I684890

(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 I684890 B**

(45)公告日： 中華民國 109 (2020) 年 02 月 11 日

(21)申請案號：105104313 (22)申請日： 中華民國 105 (2016) 年 02 月 15 日

(51)Int. Cl.： ***G06F21/62 (2013.01)***

(30)優先權：2015/02/13 美國 62/115,891

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

(72)發明人：路易士 堤摩太 LEWIS, TIMOTHY ANDREW (US)

(74)代理人：林志剛

(56)參考文獻：

TW	200833059A	TW	201017514A
US	2014/0068594A1	US	2014/0156994A1

審查人員：馮耀嘉

申請專利範圍項數：29 項 圖式數：8 共 44 頁

(54)名稱

使用憑證導出之加密密鑰改良韌體服務安全性的計算裝置之系統及方法

(57)摘要

論述一種基於韌體之技術，其用於使用自一個或多個使用者憑證產生之一個或多個對稱密鑰來解密使用者設定檔資訊，且在允許存取韌體提供之服務之前鑑認使用者。

A firmware-based technique for using one or more symmetric keys generated from one or more user credentials to decrypt user profile information and authenticate the user before allowing access to firmware-provided services is discussed.

指定代表圖：

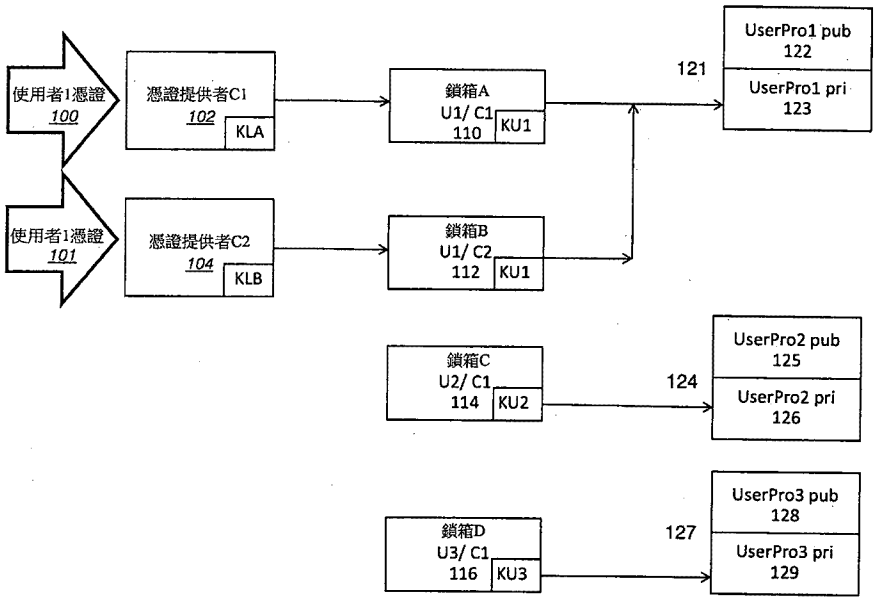

圖1

符號簡單說明：

100・・・第一使用者1憑證

101・・・第二類型之使用者1憑證

102・・・憑證提供者C1

104・・・憑證提供者C2

110・・・鎖箱A

112・・・鎖箱B

114・・・鎖箱C

116・・・鎖箱D

121・・・使用者設定檔容器/使用者設定檔1

122・・・未加密部分

123・・・加密部分/私用部分

124・・・使用者設定檔容器/使用者設定檔2

125・・・未加密部分

126・・・加密部分/私用部分

127・・・使用者設定檔容器/使用者設定檔3

128・・・未加密部分

129・・・加密部分/私用部分

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】(中文/英文)

使用憑證導出之加密密鑰改良韌體服務安全性的計算裝置之系統及方法

System and method for computing device with improved firmware service security using credential-derived encryption key

【技術領域】

[0001] 本發明關於韌體服務安全性。本申請案主張2015年2月13日申請之標題為「Firmware Secret Storage Using Credential Derived Encryption Key」之美國臨時專利申請案第62/115,891號的權益及優先權，所述美國臨時專利申請案的內容以全文引用之方式併入本文中。

