I607376

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I607376 B**

(45)公告日： 中華民國 106 (2017) 年 12 月 01 日

(21)申請案號：101112299 (22)申請日： 中華民國 101 (2012) 年 04 月 06 日

(51)Int. Cl.： ***G06F9/06 (2006.01)***

(30)優先權：2011/04/08 美國 61/473,234

(71)申請人：系微股份有限公司 (中華民國) INSYDE SOFTWARE CORP. (TW)
臺北市中山區民生東路 2 段 161 號 12 樓

(72)發明人：鮑伯辛 傑佛瑞 BOBZIN, JEFFERY JAY (US)

(74)代理人：林志剛

(56)參考文獻：

TW 480443 TW 200634618A

審查人員：李京叡

申請專利範圍項數：12 項 圖式數：3 共 34 頁

(54)名稱

用於處理改變依照統一可延伸韌體介面計算裝置中之系統安全資料庫及韌體儲存區請求的系統及方法

SYSTEM AND METHOD FOR PROCESSING REQUESTS TO ALTER SYSTEM SECURITY DATABASES AND FIRMWARE STORES IN A UNIFIED EXTENSIBLE FIRMWARE INTERFACE-COMPLIANT COMPUTING DEVICE

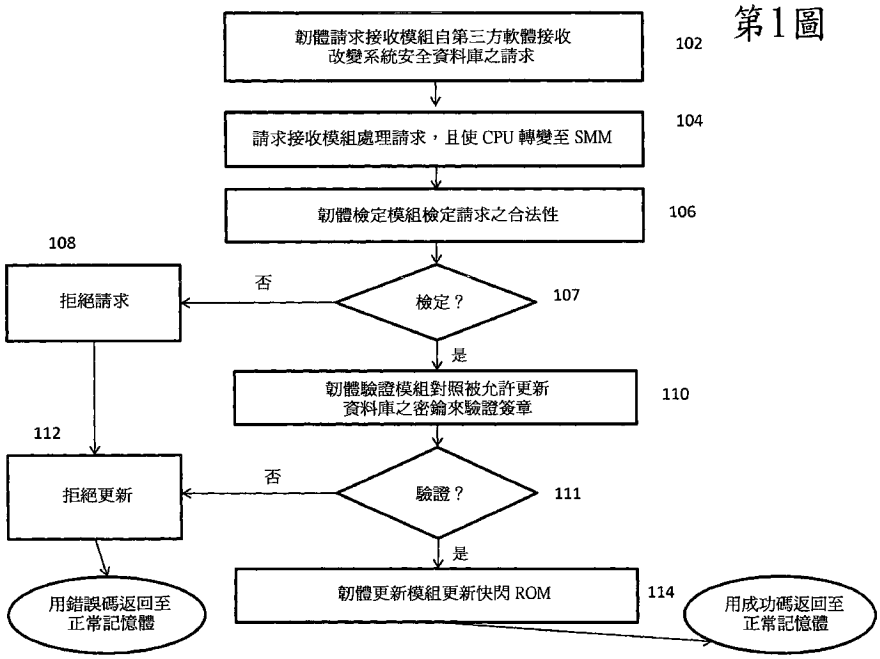
(57)摘要

本發明論述一種機制，其用於允許依照 UEFI 裝置中之韌體實施 UEFI 規範驅動程式簽署及認證變數元素，同時保護系統安全資料庫免於經受未經授權之修改，該系統安全資料庫保持核准密鑰庫以及允許及禁止的程式之列表。

A mechanism for allowing firmware in a UEFI-compliant device to implement the UEFI specification driver signing and Authenticated Variable elements while at the same time protecting the system security database holding the library of approved keys and lists of allowed and forbidden programs from unauthorized modifications is discussed.

指定代表圖：

第1圖


韌體請求接收模組自第三方軟體接收
改變系統安全資料庫之請求
102
請求接收模組處理請求，且使 CPU 轉變至 SMM
104
韌體檢定模組檢定請求之合法性
106
108
拒絕請求
否
檢定？
107
是
韌體驗證模組對照被允許更新
資料庫之密鑰來驗證簽章
110
112
拒絕更新
否
驗證？
111
是
用錯誤碼返回至
正常記憶體
韌體更新模組更新快閃 ROM
114
用成功碼返回至
正常記憶體

變數，且用以保存 UEFI 定義之安全資訊（安全資料庫）。除 UEFI 定義之資訊外，認證變數儲存區可用以儲存與電腦之最後使用相關的使用者定義之資料。因爲該使用者定義之資料含有安全資料及潛在的敏感使用者資料，所以 UEFI 規範提供以下情形：必須藉由在安全資料庫內存在識別關鍵資料來保護認證變數區/儲存區不被除彼等經授權之實體以外之任何實體改變。第三區域（亦即，UEFI 變數儲存區）含有較低安全資訊，該資訊可由使用者程式自由地更新。在各種平臺上存在某些其他區域，每一區域具有唯一的更新限制，且可擴展本文所述的方法以使之亦免於對此等區域進行未經授權之修改。

計算裝置含有稱作中央處理單元（CPU）之一或更多個元件，當在操作中時，該等 CPU 可自計算裝置讀取，且亦執行輸入-輸出命令以抹除及/或寫入快閃 ROM。CPU 具有正常操作模式及稱作系統管理模式（SMM）之第二操作模式。當 CPU 處於正常操作模式時，CPU 可存取除專用於 SMM 之某些記憶體區域之外的電腦之所有元件。相比之下，當 CPU 於 SMM 中操作時，CPU 能夠存取計算裝置之所有元件（包括專用記憶體）。電氣信號可在計算裝置之電路系統內變得可用，該電氣信號可指示 CPU 何時於 SMM 中操作。CPU 裝置可針對由稱作系統管理中斷（SMI）事件（包括由韌體觸發之 SMI 事件）之數個觸發器自正常操作模式轉變至 SMM。可利用的精確觸發器與其他系統設計略有不同，但在使用平臺合適的觸發器時，結

果始終爲主記憶體中之執行被立即暫停且執行開始於SMM 記憶體中之特定位置。某些計算裝置亦含有硬體電路，該硬體電路可偵測系統是否處於 SMM 且能夠在系統不處於 SMM時停用快閃 ROM 抹除及寫入操作。

