(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 201003457 A1
(43)公開日： 中華民國 99 (2010) 年 01 月 16 日

(21)申請案號：098116598 (22)申請日： 中華民國 98 (2009) 年 05 月 19 日
(51)Int. Cl.： *G06F21/22 (2006.01)*
(30)優先權：2008/05/21 美國 12/124,456
2008/05/21 美國 12/124,450
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
(72)發明人：顏美 YAN, MEI (CN) ；楊杰浩 YANG, CHIEH HAO (TW) ；卡瓦蜜 巴曼 QAWAMI, BAHMAN (US) ；沙貝特 沙爾西 法西德 SABET-SHARGHI, FARSHID (US) ；德懷爾 帕崔西亞 DWYER, PATRICIA (US) ；元波 YUAN, PO (US)
(74)代理人：黃章典；樓穎智
申請實體審查：無 申請專利範圍項數：43 項 圖式數：20 共 74 頁

(54)名稱

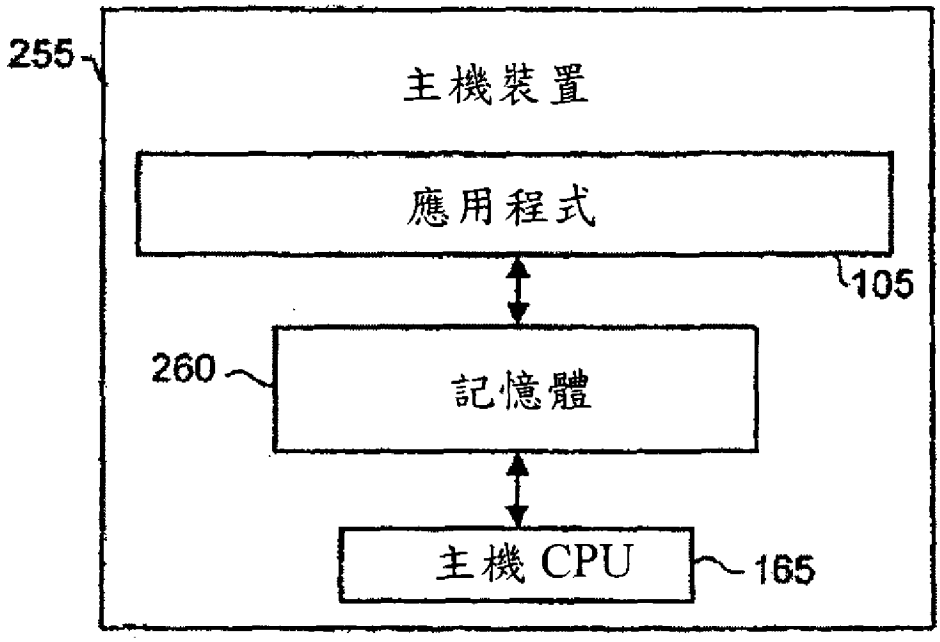
對於周邊裝置的軟體開發套件之存取鑑認

AUTHENTICATION FOR ACCESS TO SOFTWARE DEVELOPMENT KIT FOR A PERIPHERAL DEVICE

(57)摘要

用於一周邊裝置之一程式碼集係安裝於一主機裝置上。該程式碼集係用於自該主機裝置控制對該周邊裝置之存取。該程式碼集亦含有一個或多個程式碼子集，該一個或多個程式碼子集可由該主機裝置上之軟體實體用來存取該周邊裝置。必須藉由安裝於一主機裝置上之該程式碼集成功鑑認該主機裝置上之一軟體實體。一旦成功鑑認該軟體實體，則該程式碼集將提供對該軟體實體特有之該一個或多個程式碼子集之存取。該一個或多個程式碼子集可由該軟體實體用來存取該周邊裝置。

105：應用程式
165：主機 CPU
255：主機裝置
260：記憶體



(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 201003457 A1
(43)公開日： 中華民國 99 (2010) 年 01 月 16 日

(21)申請案號：098116598 (22)申請日： 中華民國 98 (2009) 年 05 月 19 日
(51)Int. Cl.： *G06F21/22 (2006.01)*
(30)優先權：2008/05/21 美國 12/124,456
2008/05/21 美國 12/124,450
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
(72)發明人：顏美 YAN, MEI (CN) ；楊杰浩 YANG, CHIEH HAO (TW) ；卡瓦蜜 巴曼 QAWAMI, BAHMAN (US) ；沙貝特 沙爾西 法西德 SABET-SHARGHI, FARSHID (US) ；德懷爾 帕崔西亞 DWYER, PATRICIA (US) ；元波 YUAN, PO (US)
(74)代理人：黃章典；樓穎智
申請實體審查：無 申請專利範圍項數：43 項 圖式數：20 共 74 頁

(54)名稱

對於周邊裝置的軟體開發套件之存取鑑認

AUTHENTICATION FOR ACCESS TO SOFTWARE DEVELOPMENT KIT FOR A PERIPHERAL DEVICE

(57)摘要

用於一周邊裝置之一程式碼集係安裝於一主機裝置上。該程式碼集係用於自該主機裝置控制對該周邊裝置之存取。該程式碼集亦含有一個或多個程式碼子集，該一個或多個程式碼子集可由該主機裝置上之軟體實體用來存取該周邊裝置。必須藉由安裝於一主機裝置上之該程式碼集成功鑑認該主機裝置上之一軟體實體。一旦成功鑑認該軟體實體，則該程式碼集將提供對該軟體實體特有之該一個或多個程式碼子集之存取。該一個或多個程式碼子集可由該軟體實體用來存取該周邊裝置。

六、發明說明：

【發明所屬之技術領域】

本發明係關於用於安全周邊裝置之技術。

【先前技術】

防止對安全周邊裝置之未經授權存取已隨著技術發展而成為一更需要關注的問題。安全周邊裝置之一實例可係記憶體裝置，例如含有必須保護以免受到未經授權使用之安全內容之記憶體裝置。

半導體記憶體愈來愈普遍地用於各種電子裝置中。舉例而言，非揮發性半導體記憶體可用於蜂巢式電話、數位相機、行動媒體播放器、個人數位助理、行動計算裝置、非行動計算裝置及其他裝置中。

保護儲存於非揮發性半導體記憶體裝置上的內容已成為一重要特徵，尤其涉及對受版權保護的材料之保護。舉例而言，一使用者可經由一電子裝置來購買受版權保護的內容，例如音樂。內容擁有者通常打算僅購買者使用該內容且可能要求所購買內容僅由一電子裝置上之經授權應用程式(例如用於購買該內容之應用程式)來播放。

安全地儲存用於保護以防對安全內容之未經授權使用之資訊可使用各種各樣的保護技術(例如加密)來實行。試圖存取加密內容之一裝置上之一應用程式在可讀取彼內容之前必須使用一加密密鑰來解密該內容。一授權存取該加密內容之應用程式將具有用於解密該內容之適當加密密鑰。未經授權應用程式仍可能能夠存取該加密內容，但沒有適

當加密密鑰，未經授權應用程式可能無法讀取該內容。然而，若一應用程式獲得該加密密鑰，則該未經授權應用程式將能夠讀取該受保護內容。需要一種用於防止一電子裝置上之一未經授權應用程式存取一安全周邊裝置上之受保護內容之改良、簡化及安全方法。

【發明內容】

本文中所述之技術係關於對一主機裝置上之一應用程式、應用程式啟動程序或其他軟體實體之鑑認以防止對一安全周邊裝置之未經授權存取。該軟體實體係使用任一鑑認機制藉由該主機裝置上的程式碼集來加以鑑認。該程式碼集與該周邊裝置相關聯且安裝於該主機裝置上以控制對該周邊裝置之存取。該程式碼集亦含有該主機裝置上之軟體實體可用於實行與該周邊裝置相關聯之任務的程式碼。一旦成功鑑認該軟體實體，則該程式碼集將使該軟體實體可用於實行與該周邊裝置相關聯之任務的程式碼可供該軟體實體使用。

一項實施例包括一種涉及將與一安全周邊裝置相關聯的一程式碼集安裝於一主機裝置上之處理程序，其中該程式碼集包括用於該主機裝置上運作該周邊裝置的程式碼，例如用於一裝置驅動程式的程式碼。該程式碼集用於鑑認該主機裝置上之一第一軟體實體。該處理程序進一步包括若成功鑑認該第一軟體實體則將該程式碼集曝露於該第一軟體實體，包括曝露允許該第一軟體實體與該周邊裝置通信的程式碼。

一鑑認處理程序之一項實施例包括在一主機裝置上之一第一軟體實體處自一使用者接收與一安全周邊裝置相關聯之一第一任務請求。自該第一軟體實體發送一憑證至一安裝於該主機裝置上以用於該周邊裝置的程式碼集。該處理程序進一步包括若該憑證有效則存取該程式碼集之一部分，包括存取允許該第一軟體實體實行與該第一軟體實體相關聯的該第一任務之程式碼。該程式碼集包括允許該主機裝置上之一個或多個軟體實體實行與該周邊裝置相關聯之任務的程式碼。該第一軟體實體使用該程式碼集之該部分來發送與該第一任務相關聯之資訊。

一鑑認處理程序之一項實施例包括當該第一軟體實體請求存取一周邊裝置時發送一個或多個鑑認選項至一主機裝置上之一第一軟體實體。該一個或多個鑑認選項係自一安裝於該主機裝置上以用於該周邊裝置的程式碼集發送至該第一軟體實體。該程式碼集包括與該主機裝置上之一個或多個軟體實體相關聯的程式碼。該程式碼集自該第一軟體實體接收一憑證。該憑證與該一個或多鑑認選項中之一者相關聯。該處理程序進一步包括若該憑證有效則提供對與該第一軟體實體相關聯之第一程式碼之存取。該第一程式碼允許對該周邊裝置之存取且係該程式碼集之一部分。

一項實施例包括一安全周邊裝置及與該安全周邊裝置通信之一主機裝置。該主機裝置包括控制對該周邊裝置之存取之一個或多個處理器。該一個或多個處理器亦藉由控制對一安裝於該主機裝置上以用於該周邊裝置的程式碼集之

存取來管理該程式碼集，其中該程式碼集允許該周邊裝置與該主機裝置上之一個或多個軟體實體之間的通信。該一個或多個處理器驗證來自該主機裝置上之一第一軟體實體之一憑證且若該憑證有效則將該程式碼集中之一程式碼子集曝露於該第一軟體實體，其中該程式碼子集與該第一軟體實體相關聯。

一項實施例包括一密碼編譯引擎及與該密碼編譯引擎通信之一主機裝置上之一個或多個處理器。該密碼編譯引擎驗證來自該主機裝置上之一第一軟體實體之一憑證。該一個或多個處理器截取對一安全周邊裝置之存取。該一個或多個處理器亦自該第一軟體實體接收該憑證且若該憑證有效則曝露與該第一軟體實體相關聯的程式碼。當該一個或多個處理器執行該程式碼時，該一個或多個處理器允許該第一軟體實體存取該周邊裝置。

一項實施例包括分別具有處理器可讀程式碼之一個或多個處理器可讀媒體，其中該處理器可讀程式碼致使該一個或多個處理器實行一方法。該方法包括當該第一軟體實體請求存取一周邊裝置時，發送一個或多個鑑認選項至一主機裝置上之一第一軟體實體，包括自一安裝於該主機裝置上以用於該周邊裝置的程式碼集發送一個或多個鑑認選項至該第一軟體實體，其中該程式碼集包括與該主機裝置上之一個或多軟體實體相關聯的程式碼。該程式碼集自該第一軟體接收一憑證。該憑證與該一個或多個鑑認選項中之一者相關聯。該方法進一步包括若該憑證有效則提供對與

該第一軟體實體相關聯之第一程式碼之存取。該第一程式碼允許對該周邊裝置之存取且係該程式碼集之一部分。

【實施方式】

所揭示技術藉由在一主機裝置上實施安全特徵來提供對一周邊裝置之安全存取。一周邊裝置可係任一藉由一主機裝置來運作之裝置，例如一記憶體裝置、一印表機、一鍵盤、等等。該周邊裝置之軟體必須安裝於該主機裝置上以便在該主機裝置上運作該周邊裝置。此軟體係一軟體開發套件(SDK)之一程式碼集，例如一動態連結程式庫(DLL)或一靜態程式庫(LIB)，其安裝於該主機裝置上以藉由該主機裝置上之一個或多個軟體實體或應用程式來運作該周邊裝置。在許多情況下，該主機裝置上之不同應用程式將端視例如應用程式類型、應用程式之功能及應用程式之授權而需要不同之API(應用程式介面)來存取該周邊裝置。當一使用者藉由一應用程式來發送一任務請求至該主機裝置且該任務請求涉及對該周邊裝置之存取時，該周邊裝置之SDK將鑑認該應用程式並驗證該應用程式經授權存取該周邊裝置。若該鑑認成功，則該SDK將僅曝露彼具體應用程式之彼等API。該SDK將不曝露該應用程式未經授權存取之API。該應用程式可使用彼應用程式特有之所曝露API來發送並實行該任務請求。此提高該周邊裝置之安全性且防止對其他應用程式之API之未經授權存取。

圖1繪示在安裝一周邊裝置之一SDK的程式碼集之前一主機裝置255之一項實例。主機裝置255具有一應用程式

105、記憶體260、及一主機CPU 165。主機裝置100可係任一電子裝置，例如一蜂巢式電話、一PC、一數位相機、行動媒體播放器、個人數位助理、行動計算裝置、非行動計算裝置及其他裝置。應用程式105可係用於一主機裝置上之任一軟體實體，例如一日曆、文件瀏覽器、媒體播放器、等等。應用程式105亦可係用於啟動一應用程式之任一軟體。記憶體260可係一主機裝置255可能需要之任一類型之記憶體。主機CPU 165可係用於運作主機裝置255之任一類型之處理器。

當由將經由一主機裝置(例如圖1中所繪示之主機裝置255)來運作之一周邊裝置之一軟體開發者創建一SDK時，該可針對將需要存取該周邊裝置之該主機裝置上的每一軟體實體或應用程式來組態SDK軟體。在許多情況下，可由具有各種需要及偏好之一特定客戶擁有或創建主機裝置上之軟體實體。SDK可基於每一軟體實體/應用程式或客戶需要及偏好(例如授權偏好或客戶應用程式之功能)來組態。圖2係一種用於基於不同應用程式及/或客戶需要及偏好來組態一SDK之一程式碼集之處理程序之一流程圖。在步驟190中，每一應用程式及/或客戶特有之SDK軟體將由SDK軟體開發者基於應用程式及/或客戶之具體要求來組態。舉例而言，用於經由一客戶應用程式來存取一周邊裝置之SDK之程式碼集通常需要一API來介接該應用程式與該周邊裝置。用於存取該應用程式之此等API之SDK軟體可具體基於客戶偏好來組態，例如組態該SDK以要求在存取該

周邊裝置之前進行應用程式鑑認，舉例而言。該SDK經組態以確定每一應用程式將需要存取哪些API。在步驟195中，用於運作該周邊裝置之SDK軟體將基於在步驟190中所實行之每一應用程式/客戶特有之SDK軟體之所需API來組態。此可包括(例如)對每一應用程式/客戶所要求之任何安全特徵所需之任一SDK軟體修改。一旦用於運作該周邊裝置之SDK軟體經組態，則該SDK將使用在步驟190中針對每一應用程式及/或客戶組態之所有軟體(例如鑑認所要求之安全軟體)及在該主機裝置上運作該周邊裝置所需之任何其他軟體(包括在步驟195中所定製之軟體)來正確地起作用。

圖3繪示一已根據圖2中所描述之處理程序組態之周邊裝置SDK 330之一程式碼集之一項實例。周邊裝置SDK 330包括例如安全層125之程式碼子集、應用程式1-3之API及一裝置驅動程式140。該SDK的該等程式碼集可係一動態連結程式庫(DLL)或一靜態程式庫(LIB)。安全層125包括用於鑑認企圖存取該周邊裝置之不同應用程式之軟體。安全層125可係如在圖2之步驟195中所闡述組態之SDK軟體之一部分。舉例而言，安全層125可在應用程式1 262之API需要額外鑑認特徵之情況下組態。稍後將更詳細地闡述安全層125。應用程式1-3之API係每一應用程式必須用來與該周邊裝置通信之API。此等API可如在圖2之步驟190中所述基於客戶對每一應用程式之偏好來組態。舉例而言，應用程式1 262的API可係針對圖1之主機裝置255中之

應用程式105所定製之API。裝置驅動程式140係允許周邊裝置在主機上正確地運作之軟體。

圖4係一描述一個用於將圖3中所示之SDK安裝於一主機裝置上之處理程序之流程圖。在圖4之步驟170中，將該安全周邊裝置連接至該主機裝置。當該安全周邊裝置連接至該主機裝置時，將用於運作該安全周邊裝置之SDK載入並安裝至該主機裝置上(步驟175)。此SDK可儲存於記憶體中以用於該安全周邊裝置。該SDK含有用於程式化該主機裝置上之主機CPU以運作該安全周邊裝置從而防止未經授權存取之軟體。一旦該SDK程式碼集正確地載入並安裝至該主機裝置上，則可藉由該安全周邊裝置來運作該主機裝置(步驟180)。

應注意，在一些實施例中，步驟175僅在一特定安全周邊裝置連接至該主機裝置之第一時間期間對該特定安全周邊裝置實行。一旦該SDK在一安全周邊裝置之第一連接期間安裝於該主機裝置上，則此特定周邊裝置之SDK不需要每當其重新連接至該主機裝置時再次安裝。在其他實施例中，該SDK每當該安全周邊裝置連接至該主機裝置時載入並安裝。