【先前技術】

[0002] 由包括於計算裝置內的韌體初始化所述裝置，且此韌體提供促進作業系統（OS）的啟動的一系列軟體服務以及提供在已啟動作業系統之後繼續可用的此等服務的較小子集。韌體為已寫入至唯讀記憶體（ROM）模組（包括（但不限於）ROM、PROM、EPROM、EEPROM以及快閃記憶體 ROM（下文統稱為「ROM」））上的軟體。在其他服務中，韌體負責操作計算裝置直至可執行將計算裝置的作業系統載入至記憶體中的啟動程序為止。一

且載入，作業系統負責計算裝置的標準操作，但出於安全性以及其他原因，在載入作業系統之後佈建某些服務可要求自作業系統返回至韌體之控制轉變。

[0003] 統一可擴展韌體介面（UEFI）為由非營利行業主體所產生的詳述作業系統與計算裝置（諸如（但不限於）個人電腦（PC））的所包括韌體之間的程式設計介面的規範。UEFI 規範描述計算裝置可藉由其以經組織方式自功率應用狀態移動至可完全操作狀態的工具集合。UEFI 規範告知所要結果但有意地並不指定實施的內部策略。UEFI 韌體規範替換行業所先前使用且通常被稱為舊式 BIOS 的早期 OS/韌體介面。

[0004] 在實施於計算裝置中時，UEFI 韌體之機器碼及韌體所使用的所有永久性資料駐留於 ROM 中。在許多狀況下，ROM 為稱為快閃記憶體 ROM 的電可抹除矽裝置。快閃記憶體 ROM 具有可由電命令抹除且可接著寫入個別元素，且裝置將無期限地保留資料的特性。當首次將功率應用於計算裝置時，系統執行將狀態清除至已知狀況並開始執行韌體的稱為重置的程序。自計算裝置中之快閃記憶體 ROM 或其他 ROM 讀取韌體。

【發明內容】

[0005] 本發明之實施例提供用於使用自使用者憑證導出之密鑰來解密使用者設定檔資訊且在允許存取韌體提供之服務之前鑑認使用者的技術。所述技術避免了韌體必

須儲存存取計算裝置上的韌體提供之服務所需要的密碼。實施例進一步使得能夠在多因子使用者識別框架中使用憑證導出之對稱密鑰，所述多因子使用者識別框架在授權韌體提供之服務之前處理兩個或兩個以上使用者憑證。

[0006] 在一個實施例中，一種方法增強計算裝置中的韌體提供之服務之安全性。計算裝置經組態有韌體，所述韌體在執行時使計算裝置利用使用者憑證驅動程式接收使用者憑證，及利用使用者憑證驅動程式自使用者憑證產生第一對稱密鑰。所述方法亦解密具有第一對稱密鑰之第一資料容器的至少一部分。第一資料容器之解密部分保存第二對稱使用者設定檔密鑰，所述第二對稱使用者設定檔密鑰先前用以加密保存使用者設定檔之第二資料容器的私用部分。第一及第二資料容器儲存於非揮發性儲存器中。所述方法進一步使用第二對稱使用者設定檔密鑰解密第二資料容器之私用部分。基於第二資料容器之私用部分之成功解密的判定來鑑認使用者，且在鑑認之後提供對韌體服務之存取。

[0007] 在另一實施例中，一種方法增強計算裝置中之韌體提供之服務的安全性。計算裝置經組態有韌體，所述韌體在執行時使計算裝置利用使用者憑證驅動程式接收使用者憑證，及利用使用者憑證驅動程式自使用者憑證產生第一對稱密鑰。韌體亦解密具有第一對稱密鑰之第一資料容器的至少一部分。所述方法利用第二使用者憑證驅動程式接收第二使用者憑證，及利用第二使用者憑證驅動程

式自第二使用者憑證產生第二對稱密鑰。韌體解密具有第二對稱密鑰之第二資料容器的至少一部分。第二資料容器之解密部分保存第三對稱使用者設定檔密鑰，所述第三對稱使用者設定檔密鑰先前用以加密保存使用者設定檔之第三資料容器的私用部分。第一、第二及第三資料容器儲存於非揮發性儲存器中。所述方法進一步使用對稱使用者設定檔密鑰解密第三資料容器之私用部分，及基於第三資料容器之私用部分之成功解密的判定來鑑認使用者。在鑑認之後向使用者提供對韌體服務之存取。