遺憾地，現今存在各種各樣的軟體，該等軟體由未經授權的第三方建立且具有損害或破壞計算裝置（諸如 PC）之正確操作的明確意圖。給定名稱「電腦病毒」或「有毒軟體」，此等惡意軟體元件愈加以啓動過程爲目標，作爲在已載入預防性（例如，防毒）軟體之前控制計算裝置之方法。啓動攻擊軟體之示例性形式被稱作最高權力的使用者套件（root-kit）或「特洛伊啓動型病毒」。

需要不定時地更新快閃 ROM（或其他 ROM）中含有之韌體及相關資料，而不會因允許最高權力的使用者套件或特洛伊啓動型病毒存取韌體而危及計算裝置之安全性。儘管快閃 ROM 可具有稱作區塊寫入致能之內在保護裝置，但此等裝置不適合保護在系統操作期間需要更新的駐留於快閃記憶體之資料項目，同時將執行更新之能力僅限於由可信賴的主管機構產生之彼等裝置。內在快閃 ROM 保護通常由位元陣列組成，該等位元陣列在設定時防止將快閃 ROM 寫入至子區域。然而，此種類型之完整寫入防止不允許可信賴的主管機構所執行之選擇性更新。

【發明內容】

本發明之實施例提供一種機制，其用於允許依照

收已簽署系統安全資料庫修改請求並處理該請求。該請求設法執行依照 UEFI 計算裝置中之系統安全資料庫的改變。該請求接收模組在 CPU 於正常 CPU 模式操作時可執行，且在處理所接收請求之後觸發 CPU 自正常 CPU 模式轉變至系統管理模式（SMM）。CPU 亦執行韌體檢定模組，該韌體檢定模組檢定經處理請求之合法性以便執行系統安全資料庫之改變。韌體檢定模組僅在 CPU 處於 SMM 時執行。CPU 進一步執行韌體驗證模組。韌體驗證模組驗證在經處理請求中含有之簽章以便執行系統安全資料庫之改變。韌體驗證模組亦僅在 CPU 處於 SMM 時執行。CPU 額外地執行韌體更新模組。該韌體更新模組在成功驗證簽章之後執行對系統安全資料庫之所請求的改變。該韌體更新模組僅在 CPU 處於 SMM 時執行。

在另一實施例中，一種依照統一可延伸韌體介面（UEFI）計算裝置包括中央處理單元（CPU），該 CPU 經配置以執行下載更新套裝，該下載更新套裝包括可執行更新程式，該可執行更新程式用於更新依照 UEFI 計算裝置中之快閃唯讀記憶體（ROM）中之韌體儲存區域。該更新套裝進一步包括韌體儲存區之至少一部分之替代影像及替代影像之已簽署散列。該更新程式觸發 CPU 自正常 CPU 模式轉變至系統管理模式（SMM）。該裝置中之 CPU 亦執行用於驗證簽章及替代影像的 SMM 駐留韌體。用於驗證簽章及替代影像的 SMM 駐留韌體僅在 CPU 處於 SMM 模式時執行。另外，該裝置中之 CPU 執行用於用替代影像

更新韌體儲存區的 SMM 駐留韌體。用於更新韌體儲存區的 SMM 駐留韌體僅在 CPU 處於 SMM 模式時執行。

【實施方式】

本發明之實施例提供一種供依照 UEFI 計算裝置執行軟體更新之驅動程式簽章核對的機制，該機制以大大限制有毒軟體篡改核准密鑰庫及保持於系統安全資料庫中之其他資訊之能力的方式論述於 UEFI 規範中。藉由將對保持系統安全資料庫及相關聯資訊之認證變數的存取限於本文所述之技術，可藉由將處理限於發生在 SMM 內部來實施由 UEFI 展望之安全處理。因爲 SMM 記憶體避開 OS 或其他程式之檢查，所以未經授權之第三方觀察且接著修改安全過程的能力變得顯著減小。

UEFI 規範之一個主要安全特徵爲允許及禁止的程式之列表（其被允許或禁止以執行需要簽章核對之某些類型之軟體更新，及能夠添加至此等列表之代理程式之識別）由依照 UEFI 計算裝置維護。然而，若用於修改列表及允許代理程式之電腦指令存在於正常記憶體（在 CPU 處於正常操作模式時可存取）中，則決定指令之真實性的能力大大降低，此係因爲指令可能來自操作於同一記憶體空間中之惡意軟體而非來自合法的安全軟體。本發明之實施例藉由確保僅經製造商核准及核對之軟體可駐留於 SMM 記憶體中且確保僅在 CPU 處於 SMM 時才處理所有指定的安全更新而解決該問題。

保護之快閃記憶體區域的請求。非安全請求接收模組可封裝請求，且調用 SMM 進行處理。一旦 SMM 經調用，此等請求可由操作於 SMM 中之韌體模組接收並處理，該韌體模組執行對快閃 ROM 之非安全區域之所請求的修改。執行該處理，因爲快閃記憶體之基於 SMM 之保護係針對整個裝置，且因此必須經由 SMM 投送所有快閃記憶體變化。

在一個實施例中，計算裝置可包括控制電路系統之韌體模組，該電路系統用以藉由停用在 SMM 外部產生之快閃 ROM 抹除及寫入操作而保護快閃記憶體。當在將功率施加於計算裝置之後韌體開始執行時，快閃記憶體保護電路系統並不操作。因此，提供韌體模組，其執行平臺特定操作以在引入任何不可信賴的韌體之前，在啓動操作之適合點處啓用快閃記憶體保護電路系統。一旦經設定，快閃記憶體保護電路系統不可逆（藉由重設除外）。因爲在重設時系統返回至自快閃 ROM 獲得之可信賴的程式碼，所以該演算法確保在系統操作之任何時刻，快閃記憶體韌體儲存區皆不可用於受不可信賴的程式碼改變。