在一項實施例中，用於運作該安全周邊裝置之SDK係在該作業系統安裝於該主機裝置上之前載入並預安裝於該主機裝置上。在此種情況下，該SDK可藉由經由該作業系統來激活或選擇其來使用。因此，步驟175不需要實施為圖4之處理程序之一部分。在另一實施例中，用於運作該周邊

裝置之SDK在安裝該主機裝置之作業系統之後載入並預安裝於該主機裝置上。同樣，在此種情況下，步驟175不需要實施為圖4之處理程序之一部分。

圖5顯示在安裝圖3之SDK 330的程式碼集之後主機裝置255與安全周邊裝置145之一項實施例。主機裝置255包括圖1中所示之原始組件(應用程式105、記憶體260及主機CPU 165)以及圖3中所示之SDK 330之組件(安全層125、應用程式1-3之API及裝置驅動程式140)。當主機裝置255之一使用者藉由應用程式105來請求一涉及安全周邊裝置145之任務時，安全層125將致使主機CPU 165鑑認應用程式105。若藉由安全層125成功鑑認應用程式105，則該安全層將曝露應用程式105特有之API子群組，例如應用程式1 262之API，假若應用程式105係應用程式1。應用程式105然後可使用該SDK程式碼之彼子集藉由裝置驅動程式140來發送該任務請求至安全周邊裝置145。應用程式105亦可使用彼等API來實行該使用者之該任務請求。

為了更具體地闡述經由一周邊裝置之一SDK來安全地存取該周邊裝置，將使用一安全記憶體裝置作為一周邊裝置之一實例。然而，應注意，該周邊裝置可係任一周邊裝置而不僅限於下文所述之一記憶體裝置之該實例。

圖6顯示在安裝一安全記憶體裝置之一SDK之前一主機裝置100中之組件之一項實施例。通常，一主機裝置100之一使用者經由一軟體實體(例如一應用程式105)來存取儲存於主機裝置100上的內容。主機裝置100上之應用程式之實

例包括保存於主機裝置100上之媒體播放器、日曆、通訊錄、等等。一應用程式亦可係該主機裝置上之可執行程式碼，其用於啟動一儲存於主機裝置100上之一不同於可執行程式碼之位置中之應用程式(即，媒體播放器、日曆、通訊錄、等等)。舉例而言，一應用程式可用於啟動一媒體播放器應用程式，該媒體播放器應用程式保存於該主機裝置內一不同記憶體部分中以用於主機裝置100或保存於一連接至主機裝置100之周邊裝置上。使用一應用程式105來存取或保存之內容可包括諸如應用程式、媒體、排程資訊或接觸資訊等內容。

應用程式105使用主機裝置100之作業系統上之一主機儲存管理器110來存取或儲存主機裝置100或任何其他周邊裝置(例如一可抽換式記憶體裝置)上的內容。主機儲存管理器110係該作業系統上之一軟體組件，其控制主機裝置100之存取及儲存功能，包括主機裝置100內及任何周邊裝置之間的存取及儲存，如下文中將更詳細解釋。

圖6亦顯示主機儲存管理器110及主機檔案系統130，主機檔案系統130係一由主機儲存管理器110管理之組件。主機儲存管理器110使用主機CPU 165來存取主機檔案系統130。主機檔案系統130儲存於主機裝置100上之記憶體中且用於定位並儲存儲存於主機裝置100上或任何周邊裝置中的內容。當一使用者向主機裝置100請求內容時，主機儲存管理器110將使用主機檔案系統130來定位該內容。當一使用者請求儲存彼內容時，主機儲存管理器110將使用

主機檔案系統130來將該內容儲存於適當位置中。

另外，儲存於主機裝置100上之內容可出於保護而加密。該主機裝置可含有一主機密碼編譯引擎185，該主機密碼編譯引擎可具有一隨機數產生器及一密碼編譯處理器，該隨機數產生器及該密碼編譯處理器可支援若干加密方法，例如對稱加密(即，AES、DES、3DES、等等)、密碼編譯雜湊函式(即，SHA-1、等等)、非對稱加密(PKI、密鑰對產生、等等)、或任何其他密碼編譯方法。

圖7顯示在周邊裝置SDK 330之程式碼集正確地載入並安裝於主機裝置100上之後與一安全記憶體裝置145共同運作之主機裝置100之一項實例。在一項實施例中，該安全周邊裝置係一可抽換式儲存裝置，其用於儲存可儲存於該安全記憶體裝置之一安全分割區中或者可儲存於該安全記憶體裝置之一公用分割區中的內容 該安全記憶體裝置可係任一類型之記憶體裝置，例如一大容量儲存裝置、一非揮發性快閃記憶體裝置、等等。該安全記憶體裝置保護以防對儲存於該安全記憶體裝置之該安全分割區中之內容之未經授權存取。若儲存於該安全記憶體裝置之該公用分割區中的內容受保護，則該安全記憶體裝置亦可保護以防對該內容之未經授權存取。若內容經加密，則該內容在該安全記憶體裝置中受保護。若內容未經加密且儲存於一公用分割區中，則該內容在該安全記憶體裝置中不受保護。若一主機裝置具有與內容相關聯之適當授權，例如允許加密或解密該內容之授權，則該主機裝置可存取並儲存該安全記

憶體裝置上的內容。

在圖7中，主機裝置100經由實體介面142實體連接至安全記憶體裝置145。應用程式105、主機CPU 165、主機裝置密碼編譯引擎185、主機儲存管理器110及主機檔案系統130係如圖6中所示之主機裝置100上的軟體組件。周邊裝置SDK 330係安裝於主機裝置100上的程式碼集且用於藉由主機裝置100來運作安全周邊裝置145。周邊裝置SDK 330使用安全周邊裝置API 120、周邊裝置SDK安全層125、主機檔案系統130、註冊表285、SDK密碼編譯程式庫168及安全檔案系統135來管理對安全記憶體裝置145之內容存取及儲存。安全周邊裝置API 120、周邊裝置SDK安全層125、註冊表285、SDK密碼編譯程式庫168、安全檔案系統135及裝置驅動程式140係軟體組件，其如圖4之步驟175中所述自安全記憶體裝置145之SDK之程式碼集載入並安裝於該主機裝置上。開放通道150及安全通道155係用於在主機裝置100與安全記憶體裝置145之間傳送內容之資料匯流排。

安全記憶體裝置145使用安裝於主機裝置100上以用於安全記憶體裝置145之軟體來控制對內容之存取及儲存。該軟體包括圖2之步驟175中所述之程式庫或其等可係預安裝於該主機裝置上之程式庫。載入並安裝於該主機裝置上之SDK程式庫可係動態連結程式庫(DLL)或靜態程式庫(LIB)，其等可整合至該主機裝置上之作業系統中。該SDK之程式碼集提供至用於安全運作安全記憶體裝置145之主

機儲存管理器110中之掛接。舉例而言，該周邊裝置SDK之程式碼集中的程式碼子集可插入於用於調用主機檔案系統130之調用鏈中以便該程式碼致使主機CPU 165控制如何存取並儲存內容。在圖7中，周邊裝置SDK安全層125、安全周邊裝置API 120、安全檔案系統135、註冊表285、SDK密碼編譯程式庫168及裝置驅動程式140係程式碼子集，其使用一安裝於主機裝置100上之裝置驅動程式140經由該安全周邊裝置SDK之程式碼集提供至該主機裝置。

一使用者可經由一軟體實體(例如一主機裝置上之一應用程式105)來存取儲存於安全記憶體裝置145中的內容，如圖7中所示。針於儲存於安全周邊裝置145中之受保護內容，需要在應用程式105可存取該內容之前首先鑑認應用程式105，如地下文中更詳細闡述。

應用程式105使用該主機裝置上之作業系統上之主機儲存管理器110來存取或儲存安全記憶體裝置145中的內容。主機儲存管理器110控制對該主機裝置之存取及儲存功能，包括該主機裝置及安全記憶體裝置145內之存取及儲存。

通常，主機儲存管理器110使用該主體裝置之作業系統上之一主機檔案系統130來控制對該主機裝置或任何周邊裝置之存取及儲存功能，如圖6中所述。主機檔案系統130可係任一標準檔案系統，例如FAT12、FAT16、FAT32、NTFS、等等。然而，針對安全記憶體裝置145，安全記憶體裝置145之周邊裝置SDK 330使用一周邊裝置SDK安全層

125以藉由使用安全記憶體裝置145之一安全檔案系統135來控制對該主機裝置之存取及儲存功能。對安全檔案系統135之存取係藉由鑑認應用程式105且一旦成功鑑認則允許僅存取應用程式105特有之API來加以控制。此等API允許對安全檔案系統135之適當介接。安全檔案系統135安裝於主機裝置100上以用於安全記憶體裝置145且係儲存於安全記憶體裝置145中的內容之檔案系統。安全檔案系統135可係任一標準檔案系統，例如FAT12、FAT16、FAT32、NTFS、等等。

周邊裝置SDK安全層125之軟體載入並安裝為在圖2之步驟175中所載入並安裝之SDK之一部分。周邊裝置SDK安全層125致使主機CPU 165鑑認應用程式105。在成功鑑認應用程式105之後，應用程式105將註冊於註冊表285中。周邊裝置SDK安全層125亦提供一應用程式控制代碼(handler)至應用程式105。該應用程式控制代碼指示允許應用程式105存取哪些API。關於由周邊裝置SDK安全層125實行之鑑認及註冊處理程序之更詳細說明將闡述於下文中。

當一使用者經由一應用程式105來請求存取內容時，周邊裝置SDK安全層125將提供在成功鑑認之後自安全周邊裝置145存取該內容所需之適當API，例如安全周邊裝置API 120。使用所存取API，應用程式105可藉由存取與該內容相關聯之權限來接收儲存於安全周邊裝置145中之內容。針對受保護內容，標頭與該內容一同儲存且含有與該

內容相關聯之資訊(例如與用於加密並解密該內容之內容加密密鑰(CEK)相關之域資訊)及可指示儲存何種類型之內容之內容元資料。

周邊裝置SDK 330中之安全周邊裝置API(應用程式介面)120用於在存取或儲存內容時介接安全周邊裝置145與應用程式105。安全周邊裝置API 120係安裝之SDK之一部分且可在成功鑑認應用程式105時由應用程式105調用。安全周邊裝置API 120係周邊裝置SDK安全層125與安全檔案系統135之間的介面橋接器。

一旦使用主機檔案系統130或安全檔案系統135中的任何一者來定位該內容或將該內容歸檔，則可使用該主機裝置上之裝置驅動程式140來存取該內容或將取該內容儲存於安全記憶體裝置145上適當位置中。此係經由實體連接主機裝置100與安全記憶體裝置145之實體介面142來實行。可使用一安全通道155或一開放通道150來存取或儲存該內容。周邊裝置SDK 330確定是否應使用一安全通道155或一開放通道150來在安全周邊裝置145與該主機裝置之間傳送該內容。

當一使用者經由應用程式105來請求儲存應不受保護之內容時，周邊裝置SDK 330將使用主機檔案系統130來儲存該內容。若該使用者請求儲存應在安全周邊裝置145中受保護之內容，則周邊裝置SDK 330將使用安全檔案系統135來儲存該內容。

周邊裝置SDK 330中之安全周邊裝置API(應用程式介

面)120用於在存取或儲存受保護內容時介接安全周邊裝置145與應用程式105。安全周邊裝置API 120係安裝之SDK之一部分且可在成功鑑認應用程式105時由應用程式105調用。安全周邊裝置API 120係周邊裝置SDK安全層125與安全檔案系統135之間的介面橋接器。

一旦使用主機檔案系統130或安全檔案系統135中的任何一者來定位該內容或將該內容歸檔，則可使用該主機裝置上之裝置驅動程式140來存取該內容或將取該內容儲存於安全周邊裝置145上適當位置中。此係經由實體連接主機裝置100與安全記憶體裝置145之實體介面142來實行。可使用一安全通道155或一開放通道150來存取或儲存該內容。周邊裝置SDK安全層125確定是否應使用一安全通道155或一開放通道150來在安全周邊裝置145與該主機裝置之間傳送該內容。

一會期密鑰係一加密密鑰，其用於在該主機與該安全記憶體裝置之間傳送內容之前加密該內容。若不需要經由一安全通道來傳送內容，則可不存在與該內容相關聯之會期密鑰，或與彼內容相關聯之會期密鑰可指示不需要加密。

若該內容與一指示應使用一安全通道155來傳送該內容之會話密鑰相關聯，則將在經由安全通道155來傳送該內容之前使用該會期密鑰來加密該內容。一旦傳送該經加密內容，則將使用相同之會期密鑰來解密該內容。該內容係使用SDK密碼編譯程式庫168在主機裝置100上加密或解密。SDK密碼編譯程式庫168含有一隨機數產生器及用於

加密之密碼編譯函式，例如對稱加密(即，AES、DES、3DES、等等)、密碼編譯雜湊函式(即，SHA-1、等等)、不對稱加密(PKI、密鑰對產生、等等)、或任何其他密碼編譯方法。安全周邊裝置145具有用於在傳送內容之前或之後在安全記憶體裝置145上加密之其自帶密碼編譯引擎，如將針對圖11更詳細解釋。若該會期密鑰指示應使用一開放通道150來傳送該內容，則傳送該內容而不加密該內容。

針對未安裝有該周邊裝置SDK之主機裝置，該主機裝置可能能夠存取儲存於一公用分割區中之內容。若該內容受保護，則儘管該裝置可能能夠存取該內容，但若該內容經加密則將不能正確讀取該內容。若該內容儲存於一安全分割區中，則該裝置無法存取該內容。

圖8顯示當該周邊裝置係一安全記憶體裝置時含於安裝於主機裝置100上之周邊裝置SDK 330中之軟體之一實例，如圖7中所示。同樣，該周邊裝置不僅限於一記憶體裝置之該實例。周邊裝置SDK 330係安裝於主機裝置100上之程式庫且含有用於在主機裝置100上運作安全記憶體裝置145之軟體，例如周邊裝置API 260、周邊裝置SDK安全層125、裝置驅動程式140、安全檔案系統135、SDK密碼編譯程式庫168及註冊表285。然而，周邊裝置SDK 330不僅限於此軟體。

應用程式API 260係由任一應用程式(例如圖7中之應用程式105) 使用之API。此等API包括用於鑑認之API，且其

等亦包括用於一旦成功鑑認一應用程式則介接該應用程式與安全檔案系統135以存取安全記憶體裝置145上之內容的API，如圖7中之安全周邊裝置API 120。應用程式API 260可含有彼特定應用程式特有之API。舉例而言，一由一個應用程式使用之API不可由另一個應用程式使用。經由周邊裝置SDK安全層125成功鑑認之一應用程式可經由一安全周邊裝置API 120存取安全記憶體裝置145中之受保護內容。下文針對圖12詳細闡述安全周邊裝置API 120。

如圖7中所示，周邊裝置SDK安全層125安裝於該主機裝置上以提供至主機儲存管理器110中之掛接並致使主機CPU 165控制如何存取並儲存安全記憶體裝置145上的內容。周邊裝置SDK安全層125的程式碼「劫持」主機裝置100上的主機檔案作業以使一應用程式能夠在存取安全周邊裝置145上的內容之前鑑認該應用程式。

如圖7中所示，裝置驅動程式140之軟體可在安全記憶體裝置145連接至主機裝置100之後載入並安裝於該主機裝置上(圖4之步驟175)或者在該作業系統安裝於該主機裝置上之前或之後預安裝於主機裝置100之作業系統上。

安全檔案系統135係含有用於存取並儲存安全記憶體裝置145中的內容之歸檔資料之檔案系統，如圖7中所圖解闡釋。

SDK密碼編譯程式庫168係含有可用於加密或解密一安全通道155之內容之密碼編譯方案的程式庫。該等密碼編譯方案可係任何已知方案，例如AES、DES、3DES、SHA-

1、PKI、密鑰對產生、等等。SDK密碼編譯程式庫168將基於與內容相關聯之權限(例如一會期密鑰)來加密或解密該內容。

註冊表285係由周邊裝置SDK安全層125用來管理並保持應用程式鑑認狀態及相關資訊的表。該表可含有諸如鑑認演算法、應用程式ID、註冊時間、到期時間、註冊狀態等資訊。關於註冊表285之更詳細說明將闡述於下文中。

繼續闡述一安全記憶體裝置之該實例，圖9繪示圖7中所示之安全周邊裝置145之一項實施例。安全周邊或記憶體裝置145含有一韌體模組210、一CPU 220、一周邊裝置密碼編譯引擎160及一系統分割區400。系統分割區400含有公用分割區240及安全分割區250。韌體模組210使用CPU 220來存取並儲存系統分割區400之公用分割區240或安全分割區250中的內容。記憶體裝置密碼編譯引擎160用於加密或解密安全記憶體裝置145內之經存取或儲存之受保護內容。

韌體模組210含有用於控制對安全記憶體裝置145上的安全分割區250及公用分割區240之內容之存取及儲存的硬體及軟體。該韌體模組程式化CPU 220以實行存取及儲存功能，例如確定應自記憶體的哪一部分存取或儲存內容以及是否保護該內容。關於韌體模組210之更詳細說明將闡述於下文對圖10之說明中。

公用分割區240係可由一使用者看到且可由主機裝置100偵測到之安全記憶體裝置145之記憶體分割區。安全記憶

體裝置145可具有一個或多個公用分割區。公用分割區240可含有一使用者或主機裝置100可開放存取之公用內容。公用分割區240亦可儲存使用一內容加密密鑰(CEK)加密之受保護內容。該CEK可使用儲存於含有與內容相關聯之資訊之內容標頭中之域資訊來產生。亦可儲存公用內容而不加密該內容。