[0008] 在實施例中，一種計算裝置提供韌體提供之服務的增強的安全性，且包含處理器、輸入裝置及韌體。在執行時，韌體中之鑑認模組使計算裝置利用使用者憑證驅動程式接收使用者憑證，及利用使用者憑證驅動程式自使用者憑證產生第一對稱密鑰。韌體亦解密具有第一對稱密鑰之第一資料容器的至少一部分。第一資料容器之解密部分保存第二對稱使用者設定檔密鑰，所述第二對稱使用者設定檔密鑰先前用以加密保存使用者設定檔之第二資料容器的私用部分。第一及第二資料容器儲存於非揮發性儲存器中。韌體進一步使用對稱使用者設定檔密鑰解密第二資料容器之私用部分。基於第二資料容器之私用部分之成功解密的判定來鑑認使用者，且在鑑認之後提供對韌體服務之存取。

[0009] 在一個實施例中，一種計算裝置提供韌體提供之服務的增強的安全性，且包含處理器、輸入裝置及韌

體。在執行時，韌體中之鑑認模組使計算裝置利用使用者憑證驅動程式接收使用者憑證，及利用使用者憑證驅動程式自使用者憑證產生第一對稱密鑰。韌體亦解密具有第一對稱密鑰之第一資料容器的至少一部分。韌體另外使計算裝置利用第二使用者憑證驅動程式接收第二使用者憑證，及利用第二使用者憑證驅動程式自第二使用者憑證產生第二對稱密鑰。韌體之執行解密具有第二對稱密鑰之第二資料容器的至少一部分。第二資料容器之解密部分保存第三對稱使用者設定檔密鑰，所述第三對稱使用者設定檔密鑰先前用以加密保存使用者設定檔之第三資料容器的私用部分。第一、第二及第三資料容器儲存於非揮發性儲存器中。韌體之執行進一步使用對稱使用者設定檔密鑰解密第三資料容器之私用部分，且基於第三資料容器之私用部分之成功解密的判定來鑑認使用者。在鑑認之後，向使用者提供對韌體服務之存取。

【圖式簡單說明】

[0010] 併入本說明書中且構成本說明書的部分的隨附圖式說明本發明的一個或多個實施例，並與描述一起幫助解釋本發明。在圖式中：

圖 1 為描繪在本發明的實施例中之憑證提供者、鎖箱及使用者設定檔的相互關係之方塊圖；

圖 2 描繪在本發明的實施例中由鑑認模組執行以在提供對韌體服務之存取之前鑑認使用者的步驟之例示性序

列；

圖 3 為描繪在本發明的實施例中使用兩個憑證提供者來存取鎖箱及相關聯的使用者設定檔之方塊圖；

圖 4 描繪在本發明的實施例中由鑑認模組執行之步驟的例示性序列，所述步驟需要在提供對韌體服務之存取之前使用兩個憑證來鑑認使用者；

圖 5 描繪由本發明的實施例執行以存取韌體服務而不用管丟失的使用者密碼之步驟之例示性序列；

圖 6 描繪由本發明的實施例執行以對改變的密碼作出回應之步驟之例示性序列；

圖 7 描繪由本發明的實施例執行以登記新的使用者設定檔之步驟之例示性序列；

圖 8 描繪適合本發明的實施例使用之例示性計算裝置。

【實施方式】

[0011] 韌體常常為特定使用者（諸如主管人、IT 管理員或生產線工作者）保留特定功能或特權。在典型狀況下，此等使用者藉由輸入存取韌體提供之服務所需要的密碼向韌體鑑認自身。在驗證密碼匹配使用者之後，韌體解鎖特定功能，諸如存取組態選單或自特定裝置啟動或停用安全性保障措施的能力。在此環境中，密碼為保密的。然而，在根本上，韌體並不太適合保存秘密。現代密碼編譯系統將焦點對準密鑰的安全性，而不是演算法的安全性。

若知曉密鑰及演算法，則會暴露秘密。不對稱密碼編譯系統藉由使加密所需要的密鑰與解密所需要的密鑰分離，略微改良所述情形，以使得解密所需要的密鑰可儲存於韌體中。然而，此做法需要防韌體被不當使用。