第 2 圖圖示使用本文所述之機制實施更新快閃 ROM 之所有或一部分韌體儲存區域之過程的一系列示例性步驟。該過程大體類似於第 1 圖中所述之過程，從而允許再使用許多共用韌體組件及有效使用韌體資源，但該過程確實包括某些差異。該系列步驟在將韌體更新套裝下載至依照 UEFI 裝置且加以執行時開始（步驟 202）。該更新套裝包

括若干部分，該等部分包括更新起始程式，該更新起始程式爲經設計以在安裝之作業系統中操作的可執行程式。除更新起始程式之外，下載更新套裝包括所有或選定部分之韌體儲存區的替代影像，以及含有更新程式之指令的資料區塊，包括（但不限於）目標系統之系統識別符。更新套裝亦包括替代影像之已簽署散列。新影像及資料區塊之已簽署散列由定義在 UEFI 規範中之密碼方法準備，該等密碼方法類似於上文對於更新認證變數區之簽署所述的彼等方法。所有或部分之更新套裝的位元組在 OEM 網站經簽署且由韌體核對。以如下方式簽署下載之更新套裝：使得有可能在建立下載後使韌體決定無下載部分已被修改。

在一個實施例中，除上文詳述之組件之外，下載套裝亦可含有補充性韌體模組以執行抹除及寫入快閃記憶體影像之實際過程。補充性韌體模組（若存在）亦由上文所述之過程簽署且類似地加以驗證。

更詳細地，更新起始程式載入至記憶體中，且核對更新套裝之其他部分的完整性。若下載完整性核對爲成功的，則更新起始程式準備記憶體位置資訊以用於將發生在 SMM 中之即將到來的操作，且使用適合於經更新之裝置平臺之方法用信號通知轉變至 SMM 的請求（步驟 204）。應瞭解，可存在數個類似的更新起始程式，每一更新起始程式具有不同變化，該等變化經設計以於特定作業系統中操作且經設計以在本發明之範疇內更新的平臺上正確地操作。作爲請求之結果，CPU 經由平臺適合技術轉變至

SMM（步驟 204）。在一個實施例中，一旦 CPU 已切換至 SMM，僅在 SMM 內操作之韌體檢定模組即可接收更新請求，且檢定請求更新起始程式之識別（步驟 206）。舉例而言，藉由對準先前記錄之更新起始程式載入位址核對 SMM 請求在記憶體中的位置且藉由檢查記憶體中之更新套裝之影像以確認尚未改變影像來檢定請求。若未檢定請求（步驟 207），則拒絕請求及更新（步驟 208 及步驟 212），在該狀況下，CPU 使用錯誤碼返回至正常記憶體模式。另一方面，若檢定請求（步驟 207），僅在 SMM 中操作之韌體驗證模組試圖藉由使用已簽署散列檢定替代韌體影像來驗證更新請求。可存在駐留於工廠安裝之快閃 ROM 影像中的一個或可能多個公開密鑰，其經啓用以驗證韌體更新影像簽章。此等密鑰駐留於受保護區域中之一者中，但根據系統之特定需求可駐留或可不駐留於認證變數區中。接收更新請求之 SMM 駐留韌體驗證模組首先執行檢定更新程式所提交之更新由經授權以執行韌體更新之私密密鑰簽署所需的密碼核對。只有當密碼核對通過時，才會將更新傳遞至負責抹除及寫入韌體儲存區域之韌體，否則將拒絕更新（步驟 212）。另一方面，在成功驗證之後，僅可在 CPU 處於 SMM 時執行之韌體更新模組更新韌體儲存區（步驟 214）。在更新韌體儲存區之後，在使用用於更新操作之成功碼返回至正常記憶體之前，UEFI 裝置將再啓動。在一些實施例中，爲了額外安全，可採用額外安全預防。舉例而言，在一個實施例中，UEFI 裝置可再

啓動隨後驗證，且在執行韌體更新之前再啓動隨後驗證。在返回至更新過程後，可再次在執行更新之前驗證更新套裝。在此類實施中，UEFI 裝置將在更新之後且在返回至正常記憶體之前第二次再啓動。

快閃 ROM 之實際抹除及寫入可需要數秒，且在系統處於 SMM 時，系統不回應於其他使用者程式。爲了提供較好的使用者體驗，當需要較大的更新時，在一個實施例中，可藉由返回至主記憶體中之呼叫程式（變數更新套裝程式或更新程式）的機制將更新之實際處理分成較小部分，其中旗標指示部分的完成。此操作分離可潛在地發生若干次。在接收到此部分完成旗標之後，呼叫程式暫停操作達某一短暫時段以允許其他使用者程式暫時地執行且接著用繼續旗標再進入 SMM。在更新程式之狀況下，可在返回至主記憶體後更新使用者螢幕上之直觀進度指示。在再進入 SMM 後，SMM 韌體採用確保在暫停期間不修改在進行中之更新之記憶體影像所需的任何步驟。僅爲了清楚起見，自第 1 圖及第 2 圖中省略此可選步驟。

第 3 圖圖示適合於實行本發明之實施例的示例性環境。依照 UEFI 計算裝置 300 包括能夠在正常模式及 SMM 中操作之 CPU 302。計算裝置 300 可爲 PC、膝上型電腦、平板計算裝置、伺服器、智慧型電話或配備有處理器且能夠遵照 UEFI 規範之需求的某一其他類型的計算裝置。計算裝置 300 亦可包括記憶體 304，諸如隨機存取記憶體（RAM）。儲存於硬驅動機或等效大量儲存裝置上、在計算

裝置 300 中或與計算裝置 300 通訊之作業系統 312 可載入至記憶體 304 中作爲計算裝置所執行之啓動過程的部分。

計算裝置 300 亦可包括快閃 ROM 320。在一些狀況下，系統設計可併有多個快閃 ROM 裝置。在該情況下，使用多個快閃 ROM 裝置，可使用相同程序存取所有快閃 ROM 裝置，且所有快閃 ROM 裝置經受上文陳述之同一安全過程。快閃 ROM 320 可包括上文所述之韌體模組，該等韌體模組可於計算裝置之操作的不同時刻操作。舉例而言，快閃 ROM 320 可包括在 CPU 302 處於正常操作（非 SMM 操作）340 時可操作的韌體請求接收模組 321。快閃 ROM 320 亦可保持韌體檢定模組 322、韌體驗證模組 323 及韌體更新模組 324，該等模組僅在 CPU 於 SMM 350 中操作時才可操作。儘管本文中之描述將韌體檢定模組 322、韌體驗證模組 323 及韌體更新模組 324 描述爲單獨模組，但應瞭解，在不脫離本發明之範疇的情況下，可將模組之功能性組合至更小或更大數目個模組中。