安全分割區250係不可由一使用者看到且不可由該主機裝置偵測到之安全記憶體裝置145之隱藏記憶體分割區。安全記憶體裝置145可具有一個或多個安全分割區。安全分割區250可含有不可由該使用者或主機裝置100開放存取之受保護內容。該受保護內容可使用一CEK來加密。儲存於安全分割區250中之內容可由具有用於存取該內容之適當權限之經鑑認應用程式存取。與該CEK相關聯之資訊及與該內容相關聯之權限儲存於含有與該內容相關聯之資訊之內容標頭中。在一項實施例中，系統分割區400之公用分割區240及安全分割區250儲存於一包括一控制器及一個或多個快閃記憶體陣列之快閃記憶體裝置中。

由於安全分割區250係不可由一使用者或該主機裝置偵測到之隱藏分割區，因此安全分割區250可含有用於在主機裝置100上運作安全記憶體裝置145的軟體，包括權利物件、應用程式憑證、等等。

周邊裝置密碼編譯引擎160用於使用周邊記憶體裝置145內之CEK或會期密鑰來加密或解密該內容。記憶體裝置密碼編譯引擎160含有一隨機數產生器及一密碼編譯處理

器，該隨機數產生器及該密碼編譯處理器可支援若干加密方法，例如對稱加密(即，AES、DES、3DES、等等)、密碼編譯雜湊函式(即，SHA-1、等等)、非對稱加密(PKI、密鑰對產生、等等)、或任何其他密碼編譯方法。

圖10繪示韌體模組210之一項實施例之細節。韌體模組210含有一周邊裝置介面模組144、一快閃記憶體管理器310、一受保護內容存取管理器320、一密碼編譯引擎程式庫235及一DRM(數位權利管理)模組315。周邊裝置介面模組144含有用於藉由主機裝置實體介面142來介接安全記憶體裝置145與主機裝置100之硬體及軟體。周邊裝置介面模組144之硬體組件可包括任一類型之介面(例如一通用串列匯流排(USB)、安全數位(SD)或微型快閃(CF)介面)之組件。快閃記憶體管理器310含有致使CPU 220存取或儲存公用分割區240中之不受保護內容且可致使CPU 220使用DRM模組315基於權限來存取或儲存該內容的軟體。受保護內容存取管理器320含有致使CPU 220使用對該受保護內容之權限來存取或儲存受保護內容且可致使CPU 220使用DRM模組315基於該等權限來存取或儲存受保護內容的軟體。受保護內容存取管理器320亦可使用密碼編譯引擎程式庫235，密碼編譯引擎程式庫235儲存使用一會期密鑰或一CEK來加密內容所需之資訊。快閃記憶體管理器310及受保護內容存取管理器320兩者經由該主機裝置上之裝置驅動程式140來存取並儲存該主機裝置之內容。

若不需要保護，則快閃記憶體管理器310使用CPU 220來

控制對安全記憶體裝置145中之不受保護內容之存取及儲存。當經由裝置驅動程式140自主機裝置100接收到一保存不受保護內容之請求時，快閃記憶體管理器310將根據主機檔案系統130來將該內容保存於適當位置中。當藉由裝置驅動程式140經由主機裝置檔案系統130接收到一存取不受保護內容之請求時，快閃記憶體管理器130將使用主機檔案系統130自該適當位置存取該內容。快閃記憶體管理器310亦在應用程式105試圖存取安全記憶體裝置145中之受保護內容時提供對受保護內容存取管理器320之存取。

若需要保護，則受保護內容存取管理器320使用CPU 220來控制對安全記憶體裝置145中之受保護內容之存取及儲存。受保護內容存取管理器320將與受保護內容相關聯之權限儲存至DRM模組315或自DRM模組315擷取與受保護內容相關聯之權限。受保護內容存取管理器320使用圖7中所示之安全檔案系統135來存取或儲存受保護內容。舉例而言，當經由裝置驅動程式140自該主機裝置接收到一保存受保護內容之請求時，周邊裝置SDK安全層125將使用SDK密碼編譯程式庫168以在應經由一安全通道155來發送受保護內容之情況下使用與該內容相關聯之一會期密鑰來加密該內容。經加密內容隨後經由安全通道155發送至安全記憶體裝置145並在安全記憶體裝置145處使用密碼編譯引擎程式庫235中之會期密鑰及適當密碼編譯方案來解密。經解密內容隨後由周邊裝置密碼編譯引擎160使用該內容的一CEK來加密。使用該CEK加密之內容隨後根據安

全檔案系統135來保存於適當位置中。

針對經由一開放通道發送之受保護內容，實行一用於傳送該內容之類似方法，但不對安全通道155進行會期密鑰加密。當經由裝置驅動程式140自主機裝置100接收到一存取受保護內容之請求時，受保護內容存取管理器320將使用安全檔案系統135自適當位置存取該內容並經由一開放通道150將該內容提供至主機裝置100上之主機儲存管理器110。一旦適當權限由受保護內容存取管理器320確定，則受保護內容存取管理器320將經由快閃記憶體管理器310來存取並儲存內容。

受保護內容存取管理器320亦可使用DRM模組315以基於與該內容相關聯之權限(例如(舉例而言)版權權限)來提供對內容之存取。DRM模組315可支援任一特定DRM技術，例如OMA、DRM、MS DRM、等等。

密碼編譯引擎程式庫235含有可用於藉助安全記憶體裝置145內之一CEK或一會期密鑰來加密內容之密碼編譯方案。當應在安全記憶體裝置145中加密或解密內容時，受保護內容存取管理器320將自密碼編譯引擎程式庫235存取適當密碼編譯方案。該等密碼編譯方案可係任何已知方案，例如AES、DES、3DES、SHA-1、PKI、密鑰對產生、等等。

圖11繪示安全記憶體裝置145之一系統分割區400之一實例。系統分割區400包括安全記憶體裝置145中的所有記憶體分割區。換句話說，系統分割區400係由圖9中所示之公

用分割區240及安全分割區250構成。安全記憶體裝置145可具有任一數量之公用或安全分割區。如先前所述，一公用分割區可由一使用者或一主機裝置偵測到並開放存取。儲存於一公用分割區中之不受保護內容可不加鑑認地存取。然而，儲存於一公用分割區中之受保護內容則必須在成功鑑認之後方可存取。一安全分割區係一不可由一使用者或一主機裝置偵測到之隱藏分割區。任何企圖開啟一安全分割區中之內容的應用程式首先必須予以鑑認。

當受保護內容保存至安全記憶體裝置145時，受保護內容存取管理器320根據與該內容相關聯之權限來組織該內容且隨後由快閃記憶體管理器310儲存該內容。公用及安全分割區可具有若干域或邏輯群組，該等域或邏輯群組含有若干具有相同CEK之受保護內容群組。每一域或邏輯群組皆與一個CEK相關聯，該CEK用於自彼域或群組解密內容或將內容加密至彼域或群組。任一具有用於開啟一域或群組內之內容之適當權限的應用程式亦可能能夠開啟儲存於相同之域或群組中之其他內容。

圖11中之公用分割區P0 410含有兩個邏輯群組(域1及域2)。儲存於域1中之所有內容皆將使用一個CEK來加密並解密內容。儲存於域2中之所有內容皆將使用另一個CEK來加密並解密該內容。一企圖存取此等群組中之任何一者的軟體實體將需要在可讀取該內容之前加以鑑認。由於公用分割區P0未隱藏且可開放存取，因此可看到且可能存取含於一群組內之受保護內容但不可讀取該內容，除非使用

適當CEK來正確地解密該內容。因此，有可能一群組中之內容可由一未經授權使用者破壞但不可讀取該內容。

公用分割區P0 410中之檔案A 440不含於一群組內因此其不具有與其相關聯之CEK。因此，任一使用者皆可存取並讀取檔案A 440。

安全分割區P1 420含有檔案E及檔案F。檔案E及檔案F可係任何需要在一安全分割區中加以保護之檔案。舉例而言，檔案E或檔案F可由SDK用來儲存安全資訊，例如內容許可證或任何內部管理資料。然而，安全分割區P1 420不僅限於儲存此等類型之檔案。安全分割區P1 420可儲存任何安全檔案。

安全分割區P2 430含有皆位於域3 490內之檔案G及檔案H。域3與一用於加密並解密該內容之CEK相關聯。舉例而言，若一應用程式企圖存取域3中之檔案G，則首先必須鑑認該應用程式。一旦鑑認該應用程式，則該應用程式可使用域3之CEK來存取檔案G且亦可存取域3內之檔案H。

安全分割區P3 450顯示可用於儲存任一受保護內容之一空分割區。

圖12顯示含於周邊裝置SDK 330中之應用程式API 260之一實例。應用程式API 260包括標準及安全儲存API 340、鑑認API 350、組態API 360、DRM API 370及一使用者可能需要用於運作主機裝置100上之安全記憶體裝置145之任何其他定製API 380。該等不同類型之API中之每一者可係一軟體實體特有的，例如一應用程式或一應用程式啟動程

序105。在一項實施例中，每一應用程式之API皆儲存為一邏輯群組，例如一域。舉例而言，APP 1之API 262儲存成與其他應用程式之API分開之一群組中。在一項實施例中，每一群組僅含有一個應用程式之一種類型之API。舉例而言，APP 1之安全儲存API 262可視為一個群組。

APP 1之API 262顯示整個API群組中係應用程式1特有之API子群組。該SDK經組態以在成功鑑認時允許APP 1之API 262由應用程式1存取(參見圖2，步驟190)。在一項實施例中，APP 1之API 262係該SDK之程式碼集中可由一個或多個不同應用程式調用之程式碼子集。在另一實施例中，APP 1之API 262只可由應用程式1軟體實體調用。APP 1之API 262包括安全儲存API、組態API、DRM API及定製API。然而，APP 1之API 262不僅限於彼等API。

標準及安全儲存API 340含有一應用程式或一應用程式啟動程序105擷取並儲存安全記憶體裝置145上之內容，以建立一安全會期，或實行涉及對安全記憶體裝置145上之內容之存取及儲存之任何其他類型作業所需之API。舉例而言，一標準或安全儲存API 340可係一允許一應用程式105發送一請求用於存取主機檔案系統130或安全檔案系統135之內容之路徑位置的API。應用程式105可在儲存公用內容時從該群組標準及安全API 340中調用一標準API且可在藉由周邊裝置SDK安全層125鑑認應用程式1之後從APP 1之API 262群組中調用一安全API，例如圖7中所示之安全周邊裝置API 120。

鑑認API 350係用於鑑認一應用程式105之API，且其向所有應用程式開放而無需一用於存取鑑認API 350之鑑認處理程序。鑑認API 340由應用程式105調用。當一鑑認API 340由一應用程式105調用時，應用程式105可使用鑑認API 340來發送一憑證至周邊裝置SDK安全層125。周邊裝置SDK安全層125隨後將驗證由應用程式105經由鑑認API 340發送之憑證是否有效。該憑證可係任一類型之用於鑑認一軟體實體之憑證，例如一對一詢問/回應鑑認演算法之回應、一PKI證書、一PIN、一密鑰、一密碼、等等。在詢問/回應鑑認之情況下，鑑認API 350可用於發送一詢問至應用程式105。對該詢問之回應隨後可使用相同之鑑認API 340自應用程式105發送至周邊裝置SDK安全層125。

組態API 360係用於允許應用程式105組態安全記憶體裝置145或擷取關於安全記憶體裝置145之組態之資訊的API。此只有在應用程式105具有這樣做的授權之情況下才可進行。舉例而言，組態API 360可由一具體應用程式105調用以獲得關於安全記憶體裝置145上之已用及空閒記憶體空間之資訊或在成功鑑認應用程式105之後創建一新的安全分割區。

DRM API 370可由應用程式105調用以存取與內容相關聯之權限或數位權利且在該等權利有效之情況下提供對彼內容之存取。對此等權利之確認將在安全記憶體裝置145中之韌體模組210中之DRM模組315中進行。在一項實施例

中，DRM API 370可一如APP 1之API 262子群組中所示之特定應用程式105特有的。

定製API 380可係使用者可能需要用於在主機裝置100中運作安全記憶體裝置145之任何額外API。定製API 380可係一如APP 1之API 262子群組中所示之特定應用程式105特有的。

圖13係一流程圖，其描述在一周邊裝置SDK正確地安裝於一主機裝置上之後如何可藉由該安全周邊裝置來運作該主機裝置之一實例(圖4之步驟180)。更特定而言，圖13係一處理程序，其描述如何實行與該安全周邊裝置相關聯且由一使用者經由該主機裝置上之一應用程式發送之一任務請求。舉例而言，一任務請求可係一存取或儲存該安全周邊裝置上之內容之請求，包括存取並儲存檔案(例如音樂、應用程式、等等)、存取與該安全周邊裝置相關聯之資訊(例如空閒記憶體空間量)、改變用於組態該安全記憶體裝置之內容、或存取DRM資訊(例如數位權利物件)。該使用者可藉由該主機裝置上之一應用程式來請求此任務。在下一實例中，將使用一安全記憶體裝置作為該安全周邊裝置。然而，應注意，該安全周邊裝置在其使用及組態方式不僅限為此實例所提供的那樣。

在圖13之步驟505中，一使用者可發送一任務請求至主機裝置100上之一應用程式。該任務請求係在周邊裝置SDK安全層125處接收自應用程式105(步驟505)。

在步驟515中，周邊裝置SDK安全層125將對應用程式

105實行一註冊處理程序。該註冊處理程序係用於鑑認應用程式105且若該鑑認成功則將應用程式105註冊於內部註冊表285(顯示於圖7中)中之處理程序。若該註冊成功，則該周邊裝置SDK將發送一指示至應用程式105。該指示係指示出曝露所註冊應用程式105特有之API。周邊裝置SDK安全層125亦發送一應用程式控制代碼至應用程式105。該應用程式控制代碼用作一附加安全措施。每當應用程式105使用一曝露API來與周邊裝置145通信時，應用程式105亦必須藉由該API發送該應用程式控制代碼至該周邊裝置。關於該註冊處理程序之更詳細說明將闡述於圖14中。

若步驟515之註冊處理程序成功，則應用程式105將經由在該註冊處理程序期間曝露之該等API中之一者或多者發送該任務請求至周邊裝置SDK 330(步驟520)。該任務請求必須與在該註冊處理程序期間給予應用程式105之應用程式控制代碼一同發送。

在步驟525中，周邊裝置SDK 330將使用應用程式105特有之所曝露API子群組來實行該任務請求。圖18描述如何實行此步驟以將受保護內容儲存於一安全記憶體裝置中之一實例。圖19描述如何實行此步驟以存取儲存於一安全記憶體裝置中之受保護內容之一實例。

一旦在步驟525中完成該任務請求，則在步驟530中周邊裝置SDK安全層125將從內部註冊表285中解除註冊應用程式105。圖20更詳細描述如何實行此步驟。

圖14係一流程圖，其圖解闡釋如何針對與受保護內容相

關聯之一任務實行該註冊處理程序之一項實例。在步驟700中，在一使用者發送一任務請求至應用程式105之後，應用程式105將從一鑑認方法選項清單中選擇一鑑認方法。該鑑認方法選項清單由周邊裝置SDK安全層125經由一鑑認API提供至應用程式105。用於提供此一清單之API可定義(例如)為：

void ListAuthenMethod(char*AppID、char*AuthList)。

ListAuthenMethod API可向周邊裝置SDK安全層125提供應用程式105之應用程式ID(char*AppID)。該應用程式ID係與應用程式105相關聯之唯一識別符。周邊裝置SDK安全層125將傳回一由周邊裝置SDK 125支援之鑑認方法清單(char*AuthList)。應用程式105隨後將基於應用程式105經程式化以使用之鑑認方法來從由周邊裝置SDK安全層125所提供之清單中選擇使用哪一鑑認方法。

在步驟705中，應用程式105將藉由獲取所選鑑認方法之適當憑證來實行所選鑑認方法。舉例而言，若所選鑑認方法係基於PKI的，則應用程式105將藉由擷取其PKI證書作為其憑證來實行該鑑認方法。若所選鑑認方法係一詢問/回應鑑認方法，則應用程式105將藉由調用與鑑認API 350一同儲存於記憶體裝置SDK 330中之詢問/回應API來實行該鑑認方法。應用程式105將使用該詢問/回應API自周邊裝置SDK安全層125接收該詢問。該詢問可係一由主機裝置密碼編譯引擎185或記憶體裝置密碼編譯引擎160所產生之隨機數。應用程式105隨後將計算對該詢問之適當回應

作為其憑證。關於如何實行不同鑑認方法之更詳細說明闡述於對圖15A至圖15C之說明中。

在步驟710中，應用程式105將藉由調用一註冊API來發送該註冊資訊至周邊裝置SDK安全層125。用於註冊該應用程式之API可定義(例如)為：

uchar RegisterApplication(char* AppID, char*AuthMethod,
uchar* credential, uchar credentialLen)。

RegisterApplication API可允許應用程式105使用RegisterApplication API發送其應用程式ID(char* AppID)、所選鑑認方法(char*AuthMethod)、憑證(uchar*credential)及在步驟705中所擷取之憑證之長度(uchar credentialLen)至周邊裝置SDK安全層125。憑證長度應提供以支援不同鑑認方法可能需要之不同憑證長度。

在步驟715中，周邊裝置SDK安全層125將檢查以確定該憑證是否有效。若該憑證無效，則周邊裝置SDK安全層125將傳回一錯誤至應用程式105(步驟720)。

若該憑證有效，則在步驟722中，周邊裝置SDK安全層125將針對應用程式105產生一應用程式控制代碼。該應用程式控制代碼係使用任一預定義密碼編譯演算法(例如HASH，舉例而言)來產生之一唯一隨機數。該應用程式控制代碼將藉由將特定值輸入至該預定義密碼編譯演算法中來產生。此等特定值可係與應用程式105及/或應用程式105之註冊資訊相關聯之任何值，例如應用程式ID、應用程式105註冊之時間、應用程式105可註冊之時間量、或註