[0012] 令人遺憾的是，韌體並非保護密碼（或其他儲存憑證）的理想載具。不論是以純文字的形式儲存還是以某種方式雜湊，可以持續及實體地存取快閃記憶體裝置（其中儲存有韌體）的人可發現演算法及保密密碼兩者。此發現可以數種方式完成，包含經由藉由可轉儲記憶體映射之快閃記憶體內容的程式來分析系統內的韌體內容，或藉由直接自快閃記憶體裝置擷取所要資訊，且在另一系統上對其進行分析。亦至少存在第三做法，其涉及在處理密碼時分析系統中的組件之間的信號，但為免遭所述類別之分析而進行的保護措施超出了本發明之範疇。

[0013] 為了試圖解決此等安全性問題，一些現有密碼安全性解決方案將密碼以雜湊形成儲存於快閃記憶體裝置之受保護部分中。更先進的安全性技術將密碼儲存於諸如鍵盤控制器、底板管理控制器（BMC）或受信任平台模組（TPM）之次級控制器上。然而，此等額外裝置給設計添加了成本及複雜度。此外，雖然 TPM 提供安全儲存至韌體之解決方案，但使用者設定檔無法在運行時間進行更新，因為 TPM 在交遞至作業系統（OS）之前將平台密鑰鎖起來。

[0014] 本發明之實施例提供在實際上不將憑證之複

本儲存於韌體快閃記憶體裝置中的情況下驗證諸如密碼之使用者憑證的技術。在一個實施例中，此憑證可用以將與所述使用者相關聯的額外秘密安全地儲存於韌體裝置中。在另一實施例中，可需要多個憑證以存取相同的使用者資訊。實施例可整合至系統中，所述系統支援其他憑證類型（智慧卡資料、指紋感測器資料、視網膜掃描資料等）。可在由 OS 返回對計算裝置之控制至韌體後，在資源受限制之預作業系統（OS）環境中驗證所述憑證，及/或所述憑證可提供由韌體執行之恢復情境，諸如在密碼丟失的狀況下。所有此等技術會使韌體安全性受益，因為密碼或其他憑證決不會儲存於韌體中。結果，憑證無法被擷取，或與雜湊資料庫相違，從而只能猜測所述憑證，且給予對使用者資訊或使用者特權的未經授權之存取。另外，因為實施例提供用於加密使用者資料之安全技術，所以安全性進一步得到改良。

[0015] 更詳細地，本發明之實施例利用先前與韌體共用之使用者對憑證的知識來加密使用者資料。此憑證可為（但不限於）密碼、自指紋掃描獲取之資料或自視網膜掃描獲取之資料。實施例自輸入憑證導出對稱密鑰，且試圖利用密鑰來解密使用者之資料（或其雜湊），而非向使用者詢問憑證且接著比較所述憑證與憑證之先前儲存版本。對稱密鑰可用以加密及解密資料兩者。成功解密指示憑證匹配先前用以加密資料之憑證，且鑑認使用者。失敗解密指示憑證不匹配，且因此未鑑認使用者。因為解密使

用自憑證導出之對稱密鑰，而非執行與儲存憑證之比較，所以憑證自身不儲存於韌體中。此情形防止應用程式的窺探或經授權實體對快閃記憶體裝置之實體直接讀取來擷取憑證。

[0016] 圖 1 為描繪在本發明的實施例中之憑證提供者、鎖箱及使用者設定檔的相互關係之方塊圖。憑證提供者 C1（102）及 C2（104）為用於處置特定類型之使用者憑證的使用者憑證驅動程式。鎖箱 A 至 D（110、112、114、116）及使用者設定檔（121、124、127）為與特定使用者相關聯的資料容器，執行韌體可存取所述資料容器。此等資料容器儲存於非揮發性儲存器中，所述非揮發性儲存器可包含 ROM、硬碟機等。本發明之資料容器包含公用（未加密）及私用（加密）部分。鎖箱保存對稱加密密鑰，且亦與特定類型之使用者憑證（例如：C1、C2）相關聯。舉例而言，憑證提供者 C1（102）可經由連接至計算裝置之鍵盤接受第一使用者 1 憑證（100），諸如密碼。同時，憑證提供者 C2（104）可經由指紋掃描器接受第二類型之使用者 1 憑證 101，諸如指紋。如下文將進一步解釋，憑證提供者 C1（102）及 C2（104）分別基於所輸入之各別使用者憑證 100、101 產生對稱密鑰（KLA、KLB）。憑證提供者儲存於防篡改非揮發性儲存器中，其中以安全方式（諸如由 UEFI 的包套更新機制提供之方式）控制對提供者的更新。