快閃 ROM 320 可在邏輯上分割成若干功能區域。因此，快閃 ROM 320 可包括保持系統安全資料庫 331 之認證變數區 330。系統安全資料庫 331 保持用於 UEFI 規範中陳述之簽章核對之經授權的密鑰，且僅在 CPU 於 SMM 350 中操作時才可存取。類似地，快閃 ROM 320 亦可包括韌體儲存區 332，韌體儲存區 332 保持起動及安全韌體模組之可載入影像 333。快閃 ROM 320 亦可包括 UEFI 變數儲存區域 334。應瞭解，在不脫離本發明之範疇的情況下

，快閃 ROM 320 可以不同方式進行邏輯分割以包括不同於或涵蓋本文所述之區域的其他區域。

本發明之實施例可全部或部分地提供爲實施於一或更多個實體媒體上或中之一或更多個非暫時性電腦可讀取程式。舉例而言，媒體可爲軟碟、硬碟、光碟、數位多功能光碟、快閃記憶體、PROM、MRAM、RAM、ROM 或磁帶。通常，可用任何程式設計語言實施電腦可讀取程式。可使用之語言的一些實例包括 FORTRAN、C、C++、C#、Python、ActionScript、JavaScript 或 Java。軟體程式可儲存於一或更多個媒體上或中作爲目標碼。可使用硬體加速，且所有或一部分之程式碼可執行於 FPGA、特殊應用積體處理器（ASIP）或特殊應用積體電路（ASIC）上。程式碼可執行於虛擬化環境中，諸如虛擬機中。執行程式碼之多個虛擬機可駐留於單一處理器上。

由於在不脫離本發明之範疇的情況下可進行某些變化，所以意欲將以上描述中含有或隨附圖式中圖示之所有物質解釋爲說明性的而並非拘泥於字面意義。此項技術之從業人員將認識到，在不脫離本發明之範疇的情況下可改變圖式中所示之一系列步驟及架構，及本文中含有之說明爲本發明之許多可能敘述的單一實例。特定言之，應注意，在某些實施例內，第 2 圖中所述之步驟可經修改或由類似過程替代，而無需改變第 1 圖之步驟。此外，儘管爲了易於闡釋起見，本文中之描述論述了認爲係特定軟體模組所有的各種功能性，但應瞭解，在不脫離本發明之範疇的情

況下，模組可被不同地命名或以未特定論述之方式被組合或分割以便提供相同功能性。

本發明之示例性實施例之以上描述提供說明及描述，但不意欲爲詳盡的或將本發明限於所揭示之精確形式。根據以上教示，修改及變化爲可能的，且可自本發明之實踐獲取修改及變化。舉例而言，儘管已描述一系列動作，但可在與本發明之原理一致的其他實施中修改動作之次序。此外，可並行地執行非附屬動作。

【圖式簡單說明】

併入本說明書中且構成本說明書之一部分的隨附圖式圖示本發明之一或更多個實施例，且與描述一起有助於闡釋本發明。在圖式中：

第 1 圖圖示由本發明之實施例執行以利用依照 UEFI 裝置中之韌體模組的一系列示例性步驟；

第 2 圖圖示由本發明之實施例執行以利用依照 UEFI 裝置中之韌體模組更新快閃 ROM 之韌體儲存區的一系列示例性步驟；以及

第 3 圖圖示適合於實行本發明之實施例的示例性環境。

【主要元件符號說明】

102：步驟

104：步驟

106：步驟

107：步驟

108：步驟

110：步驟

111：步驟

112：步驟

114：步驟

202：步驟

204：步驟

206：步驟

207：步驟

208：步驟

210：步驟

211：步驟

212：步驟

214：步驟

300：計算裝置

302：CPU

304：記憶體

312：作業系統

320：快閃 ROM

321：韌體請求接收模組

322：韌體檢定模組

323：韌體驗證模組

324：韌體更新模組

330：認證變數區

331：系統安全資料庫

332：韌體儲存區

333：起動及安全韌體模組之可載入影像

334：UEFI 變數儲存區域

340：正常操作/非 SMM 操作

350：SMM

公告本

發明專利說明書

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101112299

※申請日：101 年 04 月 06 日　　※IPC 分類： G06F 9/06 (2006.01)

一、發明名稱：（中文／英文）

用於處理改變依照統一可延伸韌體介面計算裝置中之系統安全資料庫及韌體儲存區請求的系統及方法

System and method for processing requests to alter system security databases and firmware stores in a unified extensible firmware interface-compliant computing device