冊狀態，舉例而言。所有周邊裝置SDK API皆含有一應用程式控制代碼之一輸入參數。在一項實施例中，可針對向所有應用程式開放之API產生並使用一預設應用程式控制代碼。然而，如先前所述，鑑認API 350向所有應用程式開放且存取此等鑑認API不需要應用程式控制代碼。

一旦產生該應用程式控制代碼，則周邊裝置SDK安全層125將把應用程式105註冊於一由周邊裝置SDK安全層125管理之內部註冊表285中(步驟725)。內部註冊表285含有經鑑認應用程式及應用程式啟動程序之資訊。針對已藉由周邊裝置SDK安全層125成功鑑認之應用程式及應用程式啟動程序，周邊裝置SDK安全層125將在內部註冊表285中記錄資訊，例如應用程式控制代碼、指示經鑑認應用程式可在內部註冊表285中保持註冊之一時間量之應用程式105之一逾時週期(例如註冊時間+應用程式可註冊之時間量)、應用程式105可存取之API、或任何其他資訊。內部註冊表285用於記錄經鑑認應用程式及應用程式啟動程序以便當彼等經鑑認應用程式及應用程式啟動程序註冊於該鑑認表中時不必每當接收到一任務請求時重新鑑認該等經鑑認應用程式及應用程式啟動程序。

在步驟730中，周邊裝置SDK安全層125檢查應用程式105是否成功註冊於內部註冊表285中。若應用程式105未成功註冊於內部註冊表285中，則周邊裝置SDK安全層125將傳回一錯誤至應用程式105(步驟735)

若應用程式105成功註冊於內部註冊表285中，則周邊裝

置SDK安全層125將藉由鑑認API傳回在步驟722中所產生之應用程式控制代碼至應用程式105(步驟738)。周邊裝置SDK安全層125亦將傳回一指示註冊成功之指示(例如status-ok)至應用程式105(步驟740)。status_ok指示讓應用程式105知道將曝露應用程式105特有的且實行該任務所需之API子群組以供應用程式105使用。

在步驟745中，周邊裝置SDK安全層125隨後將使該API子群組自周邊裝置SDK 330曝露於應用程式105，例如圖12中所示之子群組262。此API子群組將允許應用程式105與安全周邊裝置145通信。然而，對此程式碼部分之存取只有在鑑認之後應用程式105提供一有效應用程式控制代碼之情況下才允許。藉由創建應用程式105與安全周邊裝置145之間的適當連結，此API子群組允許應用程式105實行該任務請求。

圖15A至圖15C顯示用於實行由周邊裝置SDK安全層125支援之不同類型之鑑認方法之處理程序之實例(圖14之步驟710及715)。圖15A係一種用於實行一基於密碼之鑑認之處理程序之一項實例之一流程圖。藉由可用於鑑認之一密碼程式化應用程式105。在圖15A之步驟535中，應用程式105存取應用程式105經程式化以使用之密碼。應用程式105將藉由一鑑認API發送該密碼至周邊裝置SDK安全層125。周邊裝置SDK安全層125隨後將藉由檢查以確定該密碼是否有效來繼續進行圖14之處理程序(圖14之步驟715)。

圖15B係一種用於實行一基於詢問-回應之鑑認之處理程

序之一項實例之一流程圖。在步驟545中，應用程式105藉由一鑑認API自周邊裝置SDK安全層125接收一詢問。舉例而言，該API之形式可係void GetChallenge(char*AppID, uchar*challenge, uchar*challengeLen)。API GetChallenge可允許應用程式105向周邊裝置SDK安全層125提供其應用程式ID(char*AppID)。周邊裝置SDK安全層125隨後可傳回該詢問(uchar*challenge)以及該詢問(uchar*challenge)之長度至應用程式105。

在步驟500中，應用程式105將藉由將所接收詢問輸入至應用程式105經程式化以使用之一密碼編譯函式中來計算一回應。在步驟555中，應用程式105將發送所計算回應至周邊裝置SDK安全層125。周邊裝置SDK安全層125亦將以相同之密碼編譯函式使用相同之詢問來計算一回應(步驟560)並比較所計算回應與接收自應用程式105之回應(步驟565)。此比較步驟係周邊裝置SDK安全層125如何檢查憑證(例如來自應用程式105之回應)是否有效(圖14之步驟715)。圖14之註冊處理程序可基於此憑證繼續。

圖15C係一用於對應用程式105實行一基於PKI之鑑認之處理程序之一項實例之一流程圖。在步驟570中，應用程式105發送一證書至周邊裝置SDK安全層125。該證書係與應用程式105一同儲存之憑證之一部分。應用程式105經程式化以經由一鑑認API來提供此證書。

在步驟575中，周邊裝置SDK安全層125將驗證該證書。在步驟580中，若該證書有效，則周邊裝置SDK安全層125

將藉由一自由該應用程式所發送之證書擷取之公用密鑰來加密一隨機產生數(步驟570)。該隨機數可使用SDK密碼編譯程式庫168來產生並加密。該經加密隨機數隨後自周邊裝置SDK安全層125發送至應用程式105(步驟585)。

在步驟590中，應用程式105將使用與由周邊裝置SDK安全層125所使用之公用密鑰相關聯之一私用密鑰來解密接收自周邊裝置SDK安全層125之經加密隨機數。經授權應用程式因其等具有正確的私用密鑰而能夠解密該經加密隨機數。在步驟590中，應用程式105將發送該經解密隨機數至周邊裝置SDK安全層125以供驗證(圖14之步驟715)。此刻，圖14之處理程序可繼續。

圖16繪示圖12之註冊處理程序之一實例之一方塊圖。應用程式1 107將首先使用選自在圖14之步驟700中由周邊裝置SDK安全層125所提供之清單之鑑認方法來實行一鑑認方法(圖12之步驟705)並發送該註冊資訊至周邊裝置SDK 330內之周邊裝置SDK安全層125(步驟710)。若周邊裝置SDK安全層125確定該憑證有效(步驟715)，則周邊裝置SDK安全層125將針對應用程式1產生一應用程式控制代碼(步驟722)，將應用程式1 107註冊於內部註冊表285中(步驟725)，並將APP 1之API 262子群組曝露於應用程式1 107(步驟745)。

圖17繪示請求存取一安全記憶體裝置145之若干經鑑認應用程式之軟體層之一實例。不同API可基於該SDK係如何針對每一應用程式而組態來存取，如圖2之步驟190中所

述。舉例而言，在應用程式1 107藉由周邊裝置SDK安全層125予以成功鑑認且註冊於內部註冊表285中之後，應用程式1 107將可存取應用程式1 262之API子群組。舉例而言，應用程式1 107可調用彼等API來安全儲存並存取一安全記憶體裝置145上的受保護內容，組態安全記憶體裝置145，等等。APP 1之API 262將提供適當介接以使應用程式1能夠經由安全檔案系統135及裝置驅動程式140來實行對受保護內容之所請求任務。在應用程式1 107之情況下，該SDK經組態以提供一用於存取APP 1之該等API中之每一者之全套功能(參見圖2之步驟190)。

應用程式2及應用程式3係已藉由檔案系統篩選器125予以成功鑑認且註冊於內部註冊表285中之其他應用程式之實例。應用程式2可使用APP 2之API子群組(例如安全儲存API及DRM API)經由安全檔案系統135及裝置驅動程式140來存取並儲存受保護內容，且亦可使用該SDK中之組態API來組態安全記憶體裝置145。然而，應用程式2可能不可存取該SDK內之任何定製API。允許應用程式2存取之API係基於如圖2之步驟190中所述之SDK組態。類似地，應用程式3可使用APP 3之API子群組經由安全檔案系統135及裝置驅動程式140來存取並儲存受保護內容。然而，應用程式3不可存取該SDK內之組態、DRM及定製API，因為在圖2之步驟190中該SDK未經組態以允許應用程式3存取此等API。

繼續闡述一作為該周邊裝置之安全記憶體裝置之實例，

圖18係一流程圖，其描述周邊裝置SDK 330如何實行將受保護內容儲存於安全記憶體裝置145中之任務之一項實例(圖13之步驟525)。在步驟900中，一旦圖13之註冊處理程序完成且該任務請求已使用所曝露API中之一者或多者發送，則周邊裝置SDK 330將指揮安全記憶體裝置145之安全檔案系統135定位一用於儲存安全記憶體裝置145中之該受保護內容之位置。應用程式105可調用在圖14之步驟745中所曝露之API子群組中之該等API中之一者來為安全檔案系統135提供所期望之儲存位置。

在步驟905中，周邊裝置SDK 330將存取與其中欲儲存受保護內容之儲存位置相關聯之權限，例如一用於創建一安全通道155之會期密鑰。在步驟910中，周邊裝置SDK 330將基於在步驟905中所存取之權限來確定是否應使用一安全通道來傳送該受保護內容。

若周邊裝置SDK 330確定不應使用一安全通道，則該受保護內容將經由一開放通道150自主機裝置100上之主機儲存管理器110傳送至安全記憶體裝置145(步驟915)。應用程式105可藉由調用在圖14之步驟745中所曝露之API子群組中之該等API中之一者來傳送此內容。受保護內容存取管理器320將存取該儲存位置之CEK並指揮周邊裝置密碼編譯引擎160使用該CEK及密碼編譯引擎程式庫235來加密該內容(步驟920)。受保護內容存取管理器320隨後將把經加密之受保護內容儲存於適當儲存位置中(步驟925)。

若在步驟910中周邊裝置SDK 330確定應使用一安全通道

155，則周邊裝置SDK 330將經由所曝露之API子群組中之該等API中之一者自應用程式105接收該內容並指揮SDK密碼編譯引擎168使用該會期密鑰及適當密碼編譯編譯方案來加密主機裝置100內之受保護內容(步驟930)。在步驟935中，該經加密內容將藉由一安全通道155自主機裝置100上之主機儲存管理器110傳送至安全記憶體裝置145。周邊裝置密碼編譯引擎160隨後將在安全記憶體裝置145及密碼編譯引擎程式庫235中解密所傳送之受保護內容(步驟940)。

在步驟920中，受保護內容存取管理器320將存取其中欲儲存該受保護內容之儲存位置之CEK並指揮周邊裝置密碼編譯引擎160使用該CEK及密碼編譯引擎程式庫235來加密該內容。受保護內容存取管理器320隨後將把經加密之受保護內容儲存於適當儲存位置中(步驟925)。

圖19係一流程圖，其描述周邊裝置SDK安全層125如何實行存取儲存於安全記憶體裝置145中之受保護內容之任務之一項實例(圖13之步驟525)。在步驟800中，一旦圖13之註冊處理程序完成且該任務請求已使用所曝露API中之一者或多者發送，則周邊裝置SDK安全層125將指揮安全檔案系統135在安全記憶體裝置145之適當位置中定位所請求之受保護內容。應用程式105可調用圖14之步驟745中所曝露之API子群組中之該等API中之一者來為安全檔案系統135提供所期望之儲存位置。

受保護內容存取管理器320存取與受保護內容之位置相關聯之權限，包括該CEK及該會期密鑰(步驟805)。安全內

容存取管理器320隨後自安全記憶體裝置145中之位置存取受保護內容(步驟810)並指揮周邊裝置密碼編譯引擎160使用該CEK及密碼編譯引擎程式庫235來解密該內容(步驟815)。

在步驟820中，受保護內容存取管理器320隨後確定是否應使用一安全通道來將該受保護內容傳送至主機裝置100上之主機儲存管理器110。若在步驟805中所存取之會期密鑰指示應使用一開放通道150來傳送該受保護內容，則受保護內容存取管理器320將經由開放通道150將該內容傳送至主機裝置100上之主機儲存管理器110(步驟825)。

若在步驟820中，受保護內容存取管理器320確定應使用一安全通道155來將受保護內容傳送至主機裝置100上之主機儲存管理器110，則受保護內容存取管理器320將指揮周邊裝置密碼編譯引擎160使用該會期密鑰來加密安全記憶體裝置145內之受保護內容(步驟830)。受保護內容存取管理器320隨後將經由安全通道155將經加密之受保護內容傳送至主機裝置100上之主機儲存管理器110(步驟835)。一旦傳送該受保護內容，則將使用SDK密碼編譯程式庫168以使用相同之會期密鑰來解密該受保護內容(步驟840)。

在該受保護內容經成功傳送(步驟825及步驟835)且若必要經解密(步驟840)之後，應用程式105將接收所請求之受保護內容(步驟850)。應用程式105將使用在圖14之步驟745中所曝露之API子群組中之該等API中之一者來接收所請求之受保護內容。

圖20係一流程圖，其描述如何從周邊裝置SDK安全層125中之內部註冊表285中解除註冊應用程式105之一項實例(圖13之步驟530)。在步驟945中，周邊裝置SDK安全層125將檢查以確定該任務是否已完成。若該任務已完成，則周邊裝置SDK安全層125將清除註冊表285內任何與應用程式105相關聯之資訊(步驟970)。周邊裝置SDK安全層125隨後將從內部註冊表285中解除註冊應用程式105(步驟975)。用於解除註冊應用程式105之步驟可藉由調用應用程式API(例如uchar UnRegisterApplication(char*AppID)，舉例而言)來實行。此API將藉由從內部註冊表285中移除所對應之應用程式ID來解除註冊應用程式105。用於實行該所請求任務之處理程序隨後結束(步驟980)。

若在實行該任務請求時該任務尚未完成，則周邊裝置SDK安全層125檢查以確定應用程式105是否已在該逾時週期期間註冊達指示於內部註冊表285中之時間量(步驟950)。若該逾時週期已過，則周邊裝置SDK安全層125將清除註冊表285內任何與應用程式105相關聯之資訊(步驟955)。周邊裝置SDK安全層125隨後將請求重新鑑認應用程式105(步驟960)。可使用一類似於圖14之鑑認處理程序來重新鑑認應用程式105。周邊裝置SDK安全層125將確定該重新鑑認是否成功(步驟965)。若重新鑑認成功，則將繼續實行該任務(步驟525)。若重新鑑認不成功，則周邊裝置SDK安全層125將藉由調用適當API(例如uchar UnRegisterApplication(char*AppID)來從內部註冊表285中

解除註冊應用程式105(步驟975)。此API將藉由從內部註冊表285中移除所對應之應用程式ID來解除註冊應用程式105。用於實行該任務之處理程序隨後將結束(步驟980)。

若在步驟950中周邊裝置SDK安全層125確定內部註冊表285中之逾時週期未過，則在步驟525中周邊裝置SDK安全層125將繼續實行該任務請求。

上文對各實施例之述詳細說明並非旨在為窮盡性的或將本發明限制至所揭示之精確形式。根據上文之教示亦可以做出許多修改及改變。所述實施例之選擇旨在最好地解釋本發明之原理及其實際應用，從而使熟習此項技術者能夠在各種實施例中並藉助適合於所涵蓋之特定使用之各種修改來最佳地利用本發明。上文說明並非旨在用以限制隨附申請專利範圍中列舉之本發明之範疇。

【圖式簡單說明】

圖1係在安裝一安全周邊裝置之一SDK之前一主機裝置之一方塊圖。

圖2係描述一種用於組態與一安全周邊裝置相關聯之一SDK之處理程序的一流程圖。

圖3繪示一安全周邊裝置SDK之一項實例。

圖4係描述一種用於將一安全周邊裝置載入至一主機裝置中之處理程序之一流程圖。

圖5係一繪示在安裝一安全周邊裝置之一SDK之後一主機裝置之一項實施例之方塊圖。

圖6係一繪示在安裝一安全記憶體裝置的程式碼之前主

機裝置組件之一項實施例之方塊圖。

圖7係一繪示一主機裝置及一安全記憶體裝置之組件之一項實施例之方塊圖。

圖8係一記憶體裝置SDK之一項實施例之一方塊圖。

圖9係一繪示一安全記憶體裝置之一項實施例之方塊圖。

圖10係一繪示一安全記憶體裝置之一韌體模組之一項實施例之方塊圖。

圖11繪示一安全記憶體裝置內之各分割區之一項實例。

圖12係含於一記憶體裝置之一SDK中之應用程式API之一項實例。

圖13係一描述一個用於存取一安全周邊裝置之處理程序之流程圖。

圖14係一描述一用於在一主機裝置上註冊一軟體實體之處理程序之一項實施例之流程圖。

圖15A至圖15C係SDK可實施之不同鑑認方法的流程圖。

圖16繪示該註冊處理程序之一項實例。

圖17繪示成功註冊於一主機裝置上之軟體實體之一項實例。

圖18係一描述一用於將受保護內容儲存於一記憶體裝置上之處理程序之一項實施例之流程圖。

圖19係一描述一用於存取一記憶體裝置上之受保護內容之處理程序之一項實施例之流程圖。

圖20係一描述一用於解除註冊一軟體實體之處理程序之

一項實施例之流程圖。

【主要元件符號說明】

100	主機裝置
105	應用程式
107	應用程式1
110	主機儲存管理器
120	安全周邊裝置API
125	安全層
130	主機檔案系統
135	安全檔案系統
140	裝置驅動程式
142	主機裝置實體介面
144	周邊裝置介面模組
145	安全周邊裝置
150	開放通道
155	安全通道
160	周邊裝置密碼編譯引擎
165	主機CPU
168	SDK密碼編譯程式庫
185	主機裝置密碼編譯引擎
210	韌體模組
220	CPU
235	密碼編譯引擎程式庫
240	公用分割區

250	安全分割區
255	主機裝置
260	記憶體、周邊裝置API、應用程式API
262	應用程式1之API
285	註冊表
310	快閃記憶體管理器
315	DRM模組
320	受保護內容存取管理器
330	周邊裝置SDK
340	標準/安全儲存API
350	鑑認API
360	組態API
370	DRM API
380	定製API
400	系統分割區
410	P0-公用分割區
420	P1-安全分割區
430	P2-安全分割區
440	檔案A
450	P3-安全分割區

201003457

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：98116598

※ 申請日：98.5.19　　※IPC 分類：~~G06F~~ G06F 21/22 (2006.01)

一、發明名稱：（中文/英文）

對於周邊裝置的軟體開發套件之存取鑑認

AUTHENTICATION FOR ACCESS TO SOFTWARE DEVELOPMENT KIT FOR A PERIPHERAL DEVICE

二、中文發明摘要：

用於一周邊裝置之一程式碼集係安裝於一主機裝置上。該程式碼集係用於自該主機裝置控制對該周邊裝置之存取。該程式碼集亦含有一個或多個程式碼子集，該一個或多個程式碼子集可由該主機裝置上之軟體實體用來存取該周邊裝置。必須藉由安裝於一主機裝置上之該程式碼集成功鑑認該主機裝置上之一軟體實體。一旦成功鑑認該軟體實體，則該程式碼集將提供對該軟體實體特有之該一個或多個程式碼子集之存取。該一個或多個程式碼子集可由該軟體實體用來存取該周邊裝置。

三、英文發明摘要：

A set of code for a peripheral device is installed on a host device. The set of code is used to control access to the peripheral device from the host device. The set of code also contains one or more subsets of code that can be used by software entities on the host device for access to the peripheral device. A software entity on a host device must be successfully authenticated with the set of code installed on the host device. Once the software entity is successfully authenticated, the set of code will provide access to the one or more subsets of code specific to the software entity. The one or more subsets of code can be used by the software entity to access the peripheral device.