[0017] 如上文所指出，每一鎖箱 110、112、114、

116 具有加密部分及未加密部分。鎖箱之加密部分保存對稱使用者設定檔密鑰：圖 1 中之 KU1/KU2/KU3，所述對稱使用者設定檔密鑰先前用以加密其相關聯的使用者設定檔 121、124、127 之私用部分 123、126、129。下文在圖 7 之論述期間進一步論述最初建立及加密使用者設定檔 121、124、127 的一部分之程序。隨後，每一鎖箱之加密私用部分自身先前由憑證提供者製造之密鑰加密。舉例而言，在圖 1 中，鎖箱 A（110）包含對稱密鑰 KU1，其先前用以加密使用者設定檔容器 121 之私用部分 123。因為密鑰為對稱的，所以其亦可用以解密其先前加密的東西。密鑰 KU1 保存於由對稱密鑰 KLA 加密之鎖箱 A（110）的加密部分中，由憑證提供者 C1（102）自輸入使用者密碼產生所述對稱密鑰 KLA。

[0018] 每一使用者設定檔容器 121、124、127 含有未加密部分（UserProXpub）（122、125、128）及加密部分（UserProXpri）（123、126、129）。應注意在圖 1 中，鎖箱 A（110）及鎖箱 B（112）參考相同的使用者設定檔 121，指示在此狀況下，替代憑證可用以擷取解密使用者設定檔 121 之私用部分所需要的使用者設定檔密鑰。兩個鎖箱皆含有先前用以加密使用者設定檔 1（121）之私用部分 123 的密鑰之複本。在此狀況下，使用者可經由自使用者密碼（使用者 1 憑證（100））產生之密鑰（KLA）解鎖鎖箱 A（110）以擷取解鎖使用者設定檔 1（121）所需要的密鑰（KU1），所述使用者密碼被提供

至憑證提供者 C1（102）。替代性地，使用者可經由自指紋（使用者 1 憑證（101））產生之密鑰（KLB）解鎖鎖箱 B（112）以擷取解鎖使用者設定檔 1（121）所需要的相同密鑰（KU1），所述指紋被提供至憑證提供者 C2（104）。儘管圖 1 中未特別說明，但在存取使用者設定檔 2（124）之私用部分 126 之前解鎖鎖箱 C（114）的私用部分所需要的密鑰將自由第二使用者（U2）提供至憑證提供者 C1（102）的密碼產生。類似地，在存取使用者設定檔 3（127）之私用部分 129 之前解鎖鎖箱 D（116）的私用部分所需要的密鑰將自由第三使用者（U3）提供至憑證提供者 C1（102）的密碼產生。

[0019] 鎖箱公用（未加密）資料可含有與恆定的甚至跨平台重置的單一使用者設定檔相關聯之一個使用者識別符。鎖箱公用資料亦包含一個或多個使用者憑證提供者識別符。每一識別符唯一地識別使用者憑證提供者。鎖箱私用（加密）資料可含有鹽值（salt value），以及另一鎖箱容器（在下文進一步論述的多因子鑑認的狀況下）抑或使用者設定檔對稱密鑰及指定密鑰之類型的識別符。

[0020] 如上文所提及，使用者設定檔資料容器可含有兩個部分：公用（未加密）及私用（加密）。公用部分包含可用以將鎖箱與使用者設定檔相關聯的唯一識別符。作為一個實例，唯一識別符可為 UEFI 規範中所描述之使用者識別符。使用者設定檔之公用部分亦可包含諸如使用者名稱、使用者特權及使用者識別策略之項目。使用者設