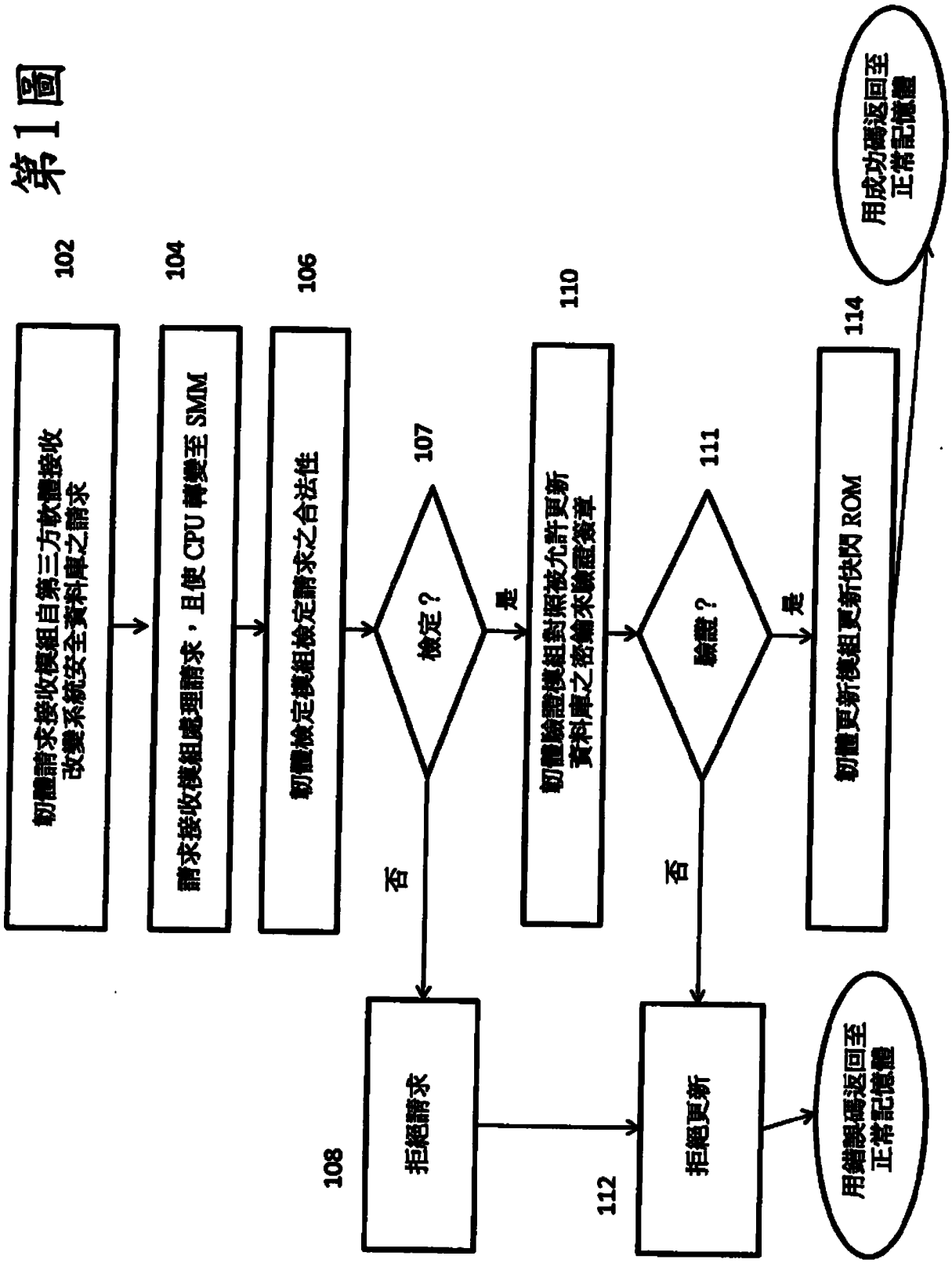
二、中文發明摘要：

本發明論述一種機制，其用於允許依照 UEFI 裝置中之韌體實施 UEFI 規範驅動程式簽署及認證變數元素，同時保護系統安全資料庫免於經受未經授權之修改，該系統安全資料庫保持核准密鑰庫以及允許及禁止的程式之列表。

三、英文發明摘要：

A mechanism for allowing firmware in a UEFI-compliant device to implement the UEFI specification driver signing and Authenticated Variable elements while at the same time protecting the system security database holding the library of approved keys and lists of allowed and forbidden programs from unauthorized modifications is discussed.

第1圖


102
韌體請求接收模組自第三方軟體接收改變系統安全資料庫之請求
104
請求接收模組處理請求，且使 CPU 轉變至 SMM
106
韌體檢定模組檢定請求之合法性
107
檢定？
否
是
108
拒絕請求
110
韌體驗證模組對照被允許更新資料庫之密鑰來驗證簽章
111
驗證？
否
是
112
拒絕更新
114
韌體更新模組更新快閃 ROM
用成功碼返回至正常記憶體
用錯誤碼返回至正常記憶體

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：無

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

六、發明說明：

【發明所屬之技術領域】

相關申請案

本申請案係關於 2011 年 4 月 8 日提出申請的題爲「System and Method for Processing Requests to Alter a System Security Database in a Unified Extensible Firmware Interface (UEFI)-Compliant Device」的美國臨時專利申請案第 61/473234 號且主張其權益，該美國臨時專利申請案之全部內容以引用方式併入本文中。

【先前技術】

統一可延伸韌體介面（UEFI）爲由非營利產業機構建立的規範，該規範詳述了作業系統與計算裝置（諸如（但不限於）個人電腦（PC））所包括的韌體之間的程式設計介面。UEFI 規範描述一套工具，計算裝置可使用該套工具以有組織的方式自功率施加狀態移至完全可操作狀態。計算裝置由包括在該裝置內之韌體初始化，且該韌體提供一定範圍的軟體服務，其促進啓動作業系統以及提供此等服務之較小子集，在已啓動作業系統之後,此等服務持續可用。UEFI 規範告知所要結果，但故意未指定實施之內部策略。UEFI 韌體規範替代由產業先前使用且通常被稱爲傳統 BIOS 之較早的 OS/韌體介面。

UEFI 規範提供稱作驅動程式簽章核對之設施，來自其他方之軟體可藉由該設施使用公開/私密密鑰密碼技術

而「簽署」於軟體來源處。在允許該軟體操作之前，該簽章由計算裝置之韌體驗證。該簽章核對集中於經添加以配置可選組件（插入板）之軟體及由作業系統爲早期啓動步驟而供應之軟體（OS 啓動載入器）。用核准密鑰庫來實現簽章核對。計算裝置必須注意不允許未經授權的軟體元件具有修改核准密鑰庫的任何能力，因爲此舉將允許惡意軟體元件使簽章核對失效。

當實施於計算裝置中時，UEFI 韌體之機器碼及韌體所使用之所有永久資料駐留於唯讀記憶體（ROM）中。在許多狀況下，ROM 爲稱作快閃 ROM 之電可抹除矽裝置。快閃 ROM 具有以下特性：快閃 ROM 可由電氣命令抹除，且可接著寫入個別元件，且裝置將無時間限制地保留資料。當首先將功率施加於計算裝置時，系統執行稱作重設之過程，該過程清除該狀態至已知條件且開始執行韌體。自快閃 ROM 讀取韌體。在其他服務中，韌體負責操作計算裝置直至可執行啓動過程，該啓動過程將計算裝置之作業系統載入至記憶體中。一旦經載入，作業系統負責計算裝置之正常操作。應注意，計算裝置之防毒程式需要在該等程式可操作之前載入作業系統。