七、申請專利範圍：

1. 一種用於提供對一安全裝置之存取之方法，其包含：

在一主機裝置上安裝與一周邊裝置相關聯之一程式碼集，該程式碼集包括用於在該主機裝置上運作該周邊裝置的程式碼；

使用該程式碼集來鑑認該主機裝置上之一第一軟體實體；及

若成功鑑認該第一軟體實體，則將該程式碼集之一部分曝露於該第一軟體實體，包括曝露允許該第一軟體實體與該周邊裝置通信的程式碼。

2. 如請求項1之方法，其中：

該程式碼集包括裝置驅動程式之程式碼、應用程式設計介面程式碼及鑑認程式碼；且

該程式碼集之該部分包括來自該應用程式設計介面程式碼及該鑑認程式碼之多個程式碼部分。

3. 如請求項1之方法，其進一步包含：

在該程式碼集處自該第一軟體實體接收一任務請求；及

使用該程式碼集之該部分來實行該任務請求。

4. 如請求項1之方法，其中該鑑認步驟包含：

自該第一軟體實體接收一憑證；及

驗證該憑證，該驗證係由該程式碼集實行。

5. 如請求項4之方法，其進一步包含：

提供一個或多個鑑認選項至該第一軟體實體，該提供

係由該程式碼集實行；及

自該第一軟體實體接收指示該一個或多個鑑認選項中之一者之一回應，該驗證步驟包括基於該回應來驗證該憑證。

6. 如請求項1之方法，其進一步包含：

若未成功鑑認該第一軟體實體，則傳回一錯誤至該第一軟體實體。

7. 如請求項1之方法，其進一步包含：

若成功鑑認該第一軟體實體，則在一密碼編譯函式中使用與該第一軟體實體相關聯之一識別符來產生一軟體實體控制代碼。

8. 如請求項7之方法，其進一步包含：

發送該軟體實體控制代碼至該第一軟體實體，該軟體實體控制代碼提供對該第一程式碼之存取。

9. 如請求項7之方法，其進一步包含：

若成功鑑認該第一軟體實體，則使用該程式碼集來註冊該第一軟體實體，包括將該軟體實體控制代碼註冊於一經鑑認軟體實體表中。

10. 如請求項9之方法，其進一步包含：

若該第一軟體實體成功註冊，則發送一曝露該程式碼集之該部分之指示，包括發送該指示至該第一軟體實體。

11. 如請求項10之方法，其進一步包含：

當註冊該第一軟體實體時，允許該第一軟體實體實行

與該周邊裝置相關聯之任務，包括允許該第一軟體實體使用該軟體實體控制代碼連同該程式碼集之該部分來實行該等任務。

12. 如請求項9之方法，其中：

該註冊步驟包括註冊與該第一軟體實體相關聯之權限，該等權限指示該第一軟體實體可存取之該程式碼集之一個或多個部分。

13. 如請求項9之方法，其進一步包含：

若該第一軟體實體在該表中註冊達該表中所指示之一預定時間量，則解除註冊該第一軟體實體。

14. 如請求項9之方法，其進一步包含：

自該第一軟體實體接收一任務請求；

使用該程式碼集之該部分來實行該任務請求；及

在實行該任務請求之後，使用該程式碼集將該第一軟體實體自該表中解除註冊。

15. 如請求項1之方法，其中：

該周邊裝置係一快閃記憶體裝置。

16. 如請求項1之方法，其進一步包含：

接收將內容儲存於該周邊裝置之一群組中之一請求，包括在該程式碼集處自該第一軟體實體接收該請求；

若成功鑑認該第一軟體實體，則存取與該群組相關聯之一加密密鑰；

使用該加密密鑰來加密該內容；及

使用該程式碼集之該部分來將該內容儲存於該群組

中。

17. 如請求項1之方法，其進一步包含：

接收將內容儲存於該周邊裝置之一群組中之一請求，包括在該程式碼集處自該第一軟體實體接收該請求；

若成功鑑認該第一軟體實體，則存取與該群組相關聯之一加密密鑰；

使用該加密密鑰來解密該內容；及

使用該程式碼集之該部分來存取該內容。

18. 一種用於提供對一裝置之存取之方法，其包含：

自一主機裝置上之一第一軟體實體之一使用者接收與一周邊裝置相關聯之一第一任務請求；

自該第一軟體實體發送一憑證至安裝於該主機裝置上用於該周邊裝置的一程式碼集；

若該憑證有效，則存取與該第一軟體實體相關聯的該程式碼集之一部分，包括存取允許該第一軟體實體實行該第一任務的程式碼，該程式碼集包括允許該主機裝置上的一個或多個軟體實體實行與該周邊裝置相關聯之任務的程式碼；及

使用該程式碼集之該部分來發送與該第一任務相關聯之資訊，該發送資訊係由該第一軟體實體實行。

19. 如請求項18之方法，其進一步包含：

自對鑑認方法之一選擇中挑選一鑑認方法，該發送該憑證係基於該鑑認方法，該挑選係由該第一軟體實體實行。

20. 如請求項18之方法，其進一步包含：

使用該程式碼集之該部分來發送與一第二任務相關聯之資訊而不發送一第二憑證，該發送係由該第一軟體實體實行。

21. 一種用於提供對一安全裝置之存取之方法，其包含：

回應於來自一主機裝置上之一第一軟體實體之存取一記憶體裝置之一請求而發送一個或多個鑑認選項至該第一軟體實體，該一個或多個鑑認選項係自安裝於該主機裝置上用於該記憶體裝置的一程式碼集中導出，該程式碼集包括與該主機裝置上之一個或多個軟體實體相關聯的程式碼；

自該第一軟體實體接收一憑證，該憑證與該一個或多個鑑認選項中之一者相關聯；及

若該憑證有效，則提供對與該第一軟體實體相關聯之第一程式碼之存取，該第一程式碼允許存取該記憶體裝置，該第一程式碼係該程式碼集之一部分。

22. 如請求項21之方法，其進一步包含：

若該憑證有效，則使用與該第一軟體實體相關聯之一識別符來計算一軟體實體控制代碼；及

發送該軟體實體控制代碼至該第一軟體實體，該軟體實體控制代碼由該第一軟體實體用來存取該第一程式碼。

23. 如請求項22之方法，其進一步包含：

若該憑證有效，則將該第一軟體實體註冊於一經鑑認

軟體實體表中，包括將該軟體實體控制代碼註冊於該表中；及

當該第一軟體實體註冊於該表中時，允許該第一軟體實體實行與該記憶體裝置相關聯之一個或多個任務，包括允許該第一軟體實體使用該軟體實體控制代碼連同該第一程式碼來實行該一個或多個任務。

24. 如請求項23之方法，其進一步包含：

當該一個或多個任務完成時，將該第一軟體實體自該表中解除註冊。

25. 如請求項23之方法，其進一步包含：

在該軟體實體在該表中註冊達該軟體實體控制代碼中所指示之一預定時間量之後，將該第一軟體實體自該表中解除註冊。

26. 一種用於存取一安全裝置之系統，其包含：

一周邊裝置；及

與該周邊裝置通信之一主機裝置，該主機裝置包括經調適用以控制對該周邊裝置之存取之一個或多個處理器，該一個或多個處理器經調適用以管理安裝於該主機裝置上用於該周邊裝置的一程式碼集，該程式碼集允許該周邊裝置與該主機裝置上之一個或多個軟體實體之間的通信，該一個或多個處理器經調適用以驗證來自該主機裝置上之一第一軟體實體之一憑證，該一個或多個處理器經調適用以在該憑證有效之情況下將來自該程式碼集的一程式碼子集曝露於該第一軟體實體，該程式碼子

集與該第一軟體實體相關聯。

27. 如請求項26之系統，其中：

該一個或多個處理器自該第一軟體實體接收一任務請求；且

當以該程式碼子集程式化該一個或多個處理器時，該一個或多個處理器實行該任務請求。

28. 如請求項26之系統，其中：

該一個或多個處理器提供一個或多個鑑認選項至該第一軟體實體；且

該一個或多個處理器自該第一軟體實體接收指示該一個或多個鑑認選項中之一者之一回應，該一個或多個處理器基於該回應來驗證該憑證。

29. 如請求項26之系統，其中：

若該憑證無效，則該一個或多個處理器傳回一錯誤至該第一軟體實體。

30. 如請求項26之系統，其中：

若該憑證有效，則該一個或多個處理器在一密碼編譯函式中使用與該第一軟體實體相關聯之一識別符來產生一軟體實體控制代碼。

31. 如請求項30之系統，其中：

該一個或多個處理器發送該軟體實體控制代碼至該第一軟體實體。

32. 如請求項30之系統，其中：

若該憑證有效，則該一個或多個處理器將該第一軟體

實體註冊於一經鑑認軟體實體表中；且

若該憑證有效，則該一個或多個處理器將該軟體實體控制代碼註冊於該表中。

33. 如請求項32之系統，其中：

若該軟體實體成功註冊，則該一個或多個處理器發送一指示至該第一軟體實體，該指示係指示出曝露該程式碼子集。

34. 如請求項33之系統，其中：

若以該程式碼子集程式化該一個或多個處理器，則當該第一軟體實體註冊於該表中時，該一個或多個處理器允許該第一軟體實體使用該軟體實體控制代碼來實行與該周邊裝置相關聯之任務。

35. 如請求項32之系統，其中：

該一個或多個軟體實體將與該第一軟體實體相關聯之權限註冊於該表中，該等權限指示該第一軟體實體可存取之該程式碼集中之一個或多個子集。

36. 如請求項32之系統，其中：

若該第一軟體實體在該表中註冊達該表中所指示之一預定時間量，則該一個或多個處理器解除註冊該第一軟體實體。

37. 如請求項32之系統，其中：

該一個或多個處理器自該第一軟體實體接收一任務請求；

當以該程式碼子集程式化該一個或多個處理器時，該

一個或多個處理器實行該任務請求；且

在實行該任務請求之後，該一個或多個處理器將該第一軟體實體自該表中解除註冊。

38. 如請求項26之系統，其中：

該周邊裝置係一快閃記憶體裝置。

39. 如請求項26之系統，其中：

該一個或多個處理器接收將內容儲存於該周邊裝置之一群組中之一請求，該請求係接收自該第一軟體實體；

若該憑證有效，則該一個或多個處理器存取與該群組相關聯之一加密密鑰；且

該周邊裝置包括一個或多個周邊裝置處理器，該一個或多個周邊裝置處理器使用該加密密鑰來加密該內容並將該內容儲存於該群組中。

40. 如請求項26之系統，其中：

該一個或多個處理器接收一存取該周邊裝置之一群組中之內容之請求，該請求係接收自該第一軟體實體；

若該憑證有效，則該一個或多個處理器存取與該群組相關聯之一加密密鑰；

該周邊裝置包括一個或多個周邊裝置處理器，該一個或多個周邊裝置處理器使用該加密密鑰來解密該內容；且

若以該程式碼子集程式化該一個或多個處理器，則該一個或多個處理器存取該內容。

41. 一種用於存取一安全裝置之系統，其包含：

一密碼編譯引擎，該密碼編譯引擎驗證來自一主機裝置上之一第一軟體實體之一憑證；及

該主機裝置上之一個或多個處理器，該一個或多個處理器與該密碼編譯引擎通信，該一個或多個處理器截取對與該主機裝置通信之一記憶體裝置之存取，該一個或多個處理器自該第一軟體實體接收該憑證，若該憑證有效，則該一個或多個處理器曝露與該第一軟體實體相關聯的程式碼，當以該程式碼程式化該一個或多個處理器時，該一個或多個處理器允許該第一軟體實體存取該記憶體裝置。

42. 如請求項41之系統，其中：

該一個或多個處理器提供一個或多個鑑認選項至該第一軟體實體；

該一個或多個處理器自該第一軟體實體接收對該一個或多個鑑認選項之一選擇；及

該密碼編譯引擎基於該選擇來驗證該憑證。

43. 如請求項41之系統，其中：

若該憑證有效，則該一個或多個處理器將該第一軟體實體註冊於一經鑑認軟體實體表中；且

當該第一軟體實體註冊於該表中時，該一個或多個處理器允許該第一軟體實體與該記憶體裝置之間的通信。

八、圖式：

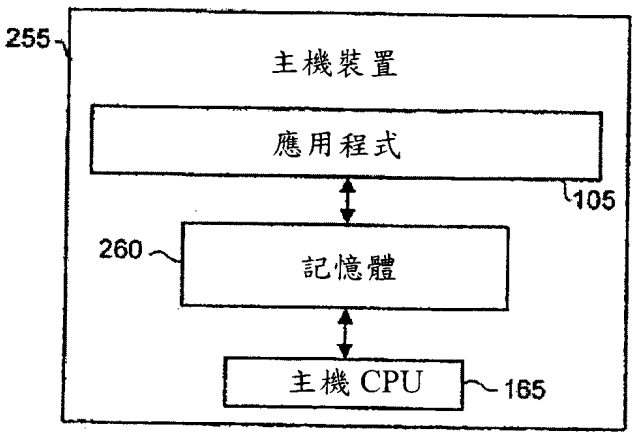


圖1

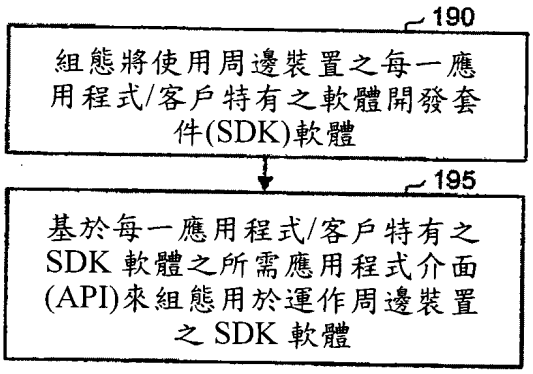


圖2

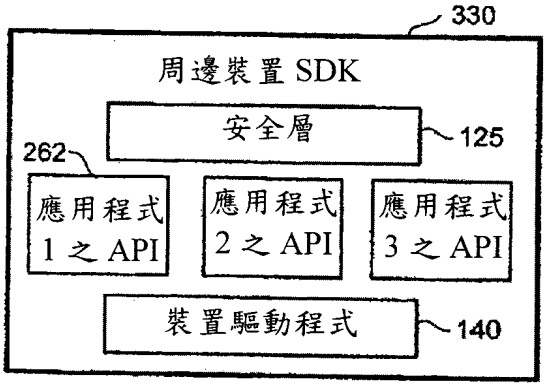


圖3

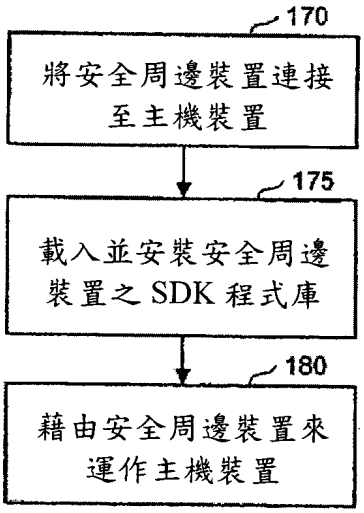


圖4

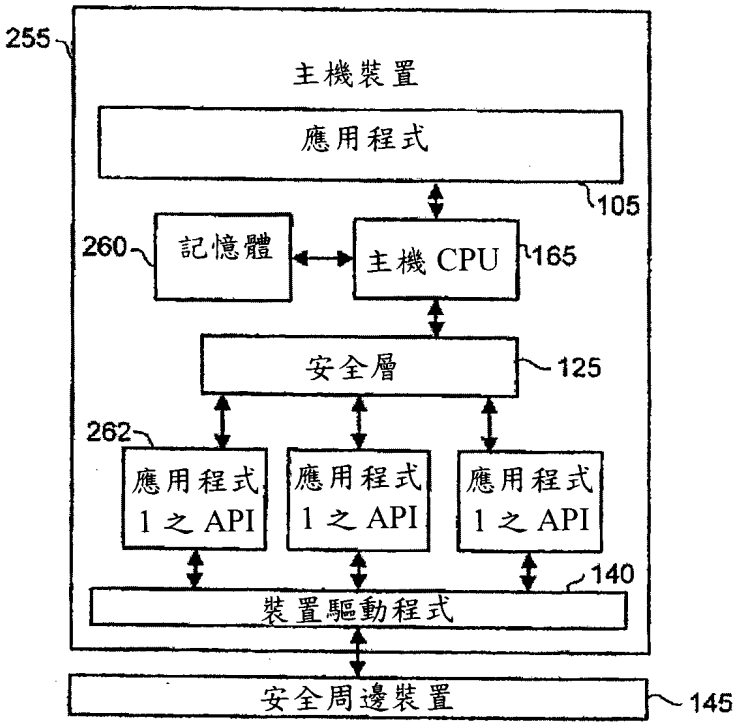

255
主機裝置
應用程式
105
260
記憶體
主機 CPU
165
安全層
125
262
應用程式 1 之 API
應用程式 1 之 API
應用程式 1 之 API
140
裝置驅動程式
安全周邊裝置
145

