟上的檔案進行離線觀看。BITLOCKER™保護使用者資料，並保證執行WINDOWS®作業系統(例如WINDOWS® VISTA)的處理器在當系統離線時不會被竄改。

BITLOCKER™可以鎖定正常的開機處理，直到使用者提供一PIN或是插入包含有金鑰資料的USB快閃碟。例如，一USB快閃裝置可以在該開機程序之前插入到該處理系統。於開機程序期間，USB快閃裝置將可被辨識，並由其存取到金鑰資料。但是目前的處理系統於開機程序期間卻無法辨識像是智慧卡及CCID(積體電路卡片介面裝置)智慧卡為此目的之裝置。

【發明內容】

此內容說明係用來介紹在一簡化型式中選出的觀念，其在以下的例示性具體實施例的詳細說明中會進一步說明。此摘要內容說明並非要提出所主張之主題事項的關鍵特徵或基本特徵，也並非要用於限制所主張之主題事項的範圍。

一平台提供了透明性的存取到由該平台的韌體所支援的任何認證機制所限制的受保護檔案。該平台能夠接收一PIN，由多種裝置(例如 USB 快閃碟或智慧卡)中取出金鑰，並相容於未提供資料儲存的其它裝置，例如生物辨識裝置或類似者。在一範例性具體實施例中，平台韌體允許BITLOCKER™ 存取到一裝置(如 CCID 智慧卡)上特別供應的檔案及/或存取該裝置的一受保護 BIOS(基本輸入/輸出系統，“Basic input/output system”)部份。

【實施方式】

一透明的第二因素或裝置用於支援一平台的認證，在一範例性具體實施例中例如包含一智慧卡、一 CCID 智慧卡(積體電路卡介面裝置智慧卡)、一生物辨識裝置(例如指紋讀取器、視網膜掃描器或類似者)、或其組合。一種用於支援一平台的認證之透明的第二因素在此處說明時係應用於 BITLOCKER™ Drive Encryption (亦稱之為 BITLOCKER™，其為 MICROSOFT® CORPORATION 的產品)，但並不限於此。該第二因素由該平台的使用者之觀點視之為透明的，因該使用者不需要知道多種因素之間差異

的細節。

BITLOCKER™ 能夠取得儲存在區塊裝置上的外部金鑰。一區塊裝置為可用一區塊的形式傳送及/或接收資訊的裝置，例如一硬碟機。存取到一區塊裝置係由該平台的韌體提供。一平台可包含任何適當的處理器或類似者。例如，適當的平台包括(但不限於)個人電腦、伺服器電腦、掌上型或膝上型電腦、多處理器系統、應用微處理器的系統、機上盒、可程式化消費性電子產品、網路PC、微型電腦、主機型電腦、可攜式裝置、可攜式媒體播放器，例如可攜式音樂播放器、例如MP3播放器、隨身聽等，可攜式運算裝置、例如個人數位助理(PDA, "Personal digital assistant")、行動電話、可攜式電子郵件裝置、薄型客戶端、可攜式遊戲裝置等，消費性電子裝置、例如電視、DVD播放器、機上盒、監視器、顯示器等，公用運算裝置、例如公共資訊查詢臺、店內音樂試聽裝置、自動化櫃員機(ATM, "Automated teller machine")、收銀機等、導航裝置，不論是可攜式或安裝在車內及/或非習用運算裝置，例如廚房電器、機動車輛控制(如方向盤)等，或其組合，在一範例性具體實施例中，該平台的韌體用於提供性能來允許BITLOCKER™為了認證目的使用一第二因素，例如智慧卡、CCID智慧卡及/或生物辨識裝置。因此，BITLOCKER™讀取該區塊裝置上特別提供的檔案或是在該區塊裝置的受保護BIOS區域中的檔案，類似於自一儲存裝置讀取檔案，例如硬碟機。

在此處應用的一範例性智慧卡為根據 ISO 7816 標準的智慧卡。此標準描述了一智慧卡的特性及功能。在一範例性具體實施例中，用於存取一智慧卡的命令係根據 ISO 7816 標準，例如 ISO 7816-4 節，其定義基本命令來存取一簡單檔案系統及該檔案系統本身。

在一範例性具體實施例中，BITLOCKER™ 金鑰(如 BITLOCKER™ 利用的外部金鑰)係儲存在該區塊裝置的一檔案系統中。當該區塊裝置進行認證時，該等金鑰由該區塊裝置取得，後續於該平台的開機程序期間由 BITLOCKER™利用。在一範例具體實施例中，存取到該區塊裝置為唯讀存取。在另一範例性具體實施例中，在該區塊裝置上的檔案受到保護。例如，存取到該區塊裝置上的檔案直到提供一 PIN 或類似者才能同意進行。或在另一範例中，僅有該區塊裝置上的預定檔案被選出可由該平台存取。因此，如果該區塊裝置遺失或被偷，在該區塊裝置上的資訊受到保護，且無法由一未認證者做存取。

第 1 圖為經由系統 12 的 BIOS(基本輸入/輸出系統)部份 20 存取一區塊裝置 18 的一範例性系統 12 的功能方塊圖。如第 1 圖所示，系統 12 包含一 PCAT(PC 先進科技)、相容性開機管理員 22、BITLOCKER™軟體 24、及 BIOS 部份 20。BIOS 部份 20 包含一區塊裝置模擬器部份 14 及一區塊裝置驅動器部份 16。區塊裝置模擬器 14 用於偵測區塊裝置 18，及開啟在該區塊裝置 18 上的檔案。BIOS 部份 20 包含一區塊裝置驅動器 16，其配置以存取儲存在區塊裝

置 18 上的資訊。

BIOS 部份 20 包含用於控制包含系統 12 的平台之開機程序的韌體。在一範例性具體實施例中，BIOS 部份 20 包含一中斷管理程式(例如中斷 1A, 16 位元 INT 1Ah)，用於管理到一可信任運算群組(TCG, "Trusted computing group")的介面，例如像是一可信任平台模組(TPM, "Trusted platform module")、一中斷管理程式(例如 INT 9h)，用於管理到一人介面裝置(HDD, "Human interface device")的介面，例如像是鍵盤，及一中斷管理程式(如 INT 13h)，用於管理到一區塊裝置介面的介面，例如像是通用序列匯流排(USB, "Universal serial bus")相容性裝置(例如 USB 碟，USB 讀卡器)。要強調的是在第 1 圖中特定中斷管理程式的描述為範例性質，其可使用任何的介面。

BIOS 部份 20 支援 USB 控制器及基本裝置，像是 HID 及儲存區塊裝置。在一範例性具體實施例中，BIOS 部份 20 配置包含區塊裝置模擬器 14 及區塊裝置驅動器 16，藉以相容於像是智慧卡 18 或生物辨識裝置(未示於第 1 圖)之裝置。在一範例性具體實施例中，區塊裝置驅動器 16 根據(至少部份)積體電路卡介面裝置的標準來設置及執行，例如像是積體電路卡介面裝置版本 1-1 的標準。其不需要實施如積體電路卡介面裝置之標準中所述之完整裝置類別，而是該裝置類別的一子集合即為適當。例如，用於允許與該讀卡器之互動及與智慧卡 18 之通訊的元件，例如提供電力給智慧卡 18，自智慧卡移開電源，並傳送命令及

回應 APDU(應用協定資料單元，“Application Protocol Data Units”)往返到智慧卡 18，皆為適當。

在一範例性具體實施例中，讀卡器經由一 PCMCIA(Personal Computer Memory Card International Association, or Peripheral Component Microchannel Interconnect Architecture)介面相容於智慧卡 18。此具體實施例提供了行動式電腦及類似者的較佳用途。智慧卡 18 的型式可為卡片、鑰匙鏈、或任何適當的組態。

在一範例性具體實施例中，如第 2 圖所示，區塊裝置 18 包含一生物辨識裝置，例如指紋讀取器、視網膜掃描器或類似者。基本上生物辨識裝置並未提供資料儲存。在區塊裝置 18 包含一生物辨識裝置或其它並未提供資料儲存的第二因素的具體實施例中，BIOS 部份 20 之韌體執行區塊裝置 18 的認證。如果區塊裝置 18 的認證成功，一代符可由區塊裝置 18 提供，其可用於存取該平台的一安全區域，其包含進行開機程序所需要的金鑰，例如開啟 BITLOCKER™。在此具體實施例中，儲存在該平台的安全區域中的資訊在區塊裝置 18 的事先成功認證之前無法讀取。