可將快閃 ROM 之內容在邏輯上分割爲若干功能劃分或區域。一個此區域爲韌體儲存區，其包括起動韌體及安全韌體模組之可載入影像，且必須被保護不受除已被授權更新韌體儲存區之實體以外之任何實體改變。稱作認證變數區或儲存區之第二區域保存在 UEFI 規範中定義的認證

S

UEFI 裝置中之韌體實施 UEFI 規範驅動程式簽章核對及認證變數元素，同時防止對快閃 ROM 之區域進行未經授權之修改。藉由本文所述之過程，將不受未經授權之修改的保護提供至數個安全性關鍵元件，該未經授權之修改將使計算裝置易受惡意軟體攻擊，該等安全性關鍵元件包括：（1）快閃 ROM 之認證變數區（含有安全資料庫）；（2）快閃 ROM 韌體儲存區之含有韌體模組之可載入影像的彼等部分；以及（3）韌體模組之 SMM 記憶體中的可執行影像，該等韌體模組核對授權且執行對快閃 ROM 之安全資料庫及韌體儲存區域的更新。在認證變數區中含有的安全資料庫保持各種資訊，其包括核准密鑰庫以及允許及禁止的程式之列表，而含有韌體模組之可載入影像的韌體儲存區之部分包括起動韌體模組與安全韌體模組兩者。更特定言之，本發明之實施例利用僅能夠在 CPU 處於 SMM 時存取及執行之韌體模組。因此，本發明之韌體模組避開 OS 或使用者程式之檢查及修改，且可以不同於觀察或修改之方式執行對 UEFI 簽章核對及其他技術的安全處理。

在一個實施例中，一種用於處理依照統一可延伸韌體介面（UEFI）計算裝置中之系統安全資料庫請求的方法包括以下步驟：自作業系統模組接收已簽署之系統安全資料庫修改請求。該已簽署之請求設法執行依照 UEFI 計算裝置中之系統安全資料庫的改變。該請求由韌體請求接收模組處理，該韌體請求接收模組由在計算裝置中之中央處理單元（CPU）於正常 CPU 模式中操作時可存取的程式碼組

成。該方法觸發使用請求接收模組將 CPU 自正常 CPU 模式轉變至系統管理模式（SMM），且檢定經處理請求之合法性以便用僅在 CPU 處於 SMM 時可執行之韌體檢定模組執行系統安全資料庫之改變。該方法額外地驗證經處理請求中含有之簽章以便執行系統安全資料庫之改變。使用僅在 CPU 處於 SMM 時可執行之韌體驗證模組發生驗證。該方法在成功驗證請求中之簽章之後執行對使用韌體更新模組作出請求的系統安全資料庫之改變。該韌體更新模組僅在 CPU 處於 SMM 時才可執行。

在另一實施例中，一種用於更新依照統一可延伸韌體介面（UEFI）計算裝置中之快閃唯讀記憶體（ROM）中之韌體儲存區域的方法包括以下步驟：在依照 UEFI 裝置處接收下載更新套裝，該下載更新套裝包括可執行更新程式、韌體儲存區之替代影像及替代影像之已簽署散列（hash）。該方法亦包括以下步驟：在依照 UEFI 計算裝置中之中央處理單元（CPU）於正常 CPU 模式操作時，用更新程式觸發 CPU 自正常 CPU 模式轉變至系統管理模式（SMM）。該方法進一步用僅在 CPU 處於 SMM 時才可執行之 SMM 駐留韌體驗證簽章及替代影像，且用替代影像更新韌體儲存區。使用僅在 CPU 處於 SMM 時才可執行之 SMM 駐留韌體發生更新。

在實施例中，一種依照統一可延伸韌體介面（UEFI）計算裝置包括中央處理單元（CPU），該 CPU 經配置以執行韌體請求接收模組。該請求接收模組自作業系統模組接

S

本發明之實施例在執行未在工廠指定及載入之任何軟體之前關閉及鎖定對 SMM 記憶體之存取，該軟體具有經過後工廠（post-factory）修正（僅由本文所述之安全韌體更新過程應用）的工廠影像。對存取及修正之該限制大大增強計算裝置執行 UEFI 規範中展望之簽章核對的能力。經由使用集中於安全處理更新請求之韌體模組，可處理更新以確保請求僅來源於有效實體。

第 1 圖圖示由本發明之實施例執行以利用依照 UEFI 裝置中之韌體模組的一系列示例性步驟。該系列步驟在韌體請求接收模組接收軟體更新之已簽署請求時開始，該軟體更新將需要改變認證變數，諸如保持系統安全資料庫之變數，該系統安全資料庫包括用以執行簽章核對之核准密鑰庫（步驟 102）。可經由 UEFI 執行時間介面（UEFI run-time interface）來接收請求。應注意，韌體請求接收模組在 CPU 於正常模式中操作時可操作且可存取。在接收到請求後，韌體請求接收模組核對請求格式，並保存用於基於 SMM 之程式碼的特定記憶體位置資訊，且藉由適合於用於處理請求之系統平臺的特定方法使 CPU 轉變至 SMM（步驟 104）。舉例而言，在一些系統中，該轉變可藉由調用 SMI 中斷而經觸發。一旦 CPU 於 SMM 中操作，僅在 CPU 於 SMM 中操作時才操作之韌體檢定模組接收請求，且藉由對照先前記錄之請求接收模組載入位址核對 SMM 請求在記憶體中之位置且藉由檢查記憶體中之套裝模組之影像以確認已改變影像，檢定該請求實際上來自韌體請求接收模組（步驟 106）。若未