圖5

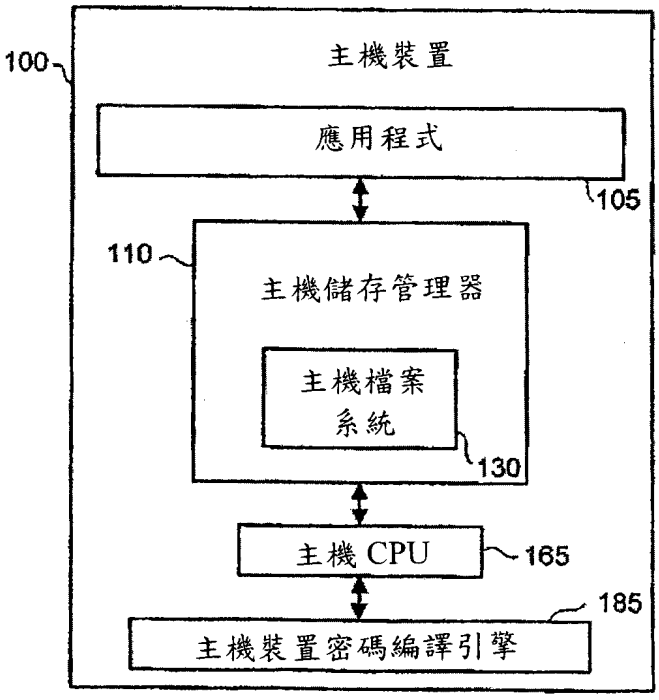

100
主機裝置
應用程式
105
110
主機儲存管理器
主機檔案系統
130
主機 CPU
165
185
主機裝置密碼編譯引擎

圖6

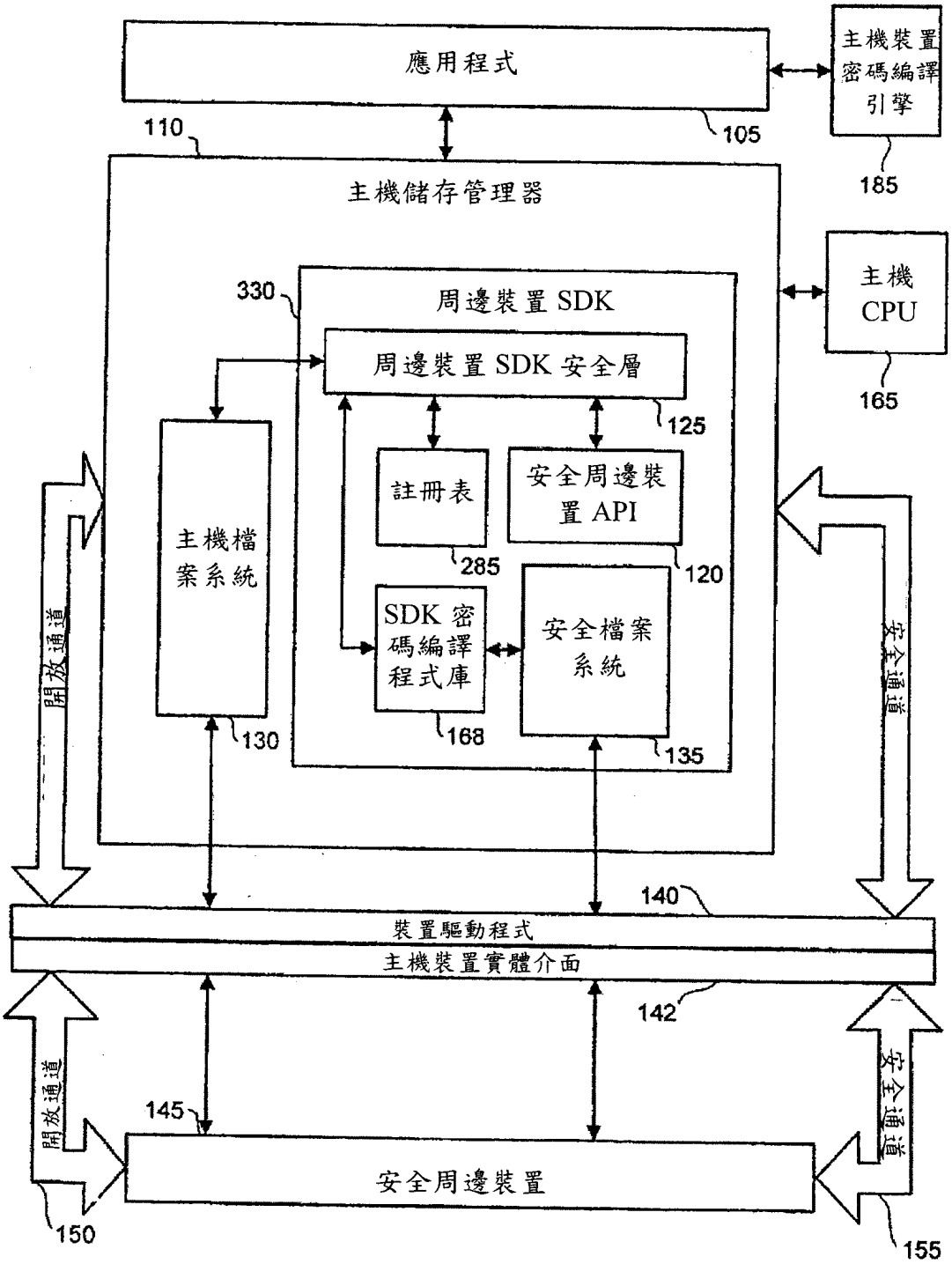

應用程式
105
主機裝置密碼編譯引擎
185
110
主機儲存管理器
主機 CPU
165
330
周邊裝置 SDK
周邊裝置 SDK 安全層
125
註冊表
285
安全周邊裝置 API
120
主機檔案系統
SDK 密碼編譯程式庫
168
安全檔案系統
135
130
開放通道
安全通道
140
裝置驅動程式
主機裝置實體介面
142
開放通道
安全通道
145
安全周邊裝置
150
155

圖 7

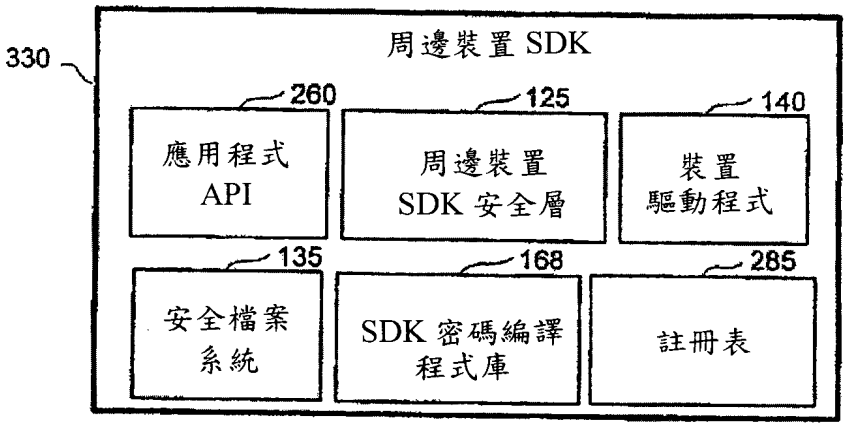

330
周邊裝置 SDK
260
應用程式
API
125
周邊裝置
SDK 安全層
140
裝置
驅動程式
135
安全檔案
系統
168
SDK 密碼編譯
程式庫
285
註冊表

圖8

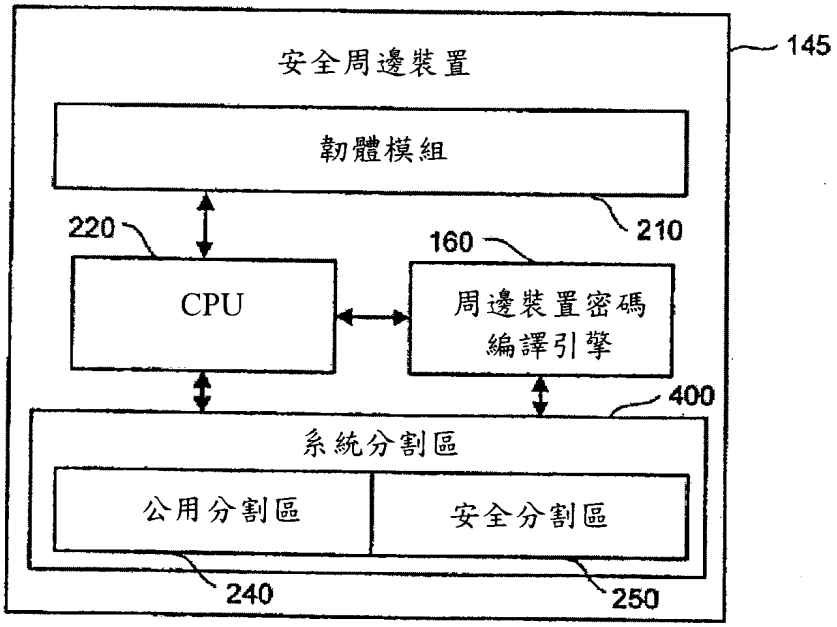

安全周邊裝置
145
韌體模組
210
220
160
CPU
周邊裝置密碼
編譯引擎
400
系統分割區
公用分割區
安全分割區
240
250

圖9

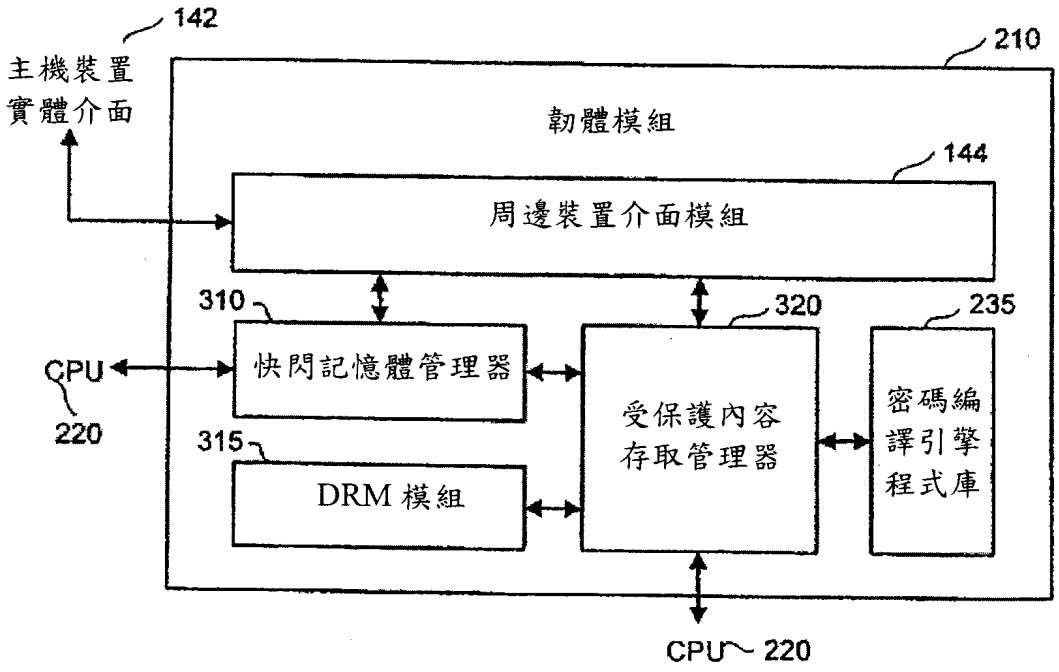

142
主機裝置
實體介面
210
韌體模組
144
周邊裝置介面模組
310
320
235
CPU
220
快閃記憶體管理器
315
DRM 模組
受保護內容
存取管理器
密碼編
譯引擎
程式庫
CPU
220

圖10

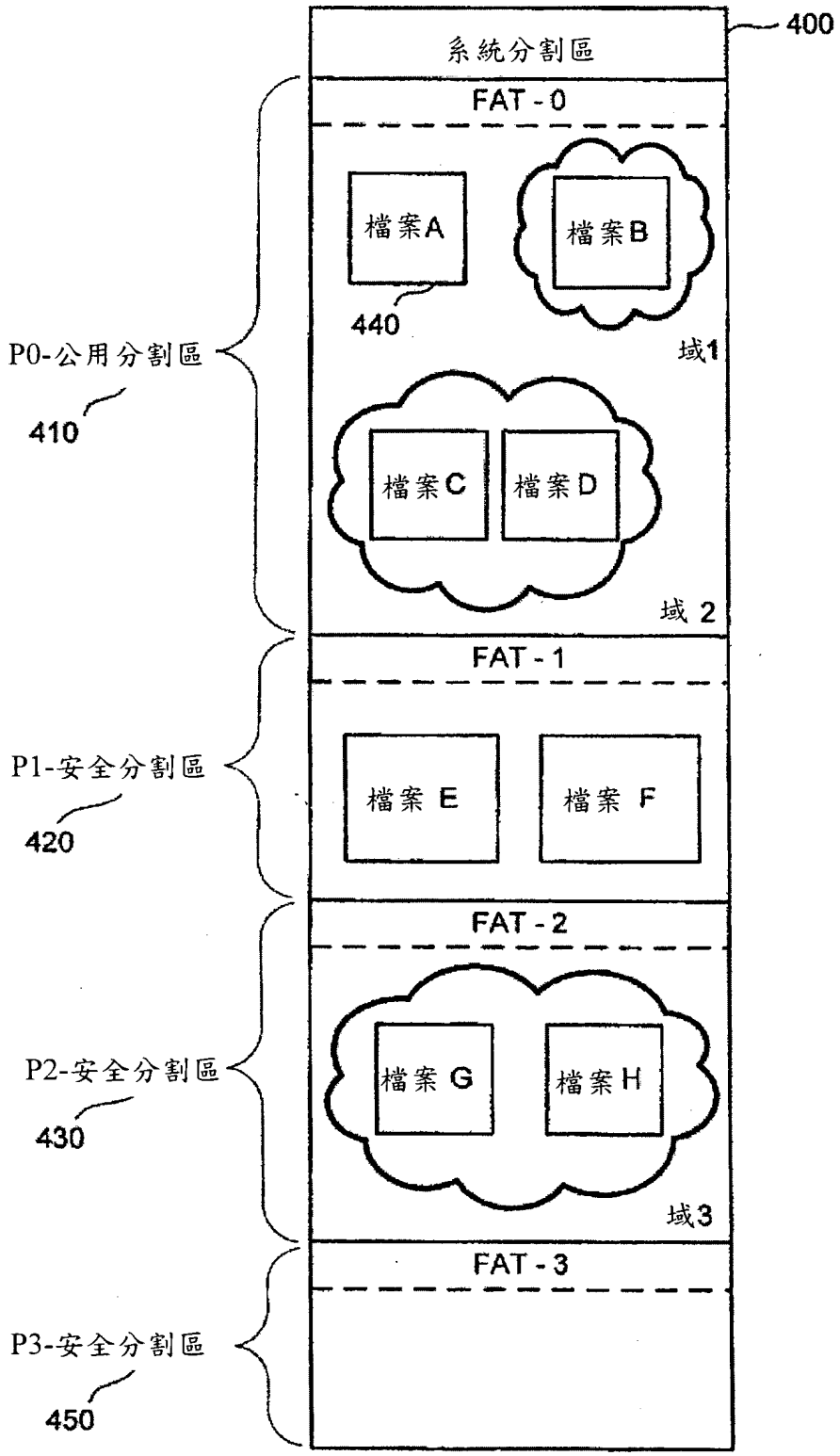

系統分割區
400
FAT - 0
檔案A
檔案B
440
域1
P0-公用分割區
410
檔案C
檔案D
域 2
FAT - 1
P1-安全分割區
420
檔案 E
檔案 F
FAT - 2
P2-安全分割區
430
檔案 G
檔案 H
域3
FAT - 3
P3-安全分割區
450