如第 1 圖及第 2 圖所示，該平台的 BIOS 部份 20 為靜態結合。也就是說，將數值關連於識別的程序中，結合是在該開機程序或該平台的作業系統開始之前即完成。因此，區塊裝置模擬器 14 及區塊裝置驅動器 16 對所有類別的區塊裝置 18 皆為固定。

第 3 圖為透過系統 28 的一延伸性韌體介面(FEI, "Firmware interface")26 存取一區塊裝置 18 的一範例性系統 28 的功能方塊圖。系統 28 類似於系統 12 的方式執行，如上所述，其差別在於系統 12 的 BIOS 實施及系統 28 的 EFI 實施。EFI 已知來用於取代 BIOS。類似於 BIOS，EFI 負責控制一作業系統的開機程序，並提供該作業系統及硬體之間的介面。EFI 26 為動態結合。也就是說，結合係在開機程序期間完成。因此，區塊裝置模擬器 14 及區塊裝置驅動器 16 可分別實施，且並不需要結合到一靜態單元。區塊裝置驅動器 16 可在 EFI 開機時間時載入。

如第 3 圖所示，系統 28 包含一 EFI 相容性開機管理員 30，BITLOCKER™軟體 24、及 EFI 部份 26。EFI 部份 26 包含一區塊裝置模擬器部份 14 及一區塊裝置驅動器部份 16。區塊裝置模擬器 14 用於偵測區塊裝置 18，並開啟在區塊裝置 18 上的一檔案。EFI 部份 26 包含一區塊裝置驅動器 16，用於存取儲存在區塊裝置 18 上的資訊。

EFI 部份 26 包含用於控制包含系統 12 的平台之開機程序的韌體。在一範例性具體實施例中，EFI 部份 26 包含一中斷管理程式，用於管理到一可信任運算群組(TCG)的介面，例如像是一可信任平台模組(TPM)、該中斷管理程式用於管理到一人介面裝置(HDD)的介面，例如像是鍵盤，及該中斷管理程式用於管理到一區塊裝置介面的介面，例如像是通用序列匯流排(USB, "Universal serial bus")相容性裝置(例如 USB 碟，USB 讀卡器)。要強調的是在第

1 圖中特定中斷管理程式的描述為範例性質，其可使用任何的介面。

EFI 部份 26 支援 USB 控制器及基本裝置，例如 HID 及儲存區塊裝置。在一範例性具體實施例中，EFI 部份 26 配置以包含區塊裝置模擬器 14 及區塊裝置驅動器 16，藉以相容於像是智慧卡 18 或生物辨識裝置(未示於第 3 圖)之裝置。在一範例性具體實施例中，區塊裝置驅動器 16 根據(至少部份)積體電路卡介面裝置的標準來設置及執行，例如像是積體電路卡介面裝置版本 1-1 的標準。其不需要實施如積體電路卡介面裝置之標準中所述之完整裝置類別，而是該裝置類別的一子集合即為適當。例如，用於允許與該讀卡器之互動及與智慧卡 18 之通訊的元件，例如提供電力給智慧卡 18，自智慧卡移開電源，並傳送命令及回應 APDU(應用協定資料單元，“Application Protocol Data Units”)往返到智慧卡 18，皆為適當。

在一範例性具體實施例中，該讀卡器經由 PCMCIA(Personal Computer Memory Card International Association 或 Peripheral Component Microchannel Interconnect Architecture))介面相容於智慧卡 18。此具體實施例提供了行動式電腦及類似者較佳的用途。智慧卡 18 的型式可為卡片、鑰匙鏈、或任何適當的組態。

在一範例性具體實施例中，如第 4 圖所示，區塊裝置 18 包含一生物辨識裝置，例如指紋讀取器、視網膜掃描器或類似者。生物辨識裝置基本上並不提供資料儲存。在區

塊裝置 18 包含一生物辨識裝置或其它並未提供資料儲存的第二因素的具體實施例中，EFI 部份 26 之韌體執行區塊裝置 18 的認證。如果區塊裝置 18 的認證成功，一代符可由區塊裝置 18 提供，其可用於存取該平台的一安全區域，其包含進行開機程序所需要的金鑰，例如開啟 BITLOCKER™。在此具體實施例中，儲存在該平台的安全區域中的資訊在區塊裝置 18 的事先成功認證之前無法讀取。

在另一範例性具體實施例中，EFI 由硬碟機或類似者的 BIOS 上開機。

於作業系統載入到該平台上之前，該區塊裝置被認證。在一範例性具體實施例中，如果實施一 BIOS，該區塊裝置在呼叫 BIOS 上的中斷 19h 之前被任證。也就是說，該區塊裝置於開機程序期間於 BIOS 之前被認證；然後開始載入該作業系統。在一範例性具體實施例中，如果實施 EFI，該區塊裝置在該開機管理員於 EFI 上被引發之前被認證。該區塊裝置可由任何適當的手段認證，例如像是透過使用一 PIN 或類似者。在該區塊被成功認證之後，在該平台的記憶體中產生一虛擬區塊裝置。

為了在平台記憶體中產生該虛擬區塊裝置，該區塊裝置的儲存即搜尋包含將允許該開機程序來開始/繼續執行的資訊之位置。在該區塊裝置上儲存的結構可包含該區塊裝置上儲存之任何適當的結構及位置或是數個位置，其中包含允許開機程序執行的資訊，即可用任何適當方式辨識。

第5圖為符合ISO 7816標準的區塊裝置之範例性檔案系統40。其要強調檔案系統40為範例性，且在該區塊裝置上可以實施任何適當的檔案系統。在一範例性具體實施例中，該區塊裝置的檔案系統40包含至少一主控檔案32(如第5圖中的MF)，至少一專屬檔案34(如第5圖中的DF)，及至少一基礎檔案36(如第5圖中的EF)。為了簡化起見，每種檔案僅標示一個檔案(32, 32及36)。檔案系統40的架構使得該專屬檔案與該基礎檔案隸屬於主控檔案32。主控檔案32為根檔案。一專屬檔案包含檔案控制資訊。一專屬檔案依照需要可包含記憶體是否可用於配置之指示。一專屬檔案可為一基礎檔案的父親，及/或一專屬檔案可為一基礎檔案。

在一範例性具體實施例中，一基礎檔案包含一指示，以代表其包含資訊來允許該開機程序的執行。例如，一基礎檔案可包含一指示，代表其包含BITLOCKER™所要利用的金鑰。在一範例性具體實施例中，如第5圖所示，一基礎檔案指定為VFAT(虛擬檔案屬性表，“Virtual file attribute table”)，以代表其包含資訊來允許該開機程序的執行。包含在一基礎檔案中具有VFAT的一ID之資訊的種類範例示於區塊38。在其它資訊當中，BITLOCKER™可使用的金鑰表示成：LFN (邏輯檔案名稱，“Logical File Name"):E5E1A420-0134-4677-88B1-855E9DC200F73EK, 及LFN:AE324B14-5264-E32A-9A23-225AB6823A32.BEK.