檢定該請求，則拒絕該請求（步驟 108）。應瞭解，無效請求可觸發顯示或登入警報信號，且將 UEFI 定義之錯誤碼傳回至請求更新之軟體。若請求被檢定爲來自請求接收模組，則僅可在 SMM 中操作之韌體驗證模組檢查包括於資料庫更新請求中之簽章資訊，且使用系統安全資料庫中之至少一個密鑰執行簽章核對（步驟 110）。應注意，在其他實施例中，系統可在更大或更小安全性之條件下操作，且簽章核對之精確策略或規則可根據系統狀態而不同。然而，不管條件之此等變化如何，對於本發明之實施例而言，簽章核對之當前可應用的策略由 SMM 駐留模組根據記錄於受保護的系統安全資料庫中之狀態資訊來應用。

計算裝置可利用公開/私密密鑰加密作爲認證變數更新驗證過程之部分。更新請求可包括內容及內容之至少部分的已簽署散列（hash），該散列（hash）由請求實體擁有之私密密鑰簽署或加密。作爲驗證過程之部分，驗證模組可重建更新內容之部分的散列（使用同一散列演算法簽署該散列）、用來自系統安全資料庫之相應的且經授權的公開密鑰解密已簽署散列，並比較原始散列與新散列。若經授權的密鑰不存在於系統安全資料庫中及/或散列爲不相同的，則請求爲無效的（步驟 112），且拒絕更新。若請求被決定爲有效的，則僅在 CPU 處於 SMM 時才操作之韌體更新模組處理該請求，且更新快閃 ROM（步驟 114）。

在一個實施例中，在 CPU 處於正常模式時操作之非安全韌體請求接收模組可用以接收更新未受簽章更新限制

第 101112299 號 民國 105 年 7 月 28 日修正

七、申請專利範圍：

1.一種用於處理一依照統一可延伸韌體介面（UEFI）計算裝置中之系統安全資料庫請求的方法，其包括：

自一作業系統模組接收一已簽署系統安全資料庫修改請求，該請求設法執行對該依照 UEFI 計算裝置中之一系統安全資料庫之一改變，該請求由一韌體請求接收模組處理，該請求接收模組在該計算裝置中之一中央處理單元（CPU）於一正常 CPU 操作模式中操作時可執行；

用該韌體請求接收模組保存與該系統安全資料庫修改請求相關的記憶體位置資訊，以供一韌體檢定模組使用，只有當該 CPU 處於一系統管理模式(SMM)時該韌體檢定模組可執行，在觸發該 CPU 自該正常 CPU 操作模式至 SMM 之轉變之前，保存該記憶體位置資訊；

使用該請求接收模組來觸發該 CPU 自該正常 CPU 操作模式至 SMM 之該轉變；

使用僅當該 CPU 處於 SMM 時才可執行的該韌體檢定模組來檢定該韌體請求接收模組的識別，該檢定步驟係藉由對照一先前記錄之請求接收模組載入位址核對該請求的記憶體中之位置而執行，以辨識被處理的該請求的起源；

驗證在該經處理請求中含有之一簽章以便執行該系統安全資料庫之一改變，使用僅在該 CPU 處於 SMM 時才可執行之一韌體驗證模組發生該驗證步驟；以及

執行使用一韌體更新模組作出請求的該系統安全資料庫之該改變，在該簽章之一成功驗證後發生該改變，該韌

體更新模組僅在該 CPU 處於 SMM 時才可執行。

2.如申請專利範圍第 1 項之方法，其中該韌體驗證模組驗證該請求中之該簽章以便使用儲存於一系統安全資料庫中之一密鑰執行該系統安全資料庫之一改變。

3.如申請專利範圍第 1 項之方法，其中該韌體請求接收模組、該韌體檢定模組、該韌體驗證模組、該韌體更新模組及該系統安全資料庫儲存於快閃 ROM 中。

4.一種用於更新一依照統一可延伸韌體介面（UEFI）計算裝置中之一快閃唯讀記憶體（ROM）中之一韌體儲存區域的方法，其包括：

在該依照 UEFI 計算裝置處接收一下載更新套裝，其包括一可執行更新程式、該韌體儲存區之一替代影像及該替代影像之一已簽署散列；

當該依照 UEFI 計算裝置中之一中央處理單元（CPU）於一正常 CPU 操作模式中操作時，執行該更新程式，該更新程式產生用於該韌體儲存區之一更新請求；

用該更新程式保存與該更新套裝相關的記憶體位置資訊，以供用於檢定該更新程式的韌體使用，只有當該 CPU 處於一系統管理模式(SMM)時用於檢定該更新程式的該韌體可執行，在觸發該 CPU 自該正常 CPU 操作模式至 SMM 之轉變之前，保存該記憶體位置資訊；

當該 CPU 於該正常 CPU 操作模式中操作時，用該更新程式觸發該 CPU 自該正常 CPU 操作模式至 SMM 之一轉變；

S

當該 CPU 處於 SMM 時，檢定該更新請求是來自於該更新程式，該檢定步驟係藉由對照一先前記錄之更新程式載入位址核對該更新請求的記憶體中之位置而執行，以辨識該更新請求的起源；

用僅在該 CPU 處於 SMM 時才可執行之 SMM 駐留韌體驗證簽章及替代影像；以及

用該替代影像更新該韌體儲存區，使用僅在該 CPU 處於 SMM 時才可執行之 SMM 駐留韌體發生該更新步驟。

5.如申請專利範圍第 4 項之方法，其中在該驗證步驟之後且在該更新該韌體儲存區之步驟之前，該依照 UEFI 計算裝置再啓動。

6.一種保持電腦可執行指令之非暫時性電腦可讀取媒體，該等電腦可執行指令用於處理一依照統一可延伸韌體介面（UEFI）計算裝置中之系統安全資料庫請求，該等指令在經執行時使至少一個計算裝置：

自一作業系統模組接收一已簽署系統安全資料庫修改請求，該請求設法執行該依照 UEFI 計算裝置中之一系統安全資料庫之一改變，該請求由一韌體請求接收模組處理，該請求接收模組之程式碼在該計算裝置中之一中央處理單元（CPU）於一正常 CPU 模式中操作時可存取；

用該韌體請求接收模組保存與該系統安全資料庫修改請求相關的記憶體位置資訊，以供一韌體檢定模組使用，只有當該 CPU 處於一系統管理模式(SMM)時該韌體檢定模組可執行，在觸發該 CPU 自該正常 CPU 操作模式至 SMM