圖11

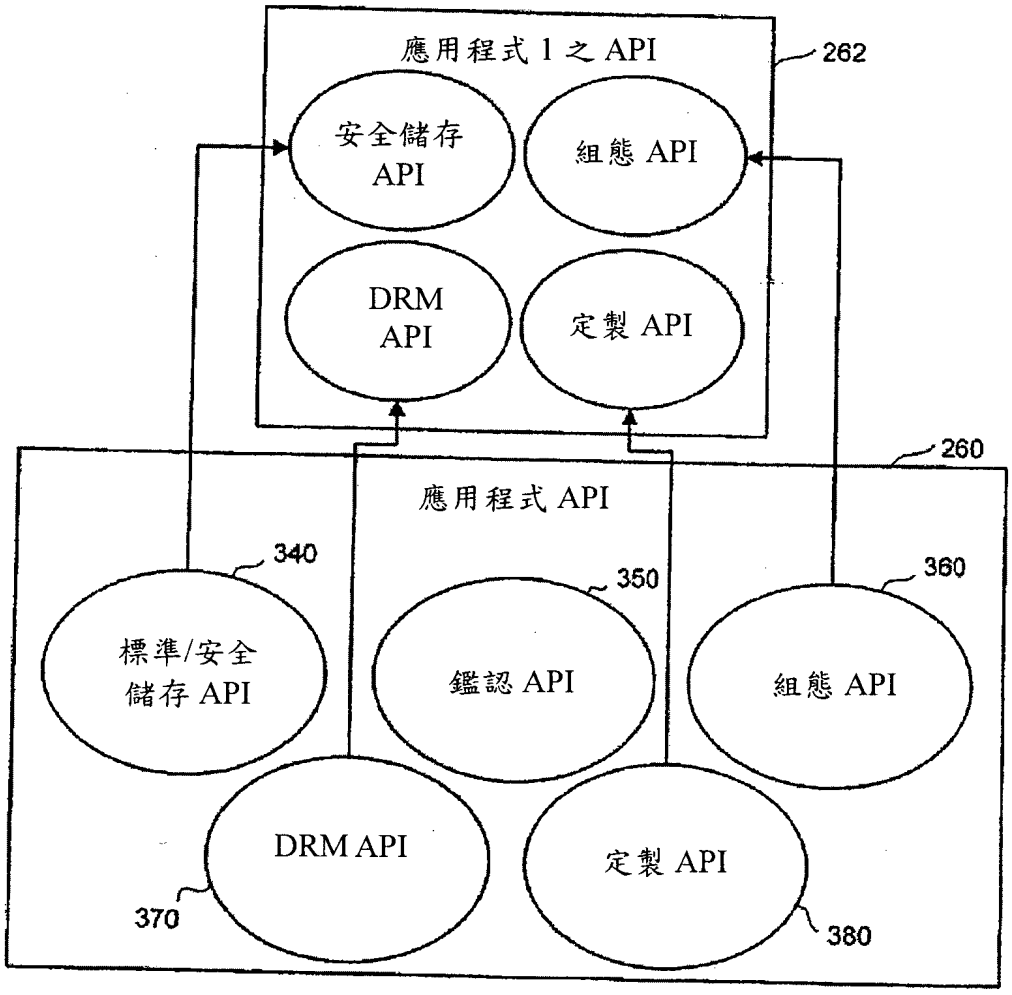

應用程式 1 之 API
262
安全儲存 API
組態 API
DRM API
定製 API
260
應用程式 API
340
標準/安全儲存 API
350
鑑認 API
360
組態 API
DRM API
370
定製 API
380

圖 12

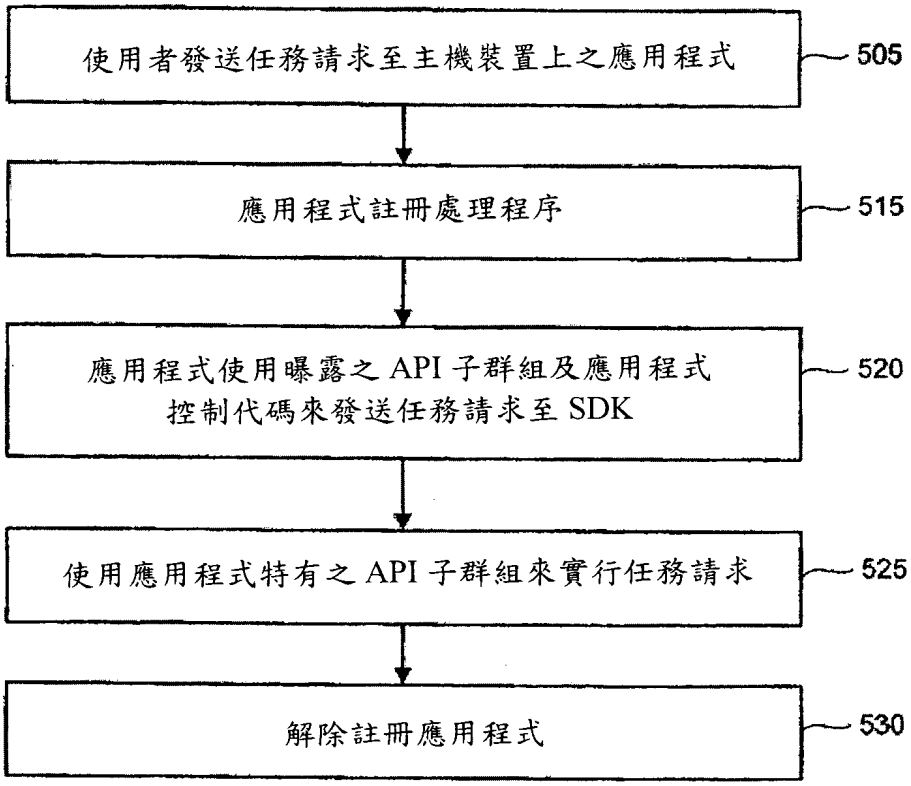

使用者發送任務請求至主機裝置上之應用程式
505
應用程式註冊處理程序
515
應用程式使用曝露之 API 子群組及應用程式
控制代碼來發送任務請求至 SDK
520
使用應用程式特有之 API 子群組來實行任務請求
525
解除註冊應用程式
530

圖13

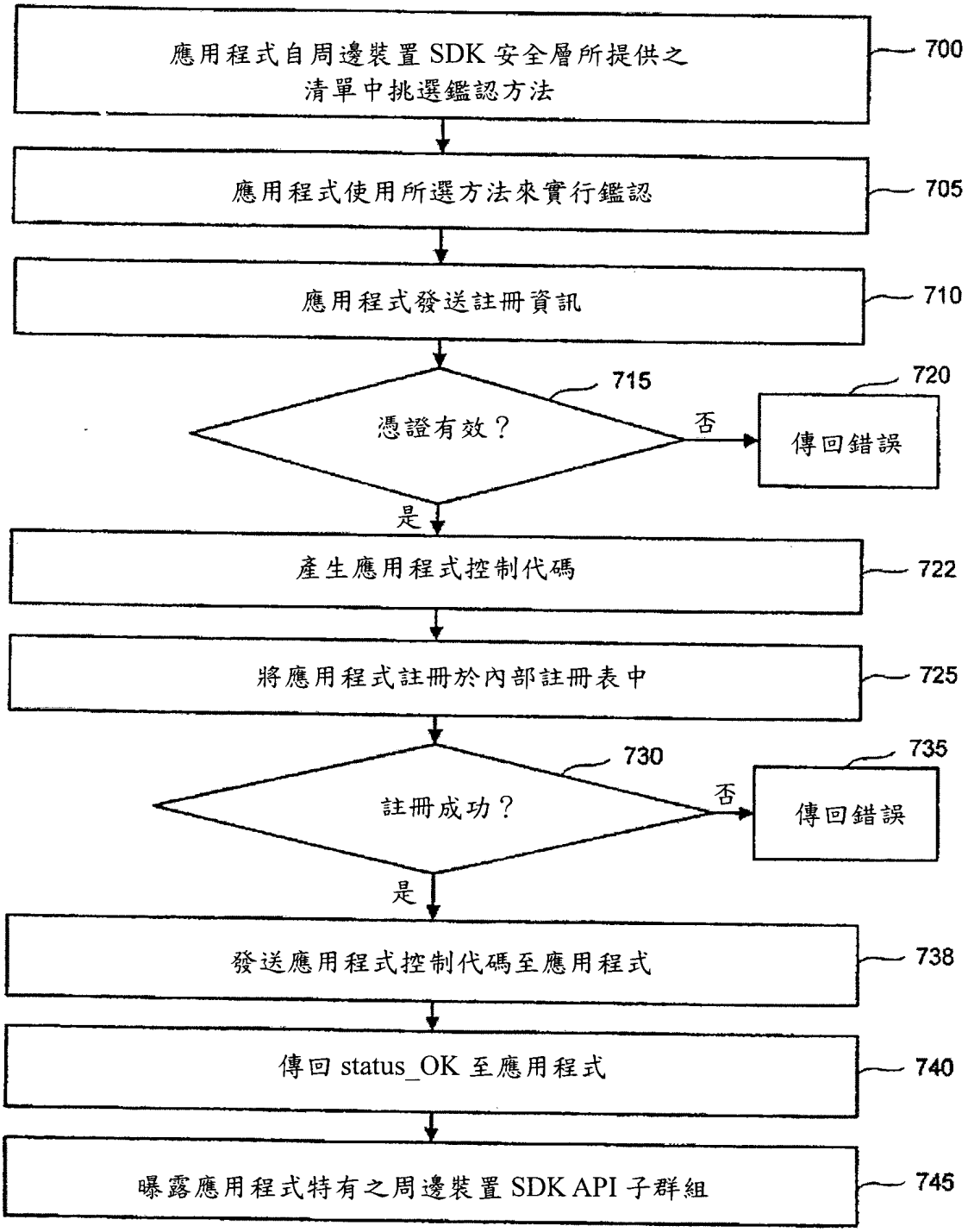

應用程式自周邊裝置 SDK 安全層所提供之清單中挑選鑑認方法
700
應用程式使用所選方法來實行鑑認
705
應用程式發送註冊資訊
710
憑證有效？
715
否
傳回錯誤
720
是
產生應用程式控制代碼
722
將應用程式註冊於內部註冊表中
725
註冊成功？
730
否
傳回錯誤
735
是
發送應用程式控制代碼至應用程式
738
傳回 status_OK 至應用程式
740
曝露應用程式特有之周邊裝置 SDK API 子群組
745

圖14

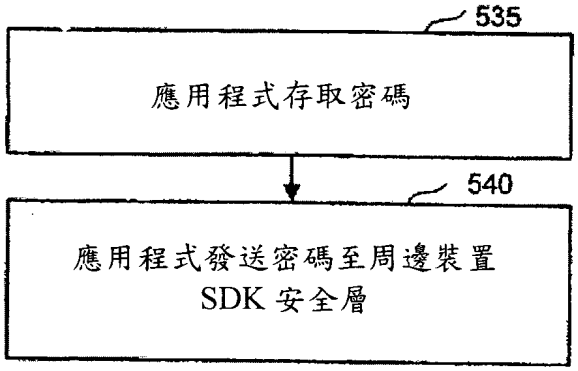


圖15A

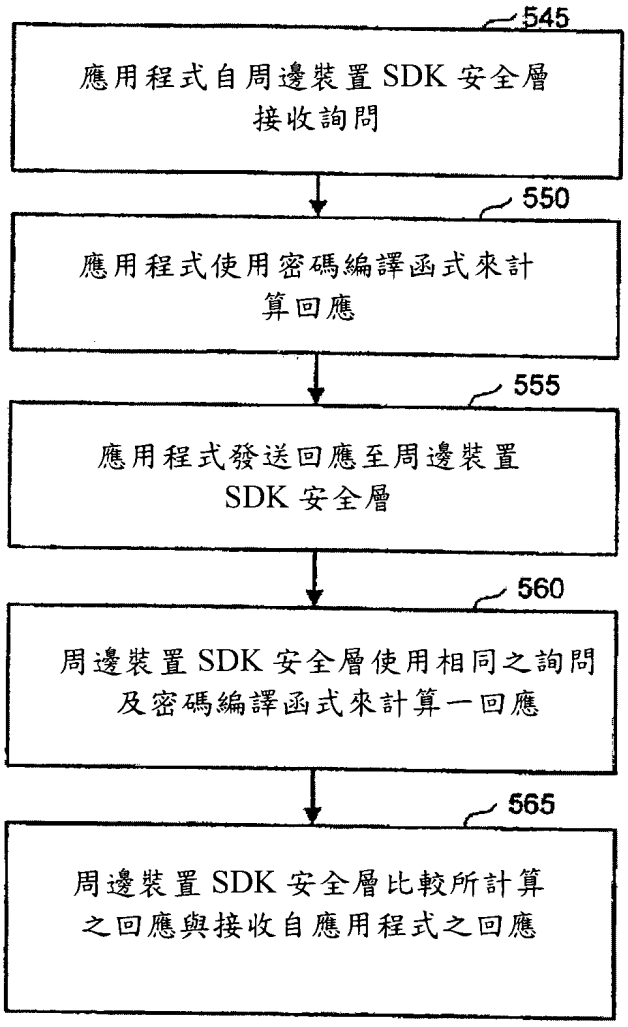


圖15B

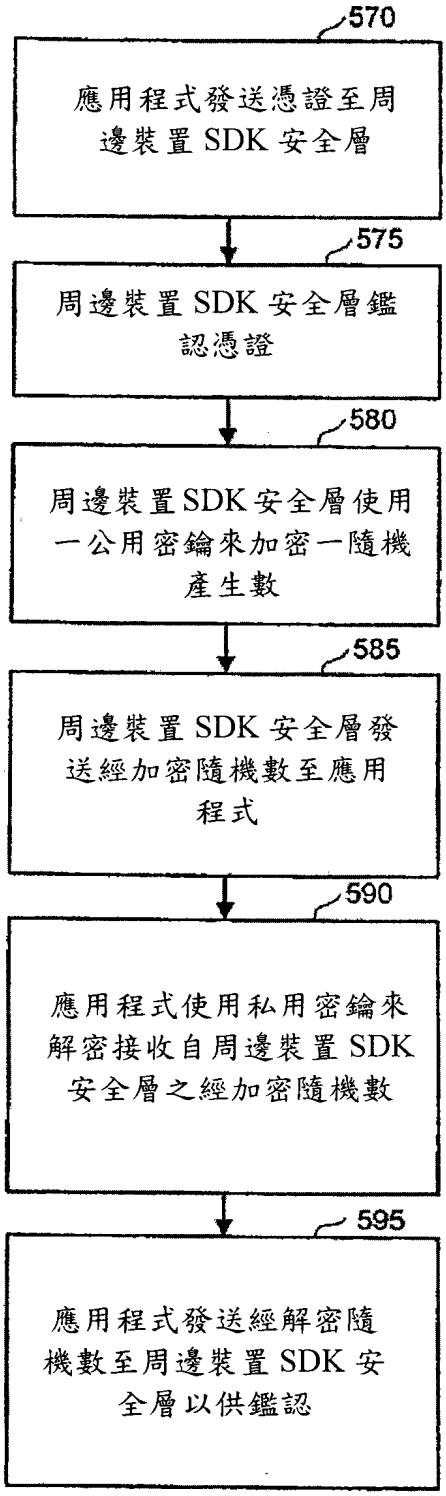


圖15C

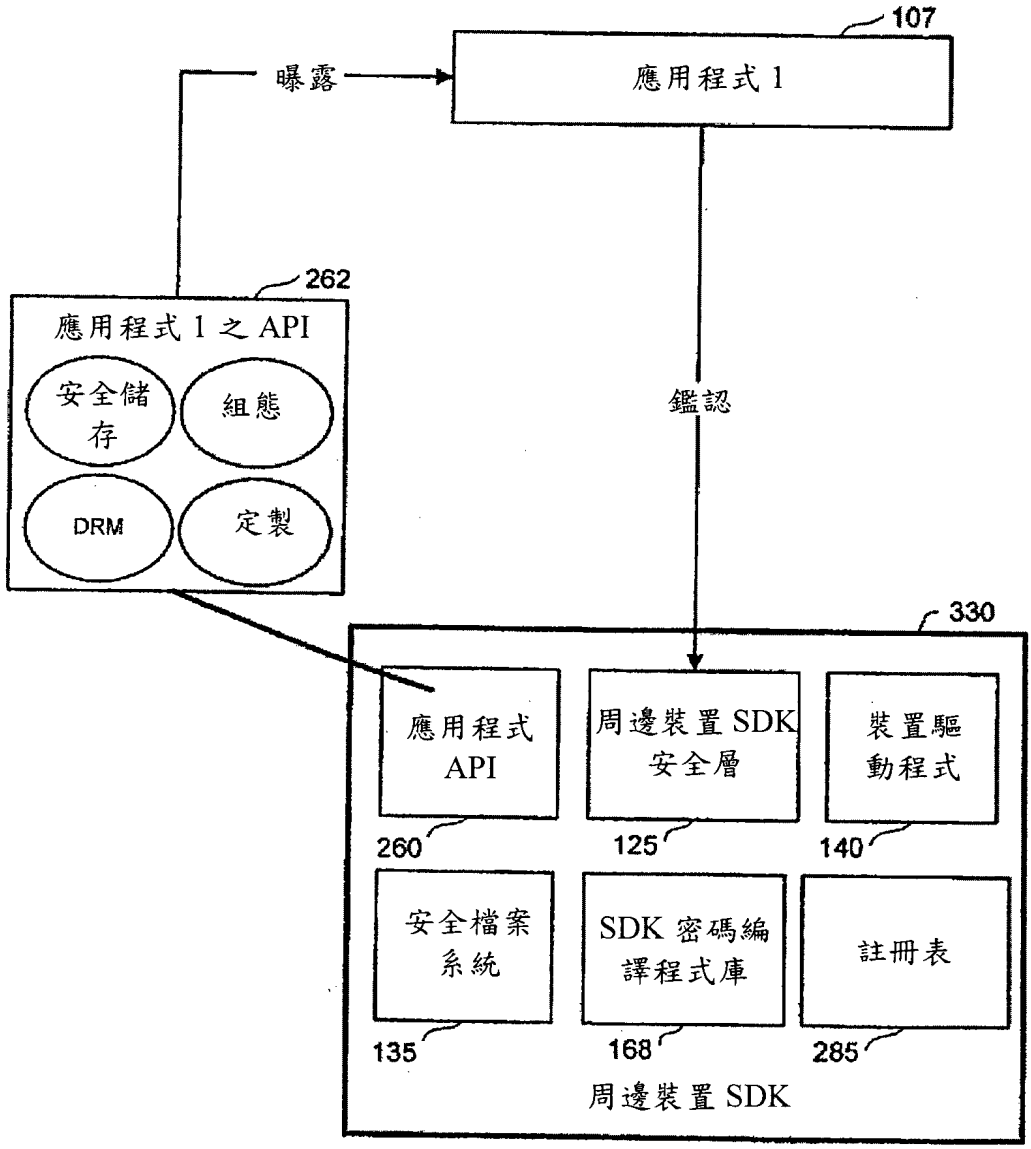

107
應用程式 1
曝露
262
應用程式 1 之 API
安全儲存
組態
DRM
定製
鑑認
330
應用程式 API
260
周邊裝置 SDK 安全層
125
裝置驅動程式
140
安全檔案系統
135
SDK 密碼編譯程式庫
168
註冊表
285
周邊裝置 SDK