第6圖為用於在平台記憶體中產生一虛擬區塊裝置的

一範例性程序的流程圖。在步驟40中，配置該平台中的記憶體，並初始化任何需要的系統結構。在一範例性具體實施例中，該區塊裝置於執行開機程序之前結合到該平台。於一範例性具體實施例中，在該區塊裝置上的檔案系統實施成一唯讀FAT，其開機磁區等於零，以防止該平台由該區塊裝置開機。於載入該作業系統在該平台上之前，該區塊裝置的主控檔案於步驟42中被載入到平台記憶體。該韌體，例如BIOS或EFI，在步驟42中遞迴地搜尋該區塊裝置上該主控檔案及隸屬專屬檔案中具有一ID VFAT(代表一ID號碼)的基礎檔案。在步驟46中，如果未發現到具有一ID VFAT的基礎檔案，在步驟58中即釋出未用到的資源，然後結束該程序。在步驟46中，如果發現到具有ID VFAT的基礎檔案，於步驟48中，載入所有這些基礎檔案到平台記憶體中。找出具有一ID VFAT的基礎檔案代表該區塊裝置係提供於開機存取，且可進行產生該虛擬區塊裝置。

於步驟50中打開及解析一基礎檔案。在根據ISO 7816標準的範例性具體實施例中，該基礎檔案被限制為一5位元組的識別。因此，該平台在該區塊裝置上維持所有檔案的一目錄，其要包含在該虛擬區塊裝置中，允許BITLOCKER™使用名稱超過5位元之外部金鑰。例如像是BITLOCKER™金鑰的資訊在步驟52中由解析的基礎檔案中拮取。在步驟54中，拮取的資訊，例如像是BITLOCKER™金鑰，即被加入到平台記憶體中虛擬區塊裝置的每一個適

當檔案中。如果存在有更多具有 ID VFAT 的基礎檔案(步驟 56)，該程序進行到步驟 50，並繼續進行，如上所述。如果不存在有具有一 ID VFAT 之基礎檔案(步驟 56)，未使用的資源即被釋放，且程序於步驟 58 中結束。在 EF 中並未辨識為 VFAT 之區塊裝置上發現的檔案並未被存取或讀取，因此不會暴露。

該虛擬區塊裝置在平台記憶體中動態產生。該虛擬區塊裝置於該開機程序期間產生一次(例如當該平台通電時)。該虛擬區塊裝置的檔案仍停留在平台記憶體中，即使該區塊裝置與該平台分離。但是，該虛擬區塊裝置於預開機期間存在，且在當載入該平台作業系統時將被摧毀。

該虛擬區塊裝置的資料夾架構將依照該區塊裝置的資料夾架構。由於僅載入具有 ID VFAT 的基礎檔案，在該區塊裝置中不想要的檔案即不會在該虛擬區塊裝置中表示。因此，僅有實際上提供資料的區塊之虛擬記憶體會被配置。第 7 圖所示為該虛擬區塊裝置的平台記憶體之範例性配置。如第 7 圖所示，平台記憶體係配置給一開機記錄磁區 60、一檔案配置表磁區 62、一備份檔案配置表磁區 64、一根目錄 66 及至少一資料儲存區域磁區 68。資料儲存區域 68 可包含資訊用於允許該開機程序來執行，例如像是 BITLOCKER™ 金鑰。在一範例性具體實施例中，每個磁區包含 512 位元組。平台記憶體可依任何適當方式配置，例如像是連續性。在一範例性具體實施例中，步驟 66 被執行，所有其它區塊皆在它們由該開機應用程式請求時立即

運算。

如上所述，該區塊裝置可包含一 CCID 智慧卡。第 8 圖為用於存取一 CCID 智慧卡之範例性程序的流程圖。要強調的是在第 8 圖中所述的程序可應用到任何適當的區塊裝置。在步驟 70 中，其決定是否偵測到該 CCID 讀卡器。如果未偵測到讀卡器(步驟 70)，如上所述，中斷 19h 在實施 BIOS 時呼叫，或是如果實施 EFI 時載入開機管理員，如步驟 90。如果偵測到該讀卡器(步驟 70)，在步驟 72 中決定是否偵測到耦合於該讀卡器之智慧卡。如果未偵測到智慧卡(步驟 72)，該程序進行到步驟 90。如果偵測到智慧卡(步驟 72)，在步驟 74 中決定該智慧卡是否符合 ISO 7816-4，或任何其它適當的協定。如果智慧卡不相容時(步驟 74)，該程序進行到步驟 90。如果智慧卡相容時(步驟 74)，來自該智慧卡之專屬開機檔案即在步驟 76 中載入到平台記憶體當中。

在步驟 78 中決定 DF 開機檔案是否有保護，例如由 PIN 所保護。如果 DF 開機檔案並未保護(步驟 78)，在平台記憶體中虛擬區塊裝置的產生即在步驟 88 中啟始。如果 DF 開機檔案受到保護(步驟 78)，在步驟 80 中發出提示要求一 PIN 或類似者。用於允許輸入 PIN 或類似者之使用者介面(UI, "User interface")在初始程式載入(IPL, "Initial program load")之前或開始開機碼之前完成。一旦鍵盤、顯示器及/或其它 UI 裝置的控制傳送到 IPL 碼，該認證提示即可不呈現。在一範例性具體實施例中，預期該智慧卡在

供應電源給該平台之前耦合(例如插入)到該讀卡器中。

於步驟 82 中接收到 PIN 或類似者。在步驟 84 中，利用 PIN 或類似者來解鎖該智慧卡。在步驟 86 中，其決定是否該讀卡器已解鎖。如果該智慧卡已解鎖(步驟 86)，該程序進行到步驟 88。如果該智慧卡未解鎖(步驟 86)，該程序進行到步驟 80。

在成功產生該虛擬區塊裝置之後，IPL 碼列舉該虛擬區塊裝置，並將其包含在對於例如 BITLOCKER™ 外部金鑰或類似者的搜尋當中。一旦該金鑰已由該開機管理員載入，且該等金鑰已經成功地解鎖該加密的磁區之後，控制即傳送到該作業系統載入器。在一範例性具體實施例中，在該虛擬區塊裝置之平台記憶體中的儲存位置並未由該作業系統載入器保護、保留或知道。因此，作業系統檔案被載入，且最終可覆寫到該虛擬區塊裝置的儲存空間。

在一運算裝置上可執行用於支援一平台的認證之一透明性第二因素的多種具體實施例。第 9 圖及以下的討論提供了對一適當的運算環境之簡短概略描述，其中可以實施這種運算裝置。雖然並不需要，用於支援一平台的認證之透明性第二因素的多個態樣係在電腦可執行指令的概略內容中說明，例如程式模組，其係由一電腦所執行，例如一客戶端工作站或一伺服器。概言之，程式模組包括例式、程式、物件、組件、資料結構等，其可執行特殊工作或實施特定的摘要資料型態。再者，經由一透明的第二因素之一平台的認證可利用其它電腦系統組態實施，其中包括掌

上型裝置、多處理器系統、應用微處理器或可程式化消費性電子產品；網路 PC、迷你級電腦、主機型電腦及類似者。再者，經由一透明的第二因素之平台的認證亦可在分散式運算環境中實施，其中工作係由透過一通訊網路鏈結的遠端處理裝置進行。在一分散式運算環境中，程式模組可以同時位於本地及遠端記憶體儲存裝置中。

一電腦系統可大致區分成三個組件群組：該硬體組件、該硬體/軟體介面系統組件、及該應用程式組件(亦稱之為「使用者組件」或「軟體組件」)，一電腦系統的多種具體實施例中，除此之外，該硬體組件可包含中央處理單元(CPU) 621、記憶體(ROM 664 及 RAM 625)、基本輸入/輸出系統(BIOS)666、及多個輸入/輸出(I/O)裝置，例如鍵盤 640、滑鼠 642、監視器 647 及/或印表機(未示出)。該硬體組件包含電腦系統之基本實體基礎建設。

該應用程式組件包含多種軟體程式，其包括但不限於編譯器、資料庫系統、文字處理器、商業程式、視訊遊戲等等。應用程式提供手段使得電腦資源用於解決問題，提供解決方案，並處理多種使用者(機器、其它電腦系統及/或終端使用者)的資料。在一範例性具體實施例中，應用程式經由一透明的第二因素執行關於一平台認證的功能，如上所述，例如偵測該區塊裝置、開啟在該區塊裝置上的檔案，搜尋該區塊裝置上的檔案，在平台記憶體中產生一虛擬區塊裝置，利用一 PIN 或類似者來解鎖該區塊裝置，並開始該開機程序等。

該硬體/軟體介面程式組件包含(在一些具體實施例中並可僅包含)一作業系統，其本身在大多數例子中包含一外殼及一核心。一「作業系統」(OS)為一特殊程式，其做為應用程式與電腦硬體之間的中介。該硬體/軟體介面程式組件亦可包含一虛擬機器管理員(VMM, "Virtual machine manager")、一共用語言執行時間(CLR, "Common Language Runtime")或其功能性同等者、一 Java 虛擬機器(JVM, "Java Virtual Machine")或其功能性同等者，或其它這些軟體組件，其可取代或加入到一電腦系統中的作業系統。一硬體/軟體介面系統之目的係提供一種環境，其中一使用者可執行應用程式。