之轉變之前，保存該記憶體位置資訊；

使用該請求接收模組來觸發該 CPU 自該正常 CPU 操作模式至 SMM 之該轉變；

使用該韌體檢定模組來檢定該韌體請求接收模組的識別，該檢定步驟係藉由對照一先前記錄之請求接收模組載入位址核對該請求的記憶體中之位置而執行，以辨識被處理的該請求的起源；

驗證在該經處理請求中含有之一簽章以便執行該系統安全資料庫之一改變，使用僅在該 CPU 處於 SMM 時才可執行之一韌體驗證模組發生該驗證；以及

執行使用一韌體更新模組作出請求的該系統安全資料庫之該改變，在該簽章之一成功驗證後發生該改變，該韌體更新模組僅在該 CPU 處於 SMM 時才可執行。

7.如申請專利範圍第 6 項之媒體，其中該韌體驗證模組驗證該請求中之該簽章以便使用儲存於一系統安全資料庫中之一密鑰執行該系統安全資料庫之一改變。

8.一種保持電腦可執行指令之非暫時性電腦可讀取媒體，該等電腦可執行指令用於更新一依照統一可延伸韌體介面（UEFI）計算裝置中之一快閃唯讀記憶體（ROM）中之一韌體儲存區域，該等指令在經執行時使至少一個計算裝置：

在該依照 UEFI 裝置處接收一下載更新套裝，其包括一可執行更新程式、該韌體儲存區之一替代影像及該替代影像之一已簽署散列；

S

當該依照 UEFI 計算裝置中之一中央處理單元（CPU）於一正常 CPU 操作模式中操作時，執行該更新程式，該更新程式產生用於該韌體儲存區之一更新請求；

用該更新程式保存與該更新套裝相關的記憶體位置資訊，以供用於檢定該更新程式的韌體使用，只有當該 CPU 處於一系統管理模式(SMM)時用於檢定該更新程式的該韌體可執行，在觸發該 CPU 自該正常 CPU 操作模式至 SMM 之轉變之前，保存該記憶體位置資訊；

在該依照 UEFI 計算裝置中之一中央處理單元（CPU）於一正常 CPU 模式中操作時，用該更新程式觸發該 CPU 自該正常 CPU 模式至一系統管理模式（SMM）之一轉變；

當該 CPU 處於 SMM 時，檢定該更新請求是來自於該更新程式，該檢定步驟係藉由對照一先前記錄之更新程式載入位址核對該更新請求的記憶體中之位置而執行，以辨識該更新請求的起源；

用僅在該 CPU 處於 SMM 時才可執行之 SMM 駐留韌體驗證簽章及替代影像；以及

用該替代影像更新該韌體儲存區，使用僅在該 CPU 處於 SMM 時才可執行之 SMM 駐留韌體發生該更新。

9.如申請專利範圍第 8 項之媒體，其中在該驗證之後且在該更新該韌體儲存區之前，該依照 UEFI 計算裝置再啓動。

10.一種依照統一可延伸韌體介面（UEFI）計算裝

置，其包括一中央處理單元，該中央處理單元經配置以執行：

一韌體請求接收模組，用以自一作業系統模組接收一已簽署系統安全資料庫修改請求並處理該請求，該請求設法執行該依照 UEFI 計算裝置中之一系統安全資料庫之一改變，該請求接收模組在該計算裝置中之一中央處理單元（CPU）於一正常 CPU 操作模式中操作時可執行，且該韌體請求接收模組用以保存與該系統安全資料庫修改請求相關的記憶體位置資訊，以供一韌體檢定模組使用，只有當該 CPU 處於一系統管理模式(SMM)時該韌體檢定模組可執行，在該處理之後，在觸發該 CPU 自該正常 CPU 操作模式至 SMM 之一轉變之前，保存該記憶體位置資訊；

該韌體檢定模組，用以檢定該韌體請求接收模組的識別，該檢定步驟係藉由對照一先前記錄之請求接收模組載入位址核對該請求的記憶體中之位置而執行，以辨識被處理的該請求的起源；

一韌體驗證模組，用以驗證在該經處理請求中含有之一簽章以便執行該系統安全資料庫之一改變，該韌體驗證模組僅在該 CPU 處於 SMM 時才執行；以及

一韌體更新模組，用以在該簽章之一成功驗證之後執行該系統安全資料庫之該所請求的改變，該韌體更新模組僅在該 CPU 處於 SMM 時才執行。

11.如申請專利範圍第 10 項之裝置，其中該韌體驗證模組驗證該請求中之該簽章以便使用儲存於一系統安全資

S

料庫中之一密鑰執行該系統安全資料庫之一改變。

12.一種依照統一可延伸韌體介面（UEFI）計算裝置，其包括一中央處理單元（CPU），該 CPU 經配置以執行：

一下載更新套裝，其包括一可執行更新程式，該更新程式用於更新該依照 UEFI 計算裝置中之一快閃唯讀記憶體（ROM）中之一韌體儲存區域，該更新套裝進一步包括該韌體儲存區之至少部分之一替代影像及該替代影像之一已簽署散列，當該依照 UEFI 計算裝置中之該 CPU 於一正常 CPU 操作模式中操作時，執行該更新程式，該更新程式產生用於該韌體儲存區之一更新請求且觸發該 CPU 自該正常 CPU 操作模式至一系統管理模式（SMM）之一轉變，用以使用該替代影像更新該韌體儲存區，用該更新程式保存與該更新套裝相關的記憶體位置資訊，以供用於檢定該更新程式的韌體使用，在該觸發該 CPU 自該正常 CPU 操作模式至 SMM 之該轉變之前，保存該記憶體位置資訊；

該韌體用以檢定該更新程式，該韌體僅當該 CPU 處於 SMM 時才可執行，該檢定步驟係藉由對照一先前記錄之更新程式載入位址核對該更新請求的記憶體中之位置而執行，以辨識該更新請求的起源；

用於驗證簽章及替代影像之韌體，該用於驗證該簽章及替代影像之韌體僅在該 CPU 處於 SMM 時才執行；以及

用於用該替代影像更新該韌體儲存區之韌體，該用於

更新該韌體儲存區之韌體僅在該 CPU 處於 SMM 時才執行。