定檔之私用部分可包含可用以驗證所述解密已成功之已知鹽值。對於大部分密碼編譯演算法，鹽值應與加密區塊大小一樣大。使用者設定檔之私用部分亦可包含其他密鑰，諸如在啟動之前使用且因此決不會暴露於其他代理程式的用於硬碟加密之密鑰，及/或用於 OS 登入之使用者名稱/密碼，可使用單獨公用/私用密鑰對以加密形式儲存所述使用者名稱/密碼。

[0021] 舉例而言，在一個實施例中，本文中所描述的技術可用以改變儲存於使用者設定檔之私用部分中的使用者登入密碼。使用者可藉由鍵入其存取韌體服務所需要的 BIOS 密碼而開始。存取韌體服務所需要的此密碼不由系統儲存，但可用以（如本文所描述）產生對稱密鑰，以將保存另一密鑰之資料容器解鎖至保存具有當前 OS 登入密碼之使用者設定檔的單獨資料容器。一旦已存取使用者設定檔，便可使用已知技術產生公用/私用密鑰對，新 OS 密碼使用私用密鑰加密，且加密密碼儲存於使用者設定檔之私用部分中。韌體將捨棄用以加密新 OS 登入密碼之私用密鑰，且 OS 登入驅動程式將儲存公用密鑰。在後續啟動期間，OS 驅動程式將試圖解密含有 OS 登入密碼之使用者設定檔的私用部分，以便使用公用密鑰進行鑑認。

[0022] 存在若干種熟知的自密碼產生密鑰之方法，諸如 PKCS#5（http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-5-password-based cryptography-standard.htm，亦被稱作 PBKDF1/2，在 RFC2898）中描述或 scrypt http：

//en.wikipedia.org/wiki/Scrypt）或 RFC5869。亦參見 http://www.di-mgt.com.au/cryptoKDFs.html。另外，如上文所論述，其他類型之使用者憑證可由使用者憑證驅動程式處理以便產生對稱密鑰。主要要求為使用者憑證驅動程式能夠基於使用者身分標識製造密碼編譯安全對稱密鑰。每一鎖箱與使用者設定檔及一個或多個使用者憑證類型相關聯。舉例而言，若可以一次又一次地可靠複製指紋，則指紋資料之雜湊可使用用於密碼之相同類別的演算法擴展至對稱密鑰中。類似技術可被用於經由視網膜掃描獲取之資料。替代性地，指紋或 PIN 數目可解鎖保存先前登記的對稱密鑰之儲存器。此外，對稱密鑰可儲存於由在登記期間產生之私用密鑰加密的 USB 密鑰上，而在韌體中維持公用密鑰以使得在插入 USB 密鑰時，韌體可自 USB 密鑰解密 KB（使用憑證之類似做法亦為可能的）。另外，特定 USB 大容量儲存裝置之 WWID 可擴展至對稱密鑰中，以使得將信任儲存於 USB 密鑰上之所有密鑰。

[0023] 本發明之實施例使用憑證導出之密鑰使得能夠在無依靠於所儲存憑證之韌體的情況下，在提供韌體服務之前進行使用者鑑認。圖 2 描繪在本發明的實施例中由鑑認模組執行以在提供對韌體服務之存取之前鑑認使用者的步驟之例示性序列。序列以識別使用者之韌體鑑認模組操作計算裝置及啟動使用者之設定檔（步驟 200）開始。在 UEFI 規範中啟動使用者之設定檔涉及將特定使用者設定檔選擇為當前使用者設定檔。當前使用者設定檔詳述了