概言之，該硬體/軟體介面系統於啟始時載入到一電腦系統，然後管理該電腦系統中所有的應用程式。該等應用程式藉由透過一應用程式介面(API, "Application program interface")請求服務並與該硬體/軟體介面系統互動。某些應用程式賦予終端使用者經由一使用者介面與該硬體/軟體介面系統互動之功能，例如一命令語言或一圖形使用者介面(GUI, "Graphical user interface")。

傳統上一硬體/軟體介面系統執行應用程式的多種服務。在一多工化硬體/軟體介面系統中多個程式可同時執行，該硬體/軟體介面系統決定那些應用程式必須依何種程序執行，以及對於每個應用程式在切換到另一個應用程式之前的一個輪迴中允許多少時間。該硬體/軟體介面程式亦管理多個應用程式之間的內部記憶體之共享，且管理與附

屬的硬體裝置之間的輸出及輸入，例如硬碟機、印表機及撥接埠。該硬體/軟體介面程式亦傳送訊息到每個應用程式(及在某些案例中傳送到終端使用者)，其係關於作業的狀態及已經發生的任何錯誤。該硬體/軟體介面系統亦卸載批次工作(例如列印)之管理，讓該啟始應用程式可免除此工作，並可恢復其它處理及/或作業。在可提供平行處理的電腦上，一硬體/軟體介面系統亦管理區分一程式，允許其可一次在一個以上的處理器上執行。

一硬體/軟體介面系統外殼(亦稱之為外殼“shell”)為一互動式終端使用者介面到一硬體/軟體介面系統。(一外殼亦稱之為一「命令解譯器」或在一作業系統中稱之為「作業系統外殼」)。一外殼為一硬體/軟體介面系統之外層，其可由應用程式及/或終端使用者直接存取。相對於一外殼，一核心為一硬體/軟體介面系統的最內層，其直接與該硬體組件互動。

如第9圖所示，一範例性通用運算系統包括一習用運算裝置660或類似者，其包括一處理單元621、一系統記憶體662、及一系統匯流排623，其結合多種系統組件，其包括該系統記憶體到處理單元621。系統匯流排623可為數種匯流排結構中任何一種，其中包括一記憶體匯流排或記憶體控制器，一周邊匯流排，及使用多種匯流排架構中任何一種的一本地匯流排。該系統記憶體包括唯讀記憶體(ROM)664，及隨機存取記憶體(RAM)625。一基本輸入/輸出系統666(BIOS)，包含基本例式來協助在該運算系統660

內元件之間傳送資訊，例如在開機期間，其可儲存在 ROM 664 中。運算裝置 660 另可包括一硬碟機 627，用於讀取硬碟機或寫入硬碟機(硬碟機未示出)、一磁碟機 628(如軟碟機)，用於讀取及寫入到一可移除磁碟片 629(如軟碟片、可移除儲存)，及一光碟機 630，用於讀取及寫入到一可移除光碟片 631，例如 CD-ROM 或其它光學媒體。硬碟機 627、磁碟機 628 及光碟機 630 由一硬碟機介面 632 分別連接到系統匯流排 623，一磁碟機介面 633、及一光碟機介面 634。該等裝置及它們相關的電腦可讀取媒體提供電腦可讀取指令、資料結構、程式模組及運算裝置 660 之其它資料的非揮發性儲存。雖然此處所述的範例性具體實施例利用一硬碟、一可移除磁碟片 629 及一可移除光碟片 631，熟習此項技術者將可瞭解到有其它種類的電腦可讀取媒體可儲存由一電腦存取的資料，例如磁匣、快閃記憶卡、數位視訊碟片、Bernoulli 卡匣、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、及類似者，其亦可用在範例性作業環境中。類似地，該範例性環境亦可包括多種監視裝置，例如熱感測器及保全或火警系統，及其它資訊來源。

一些程式模組可儲存在硬碟、磁碟片 629、光碟片 631、ROM 664 或 RAM 625 上，其中包括一作業系統 635、一或多個應用程式 636、其它程式模組 637、及程式資料 638。一使用者可透過輸入裝置，例如鍵盤 640 及指向裝置 642(如滑鼠)輸入命令及資訊到運算裝置 660。其它輸入裝置(未示出)可包括麥克風、搖桿、遊戲板、衛星碟、掃描

器或類似者。這些及其它輸入裝置通常連接到該處理單元621，其透過耦合到系統匯流排之一序列埠介面646，但亦可由其它介面做連接，像是平行埠、遊戲埠或一通用序列匯流排(USB)。一監視器 647 或其它種類的顯示裝置亦經由一介面連接到系統匯流排 623，例如一視訊轉接器 648。除了監視器 647 之外，運算裝置基本上包括其它周邊輸出裝置(未示出)，例如喇叭及印表機。第 9 圖的範例性環境亦包括一主機轉接器 655、小型電腦系統介面(SCSI, "Small Computer System Interface") 匯流排 656，及連接到 SCSI 匯流排 656 之外部儲存裝置 662。

運算裝置 660 可在使用邏輯性連接到一或多個遠端電腦的網路化環境中運作，例如遠端電腦 649。遠端電腦 649 可為另一個運算裝置(例如個人電腦)、一伺服器、一路由器、一網路 PC、一端點裝置、或其它共享網路節點、及原則上包括關連到運算裝置 660 之許多或所有如上所述之元件，，雖然僅一個記憶體儲存裝置 650(軟碟機)已經例示於第 9 圖。在第 9 圖中所述之邏輯連接包括一區域網路(LAN, "Local area network")651 及一廣域網路(WAN, "Wide area network")652。這種網路化環境為辦公室中的常見，企業化電腦網路、企業內網路及網際網路。

當用於 LAN 網路環境中時，運算裝置 660 經由一網路介面或轉接器 653 連接到 LAN 651。當用於 WAN 網路環境中時，運算裝置 660 可包括一數據機 654 或其它設施，用於在 WAN 652 上建立通信，例如網際網路。數據機 654

其可為內部或外部，其經由序列埠介面 646 連接到系統匯流排 623。在一網路化環境中，相對於運算裝置 660 或其部份所述之程式模組可儲存在遠端記憶體儲存裝置中。其將可瞭解到所示的網路連接為範例性，並可使用建立電腦之間的一通訊鏈結之其它手段。

雖然可明白經由一透明的第二因素之一平台之認證的多種具體實施例特別適用於電腦化系統，本文無意限制本發明於這些具體實施例。相反地，在此處所述之「電腦系統」係應包含能夠儲存及處理資訊的任何及所有裝置，及/或能夠使用所儲存的資訊來控制該裝置本身的行為或執行，不論是否這些裝置在本質上為電子、機械、邏輯或虛擬。

此處所述的多種技術可以實施成連接於硬體或軟體，或在適當時為兩者的組合。因此，經由一透明的第二因素的一平台之認證的方法及裝置，或某些態樣或其部份，其可採取實施成有形媒體中的程式碼的型式(即指令)，例如軟碟片、CD-ROM、硬碟機、若任何其它機器可讀取儲存媒體，其中當該程式碼被載入並由一機器執行，例如一電腦，該機器成為經由一透明的第二因素之一平台的認證之裝置。

該程式可在需要時實施成組合語言或機器語言。在任何案例中，該語言可為編譯的或解譯的語言，並結合於硬體實施。經由一透明的第二因素之一平台的認證之方法及裝置可經由實施成程式碼型式的通訊來實施，其在一些傳

輸媒體上傳送，例如透過電子連線或纜線，透過光纖，或透過任何其它形式的傳輸，其中當該程式碼由一機器接收、載入並執行時，例如 EPROM、閘極陣列、一可程式化邏輯裝置(PLD, “Programmable logic device”)，一客戶端電腦或類似者，該機器成為由特性管理虛擬機器之裝置。當實施在一通用處理器上時，該程式碼結合該處理器來提供一唯一裝置，其用於啟動經由一透明的第二因素之一平台的功能性認證。此外，用於連接經由一透明的第二因素之一平台的認證的任何儲存技術總是為硬體及軟體之組合。

本文已結合多個圖面之範例性具體實施例說明一透明的第二因素之一平台的認證，應可瞭解其它類似的具體實施例可以使用或修正，以及對本文所述的具體實施例進行添加，用於執行透過一透明的第二因素之一平台的認證之相同功能，而不與其背離。因此，本文所述之藉由一透明的第二因素之平台認證不限於任何單一具體實施例，而應視為由附屬申請專利範圍所界定的廣度及範圍。