圖16

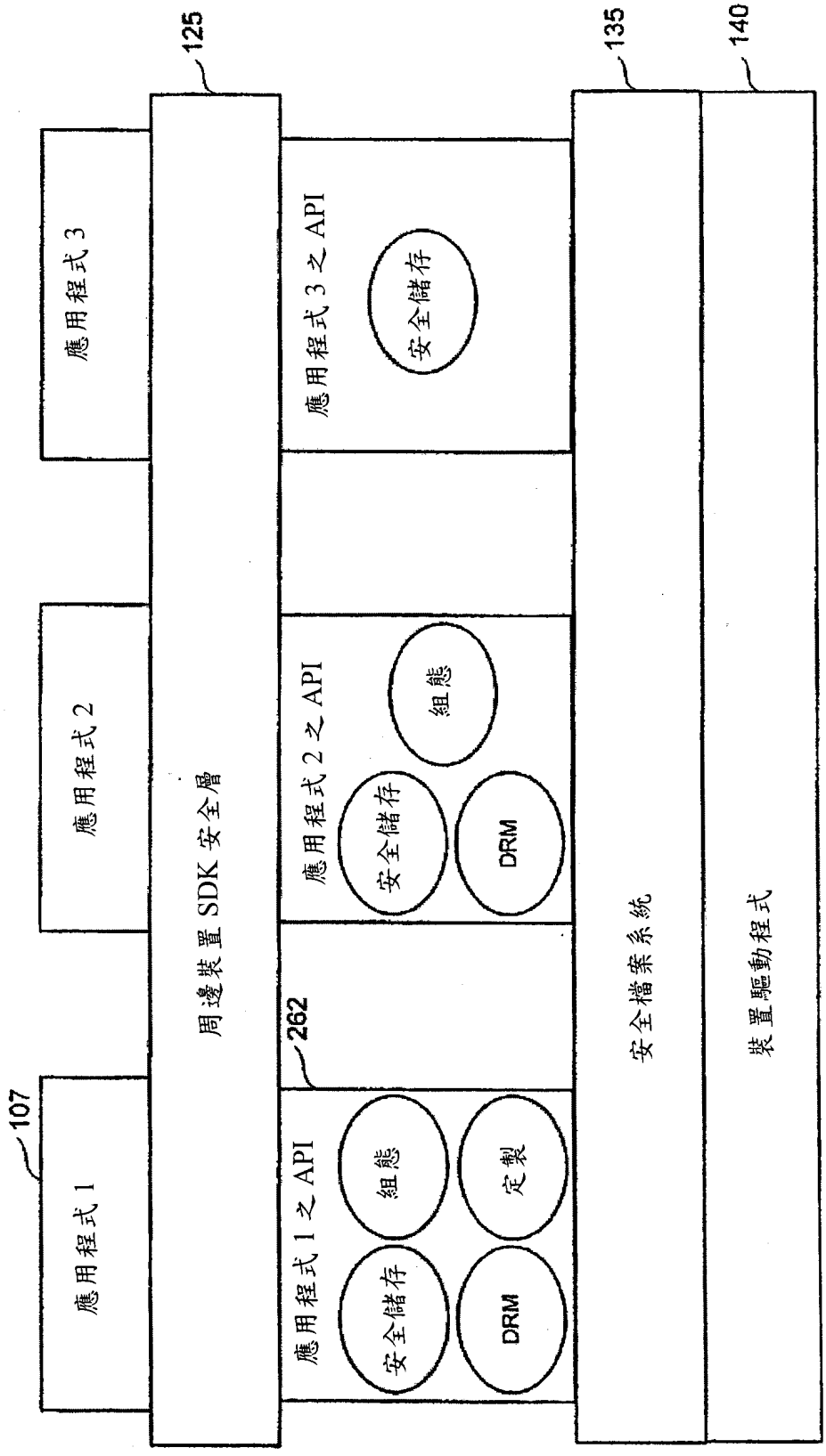

107
應用程式 1
應用程式 2
應用程式 3
125
周邊裝置 SDK 安全層
262
應用程式 1 之 API
安全儲存
組態
DRM
定製
應用程式 2 之 API
安全儲存
組態
DRM
應用程式 3 之 API
安全儲存
135
安全檔案系統
140
裝置驅動程式

圖 17

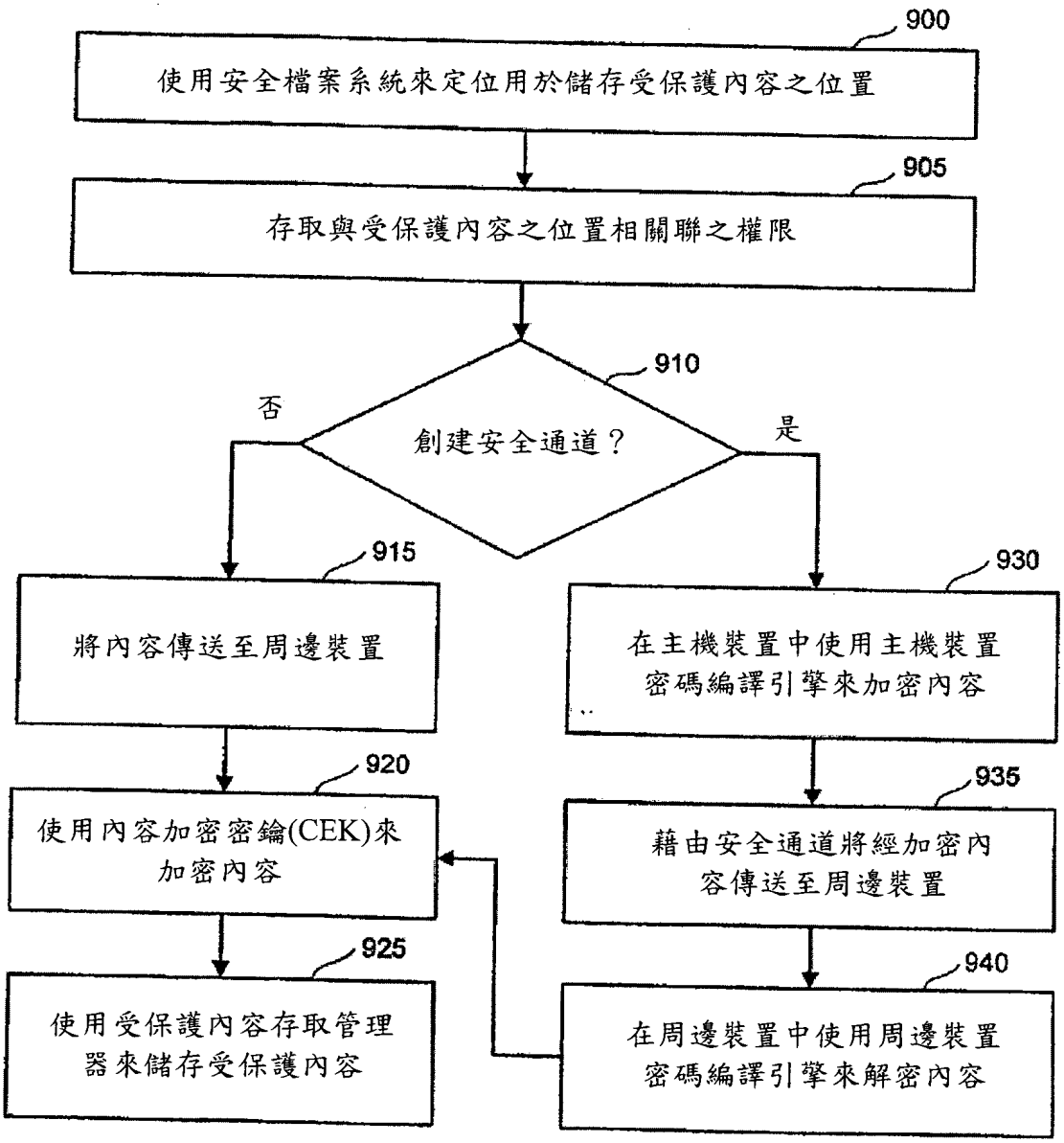

900
使用安全檔案系統來定位用於儲存受保護內容之位置
905
存取與受保護內容之位置相關聯之權限
910
創建安全通道？
否
是
915
將內容傳送至周邊裝置
920
使用內容加密密鑰(CEK)來加密內容
925
使用受保護內容存取管理器來儲存受保護內容
930
在主機裝置中使用主機裝置密碼編譯引擎來加密內容
935
藉由安全通道將經加密內容傳送至周邊裝置
940
在周邊裝置中使用周邊裝置密碼編譯引擎來解密內容

圖18

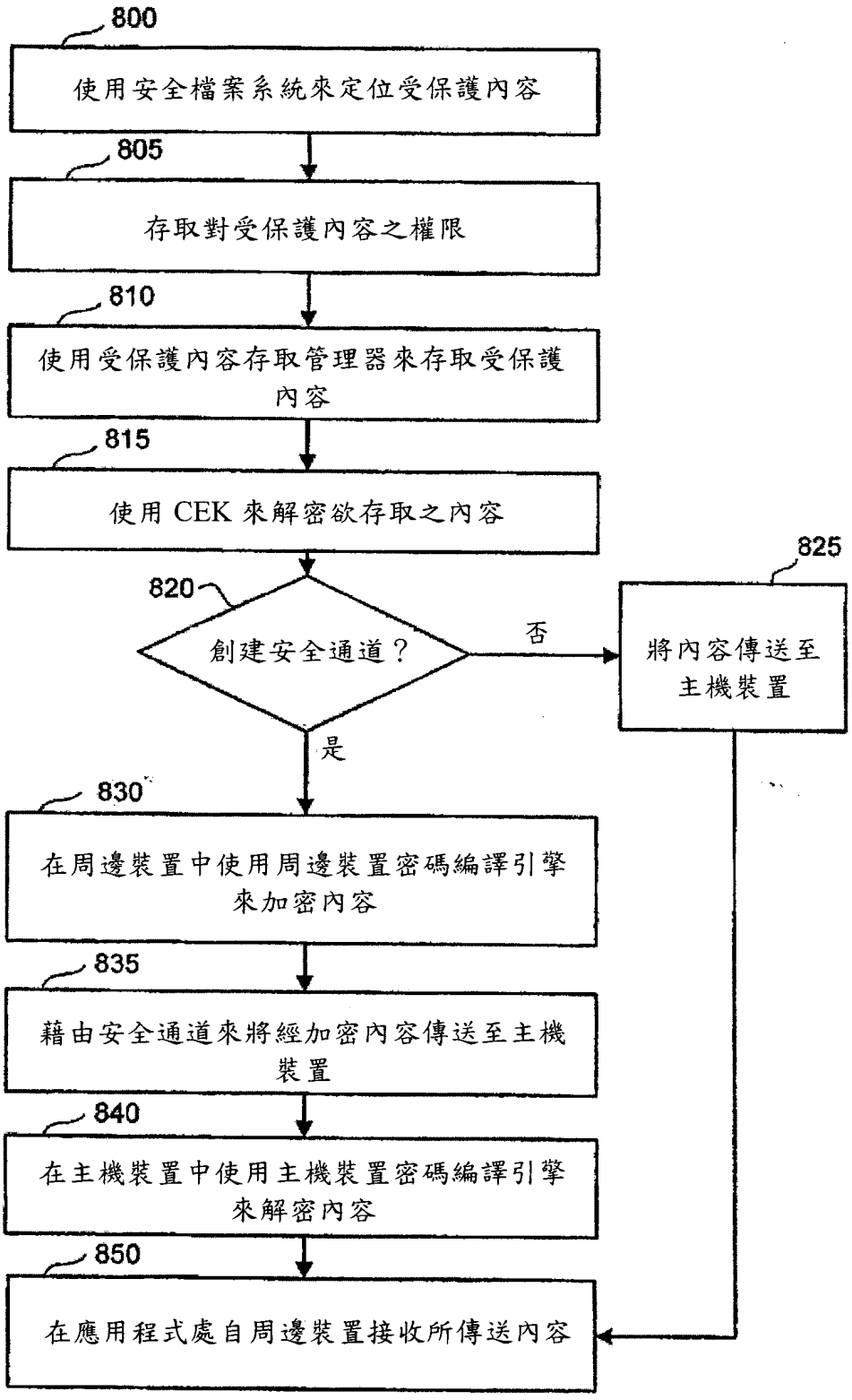

800
使用安全檔案系統來定位受保護內容
805
存取對受保護內容之權限
810
使用受保護內容存取管理器來存取受保護內容
815
使用 CEK 來解密欲存取之內容
820
創建安全通道？
否
825
將內容傳送至主機裝置
是
830
在周邊裝置中使用周邊裝置密碼編譯引擎來加密內容
835
藉由安全通道來將經加密內容傳送至主機裝置
840
在主機裝置中使用主機裝置密碼編譯引擎來解密內容
850
在應用程式處自周邊裝置接收所傳送內容

圖19

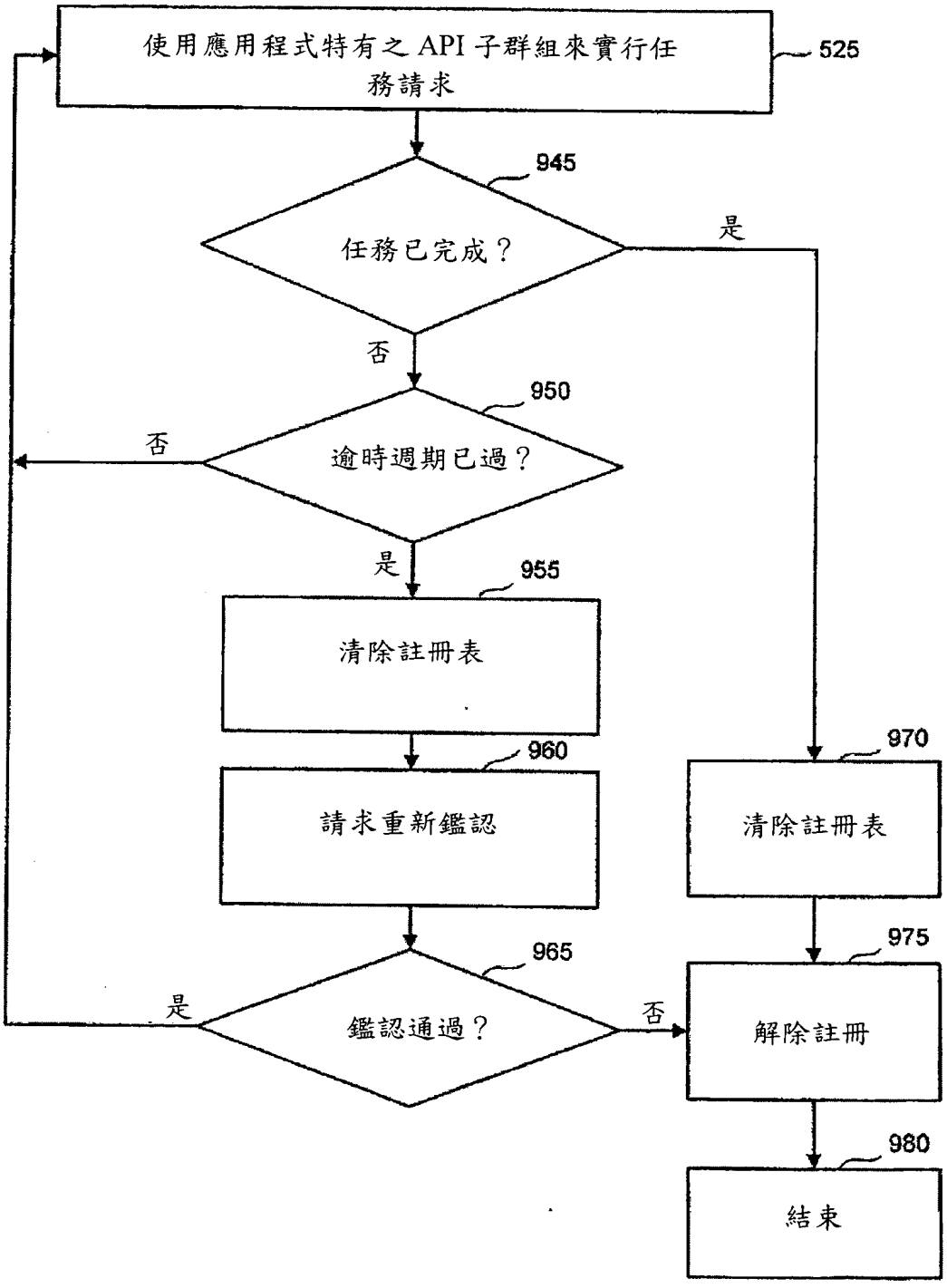

使用應用程式特有之 API 子群組來實行任務請求
525
945
任務已完成？
是
否
950
逾時週期已過？
否
是
955
清除註冊表
960
請求重新鑑認
965
鑑認通過？
是
否
970
清除註冊表
975
解除註冊
980
結束

圖20

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

105　　應用程式

165　　主機CPU

255　　主機裝置

260　　記憶體

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)