【圖式簡單說明】

配合附屬的圖式閱讀時將可進一步瞭解前述「發明內容」和「實施方式」。為了說明藉由一透明的第二因素的平台認證之目的，在圖面中所示為其範例性架構；但是藉由一透明的第二因素的平台認證並不限於所揭露的特定方法及措施。

第 1 圖為用於藉由該系統的一 BIOS 部份存取一區塊裝置的範例性系統之功能方塊圖。

第 2 圖為用於藉由該系統的一 BIOS 部份存取一生物辨識裝置的範例性系統之功能方塊圖。

第 3 圖為用於藉由該系統的一 EFI 存取一區塊裝置的範例性系統之功能方塊圖。

第 4 圖為用於藉由該系統的一 EFI 存取一生物辨識裝置的範例性系統之功能方塊圖。

第 5 圖為符合 ISO 7816 標準的區塊裝置之範例性檔案系統。

第 6 圖為用於在平台記憶體中產生一虛擬區塊裝置的一範例性程序的流程圖。

第 7 圖為該虛擬區塊裝置的平台記憶體之範例性配置。

第 8 圖為用於存取一 CCID 智慧卡之範例性程序的流程圖。

第 9 圖為可以實施藉由一透明的第二因素之平台認證的一範例性運算環境。

【主要元件符號說明】

12	系統	20	BIOS 部分
14	區塊裝置模擬器	22	開機管理員
16	區塊裝置驅動器	24	BITLOCKER™ 軟體
18	智慧卡	30	開機管理員

60 開機記錄
62 檔案配置表一
64 檔案配置表二
66 根目錄
68 資料儲存區域
621 處理單元
623 系統匯流排
627 硬碟機
628 軟碟機
629 可移除磁碟片
630 光碟機
632 硬碟機介面
633 磁碟機介面
634 光碟機介面
635 作業系統
636 應用程式
637 其他程式
638 程式資料
640 鍵盤
642 滑鼠
646 序列埠介面
647 監視器
648 視訊轉接器
649 遠端電腦
650 軟碟機
651 區域網路
652 廣域網路
653 網路介面
654 數據機
655 主機轉接器
656 SCSI 匯流排
660 電腦
662 儲存裝置
666 基本輸入/輸出系統

五、中文發明摘要：

一本發明揭示一系統的韌體，其用於允許次級裝置用於認證，例如一智慧卡。在一範例性具體實施例中，該次級裝置為符合 ISO 7816 標準的一 CCID 智慧卡。該智慧卡於開機該系統之前插入到耦合於該系統的一讀卡器。該韌體包含一模擬器及驅動器，用於允許來自該智慧卡之認證資訊用於允許該開機程序的執行。在一範例性具體實施例中，該智慧卡包含 BITLOCKER™所使用的外部金鑰。該次級裝置相容於實施一 BIOS 的系統及實施 EFI 之系統。認證亦可藉由不提供資料儲存之裝置來完成，例如一生物辨識裝置或類似者。

六、英文發明摘要：

Firmware of a system is configured to allow secondary devices, such as a smart card, to be used for authentication. In an example embodiment, the secondary device is a CCID smart card in compliance with the ISO 7816 specification. The smart card is inserted into a card reader coupled to the system prior to booting the system. The firmware comprises an emulator and driver configured to allow authentication information from the smart card to be utilized to allow execution of the boot process. In an example embodiment, the smart card comprises external keys for use with BITLOCKER™ The secondary device is compatible with systems implementing a BIOS and with systems implementing EFI. Authentication also can be accomplished via devices that do not provide data storage, such as a biometric device or the like.

十、申請專利範圍：

1. 一種平台認證系統，包含：

至少一 BIOS 部份及一 EFI 部份，包含：

一區塊裝置模擬器，用於：

偵測耦合於該系統之一區塊裝置；及

開啟在該區塊裝置上的一檔案；及

一區塊裝置驅動器，其調設為用於存取在該區塊裝置上的資訊。

2. 如申請專利範圍第 1 項所述之系統，其中該區塊裝置包含一智慧卡。

3. 如申請專利範圍第 2 項所述之系統，其中該區塊裝置包含一 CCID 智慧卡。

4. 如申請專利範圍第 1 項所述之系統，其中該區塊裝置包含一 USB 相容區塊裝置。

5. 如申請專利範圍第 1 項所述之系統，其中該區塊裝置包含一 PCMCIA 相容區塊裝置。

6. 如申請專利範圍第 1 項所述之系統，其中存取該區塊裝置上的資訊受到保護。

7. 如申請專利範圍第 1 項所述之系統，其中該區塊裝置包含一生物辨識裝置。

8. 如申請專利範圍第 7 項所述之系統，其中在該生物辨識裝置上存取的資訊包含一代符“token”，用於允許該系統一開機程序的執行。

9. 如申請專利範圍第 7 項所述之系統，其中該區塊裝置

包含一指紋讀取器。

10. 如申請專利範圍第 1 項所述之系統，其中在該區塊裝置上存取的資訊包含金鑰資訊，用於允許該系統一開機程序的執行。

11. 一種藉由一區塊裝置認證一平台的方法，該方法包含：

藉由該平台的至少一 BIOS 部份及該平台的一 EFI 部份偵測一區塊裝置；

認證該偵測的區塊裝置；

自該區塊裝置取得資訊，用於允許該系統的一開機程序的執行。

12. 如申請專利範圍第 11 項所述之方法，其中該區塊裝置包含下列至少一項：一智慧卡、與一 CCID 智慧卡。

13. 如申請專利範圍第 11 項所述之方法，其中該區塊裝置包含下列至少一項：一 USB 相容區塊裝置、與一 PCMCIA 相容區塊裝置。

14. 如申請專利範圍第 11 項所述之方法，另包含提供一認證的指示，以自該區塊裝置取得該資訊。

15. 如申請專利範圍第 11 項所述之方法，其中該區塊裝置包含下列至少一項：一生物辨識裝置與一指紋讀取器。

16. 一種電腦可讀取媒體，其上儲存有電腦可執行指令，用於藉由一區塊裝置認證一平台，其執行以下的步驟：

藉由該平台系統的一 BIOS 部份及該平台的一 EFI 部份中至少一項之一區塊裝置模擬器，偵測一區

塊裝置；及

藉由該區塊裝置模擬器，開啟該區塊裝置上的一檔案；及

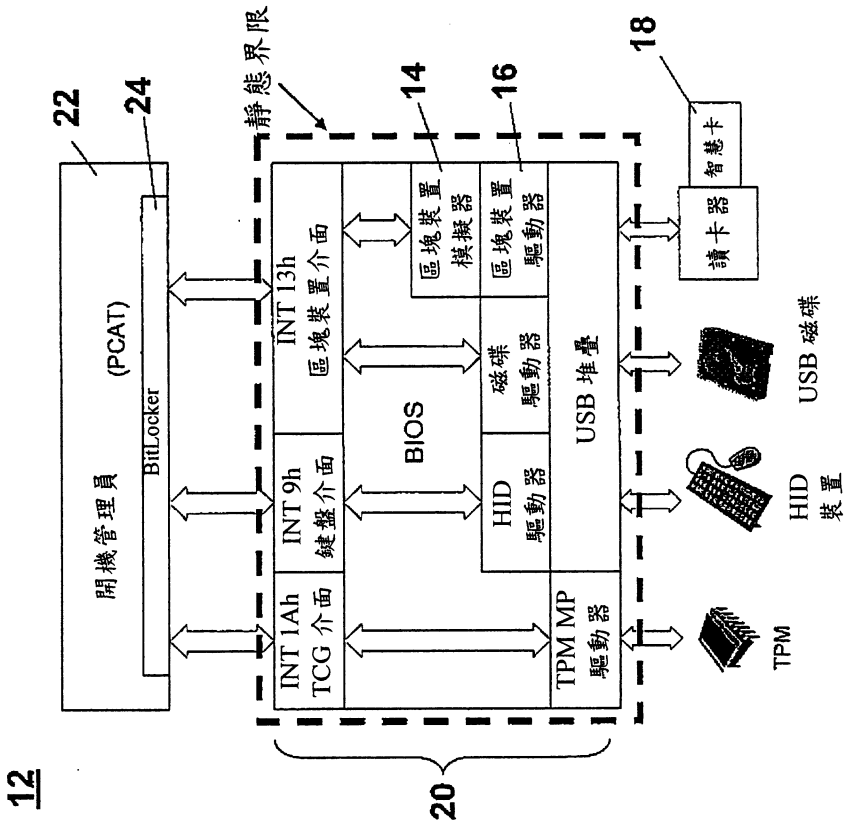
藉由 BIOS 部份及 EFI 部份中至少一項的一區塊驅動器，存取在該區塊裝置上的資訊。

17. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中該區塊裝置包含下列至少一項::一智慧卡、與一 CCID 智慧卡。

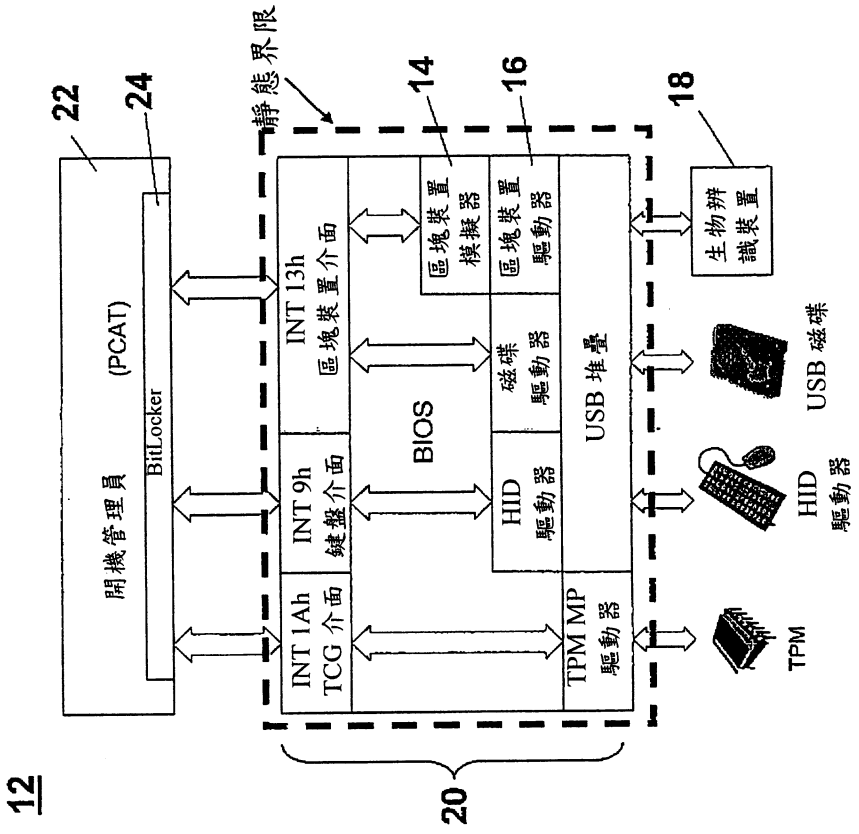
18. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中該區塊裝置包含下列至少一項：一 USB 相容區塊裝置、與一 PCMCIA 相容區塊裝置。

19. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中該區塊裝置包含下列至少一項：一生物辨識裝置、與一指紋讀取器。

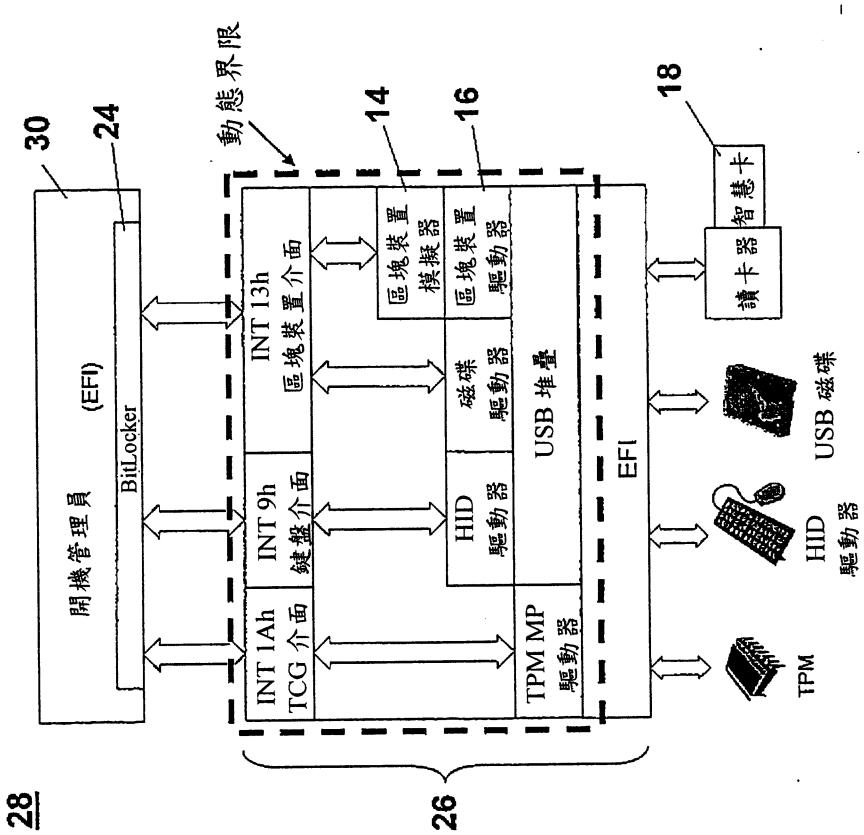
20. 如申請專利範圍第 16 項所述之電腦可讀取媒體，其中在該區塊裝置上存取的資訊包含金鑰資訊，用於允許該系統一開機程序的執行。


12
開機管理員
(PCAT)
BitLocker
22
24
靜態界限
INT 1Ah
TCG 介面
INT 9h
鍵盤介面
INT 13h
區塊裝置介面
BIOS
TPM MP
驅動器
HID
驅動器
磁碟
驅動器
USB 堆疊
區塊裝置
模擬器
區塊裝置
驅動器
14
16
18
20
讀卡器
智慧卡
TPM
HID
裝置
USB 磁碟

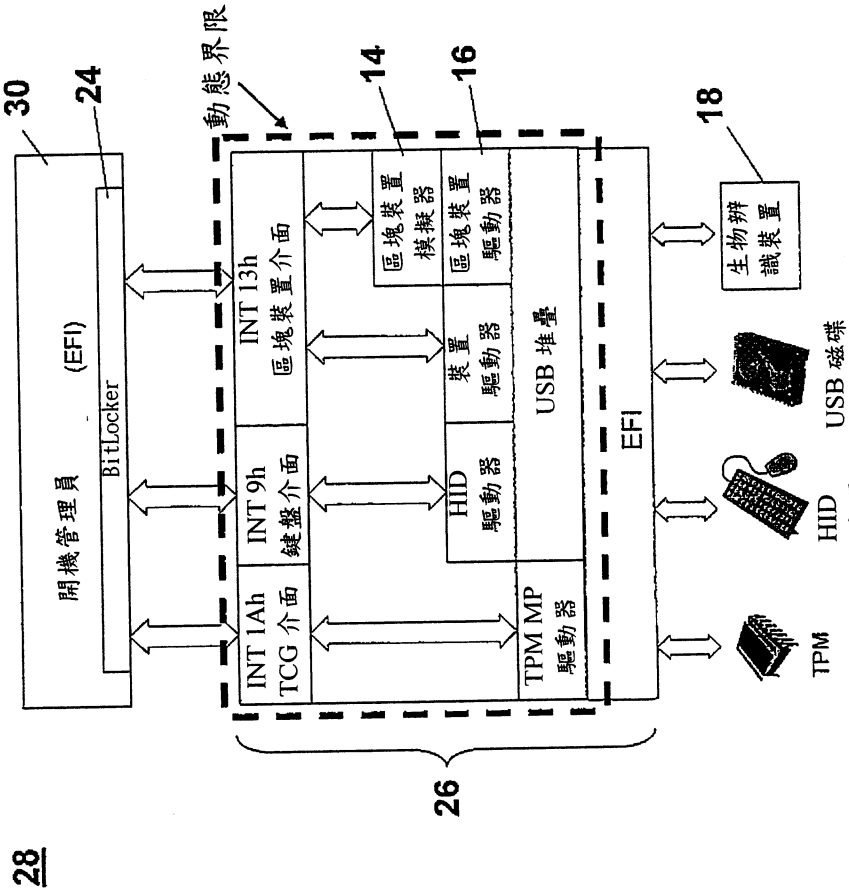
第 1 圖


12
開機管理員 (PCAT)
BitLocker
22
24
靜態界限
INT 1Ah TCG 介面
INT 9h 鍵盤介面
INT 13h 區塊裝置介面
BIOS
HID 驅動器
磁碟驅動器
USB 堆疊
TPM MP 驅動器
區塊裝置模擬器
區塊裝置驅動器
14
16
18
20
生物辨識裝置
TPM
HID 驅動器
USB 磁碟

第 2 圖

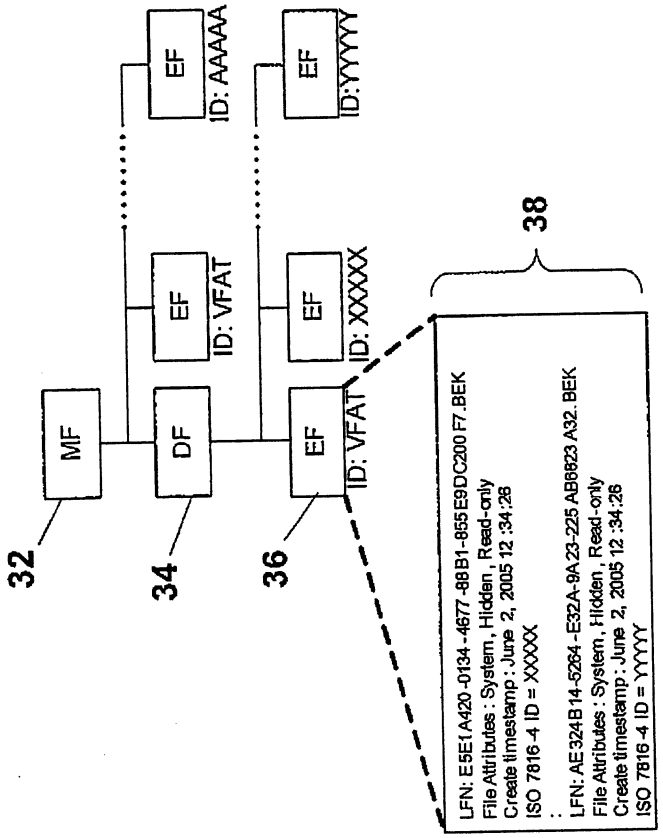

28
30
開機管理員 (EFI)
BitLocker
24
動態界限
INT 1Ah TCG 介面
INT 9h 鍵盤介面
INT 13h 區塊裝置介面
TPM MP 驅動器
HID 驅動器
磁碟 驅動器
區塊裝置 驅動器
USB 堆疊
EFI
區塊裝置 模擬器
14
16
26
18
讀卡器
智慧卡
TPM
HID
USB 磁碟
驅動器

第 3 圖

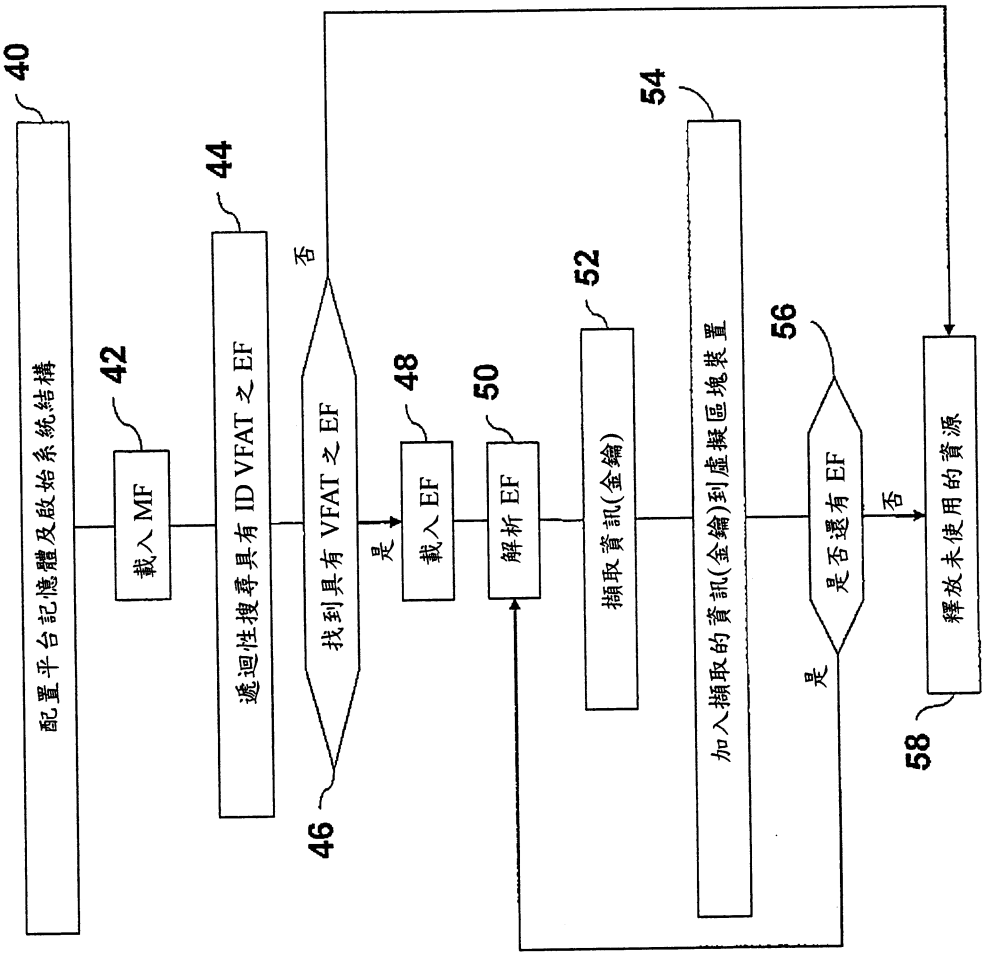

28
30
開機管理員 (EFI)
24
BitLocker
動態界限
INT 1Ah TCG 介面
INT 9h 鍵盤介面
INT 13h 區塊裝置介面
TPM MP 驅動器
HID 驅動器
裝置 驅動器
USB 堆疊
EFI
區塊裝置 模擬器
14
區塊裝置 驅動器
16
生物辨識裝置
18
TPM
HID 驅動器
USB 磁碟
26

第 4 圖

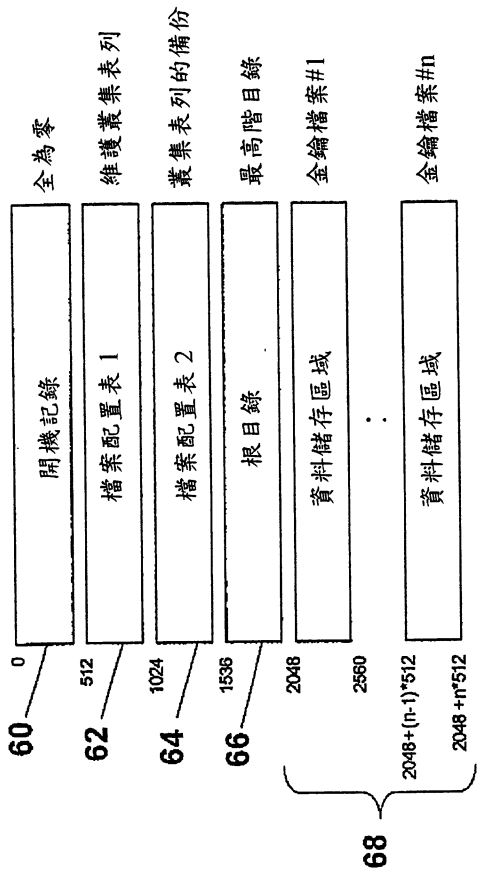
200821931



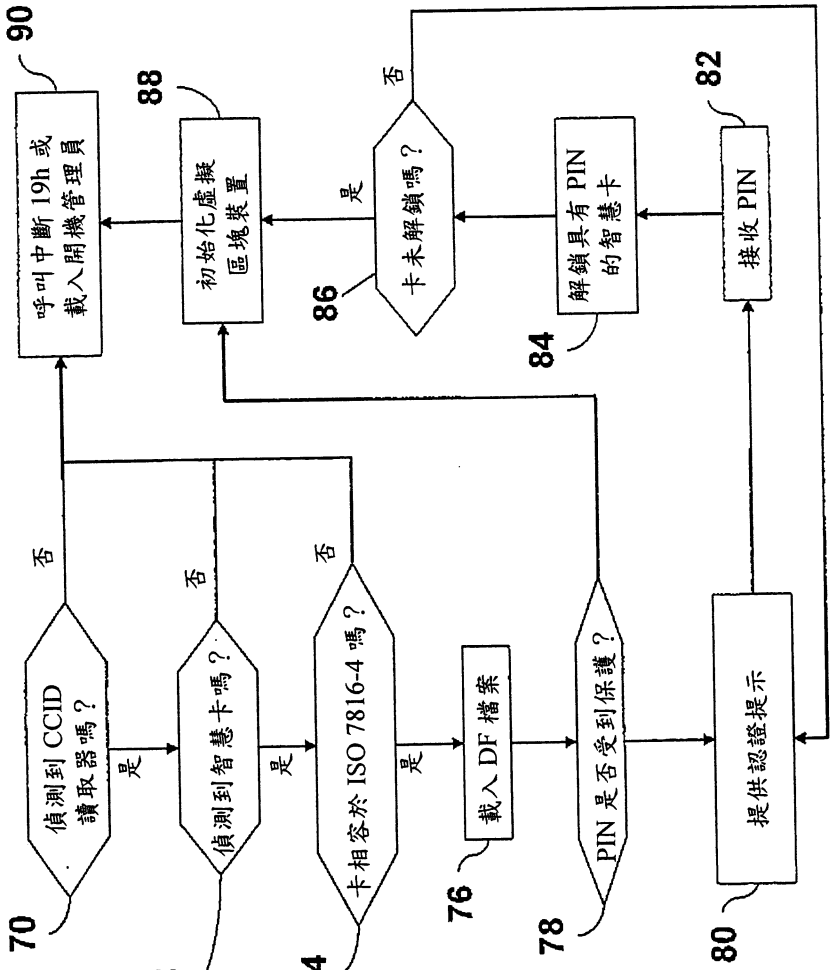
第 5 圖


40
配置平台記憶體及啟始系統結構
42
載入 MF
44
遞迴性搜尋具有 ID VFAT 之 EF
否
46
找到具有 VFAT 之 EF
是
48
載入 EF
50
解析 EF
52
擷取資訊(金鑰)
54
加入擷取的資訊(金鑰)到虛擬區塊裝置
56
是否還有 EF
是
否
58
釋放未使用的資源

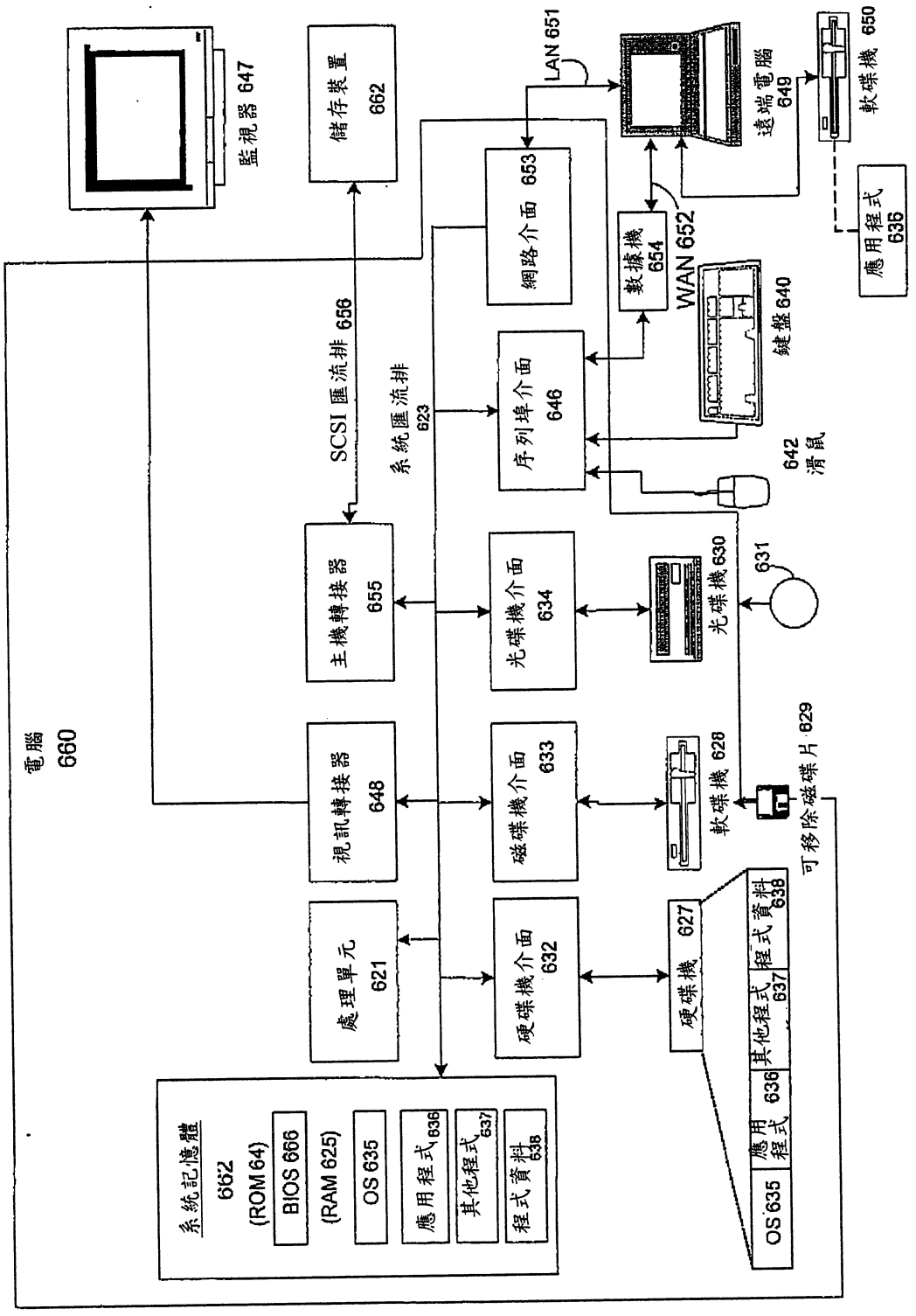
第 6 圖


0
512
1024
1536
2048
2560
2048+(n-1)*512
2048 +n*512
60
62
64
66
68
開機記錄
檔案配置表 1
檔案配置表 2
根目錄
資料儲存區域
資料儲存區域
全為零
維護叢集表列
叢集表列的備份
最高階目錄
金鑰檔案#1
金鑰檔案#n

第 7 圖


偵測到 CCID 讀取器嗎？
70
是
否
偵測到智慧卡嗎？
72
是
否
卡相容於 ISO 7816-4 嗎？
74
是
否
載入 DF 檔案
76
PIN 是否受到保護？
78
是
否
提供認證提示
80
接收 PIN
82
解鎖具有 PIN 的智慧卡
84
卡未解鎖嗎？
86
是
否
初始化虛擬區塊裝置
88
呼叫中斷 19h 或載入開機管理員
90

第 8 圖


電腦
660
監視器 647
儲存裝置
662
LAN 651
遠端電腦
649
軟碟機 650
應用程式
635
網路介面 653
數據機
654
WAN 652
鍵盤 640
642
滑鼠
SCSI 匯流排 656
系統匯流排
623
序列埠介面
646
主機轉接器
655
光碟機介面
634
光碟機 630
631
視訊轉接器
648
磁碟機介面
633
軟碟機 628
可移除磁碟片 629
處理單元
621
硬碟機介面
632
硬碟機 627
系統記憶體
662
(ROM 64)
BIOS 666
(RAM 625)
OS 635
應用程式 636
其他程式 637
程式資料 638
OS 635
應用程式 636
其他程式 637
程式資料 638

第 9 圖

七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖。

(二)、本代表圖之元件代表符號簡單說明：

12	系統	20	BIOS 部分
14	區塊裝置模擬器	22	開機管理員
16	區塊裝置驅動器	24	BITLOCKER™ 軟體
18	智慧卡		

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無