特定服務將操作之特權級別。例如，哪些裝置可用於啟動等。經由憑證提供者接收特定使用者的諸如密碼之憑證（步驟 202），所述憑證提供者接著自所接收憑證產生第 1 對稱密鑰（步驟 204）。經由使用者識別符或以其他方式識別使用者之相關聯的鎖箱，且所產生對稱密鑰用以試圖解密保存使用者設定檔密鑰之鎖箱的私用部分（步驟 206）。應瞭解，先前在使用者登記期間由相同的對稱密鑰加密相關聯的鎖箱之私用部分。在一個實施例中，由韌體接收使用者名稱及憑證兩者，且識別使用者之相關聯的鎖箱所需要之使用者識別符可藉由搜尋使用者設定檔之公用部分而發現。在另一實施例中，僅接收憑證，且搜尋與使用者憑證提供者之類型相關聯的所有鎖箱，直至發現可解密之鎖箱為止（因為不知曉使用者識別符）。在一個實施例中，成功解密可由鎖箱之經解密私用部分中含有的正確/已知鹽值指示，且可由經解密鎖箱私用資料中之不正確鹽值指示失敗解密。若所嘗試的解密不成功（步驟 207），則系統策略可引起使用者重試，或指示鑑認故障之簡單序列退出。若所嘗試的解密成功（步驟 207），則自鎖箱之私用部分擷取使用者設定檔密鑰，且使用所述使用者設定檔密鑰以試圖解密使用者設定檔資料容器之私用部分（步驟 208）。應瞭解，先前在使用者登記期間由相同的對稱使用者設定檔密鑰加密相關聯的使用者設定檔之私用部分。若所嘗試的解密不成功（步驟 209），則鑑認程序失敗。若使用者設定檔資料容器之私用部分的所嘗試

的解密成功，則使用者被視為經鑑認的（步驟 210），且鑑認模組提供對允許使用者存取之所要韌體服務之存取（步驟 212）。類似於鎖箱之解密，在一個實施例中，由經解密使用者設定檔私用資料中之正確/已知鹽值指示成功解密。由經解密使用者設定檔私用資料中之不正確鹽值指示失敗解密。失敗狀況可以與未能解密鎖箱相同的方式進行處理。在一些實施例中，出於安全性原因，在序列結束之前，用以分別解密鎖箱及使用者設定檔之私用部分的密鑰及所接收憑證之任何暫時複本由韌體捨棄。

[0024] 本發明之實施例亦支援多因子鑑認，其中可需要為不同類型之使用者憑證的兩個憑證在向使用者提供韌體服務之前皆為需要的。更特定言之，鎖箱私用資料可含有對稱密鑰或另一鎖箱私用資料結構。此組態可用以支援多因子鑑認，其中需要兩個或兩個以上裝置來識別使用者。舉例而言，可需要指紋及密碼來識別使用者。在此狀況下，鎖箱公用資料可含有使用者設定檔識別符及兩個或兩個以上使用者憑證識別符。鎖箱私用資料可由第一使用者憑證提供者產生之密鑰加密，且接著所述資料由第二使用者憑證提供者產生之密鑰加密。應注意，其做法僅支援及使用者識別策略（亦即指紋及密碼），但不支援或（指紋或密碼）。使用者識別策略可指定哪些使用者憑證應被用於特定使用者設定檔。使用者識別策略可位於使用者設定檔之公用部分中。在一個實施例中，策略可包含布林表達式，其中葉項為由諸如及與或之布林運算子接合在一起

之使用者憑證識別符（用於特定使用者憑證提供者，如特定供應商的指紋感測器，或用於若干種類之使用者憑證提供者，如指紋感測器）。上文中，使用多因子擴展，鎖箱可直接支援及運算子，且多個鎖箱可支援或運算。無法直接支援非運算子。簡單憑證提供者之一個實例讀取主機板上之開關或跨接線之當前設置。若開關或跨接線「接通」，則使用者憑證提供者報告邏輯真。因此，若策略為密碼及（跨接線或指紋），則此可被分解成具有密碼及跨接線以及密碼及指紋之兩個鎖箱。兩個鎖箱皆與相同的使用者設定檔相關聯。替代性地，可擴展鎖箱私用資料結構以支援在巢套之每一層級處支援多個「或」交替。

[0025] 圖 3 為描繪在本發明的實施例中使用兩個憑證提供者來存取鎖箱及相關聯的使用者設定檔之方塊圖。如圖 1 之論述中簡要地提到，私用部分可含有亦將需要解密之額外巢套鎖箱，而非鎖箱的私用部分含有資料。舉例而言，在圖 3 中，諸如密碼之第一使用者 1 憑證 300 可由韌體憑證提供者 C1（302）接收，且用以產生第一對稱密鑰（KLE）。第一對稱密鑰可用以解密與使用者設定檔 320 相關聯的鎖箱 E 310 之私用部分。然而，解密鎖箱 E 之私用部分可暴露鎖箱 F 312。對鎖箱 F 之私用部分的存取需要由憑證提供者 C2（304）自第二/第二類型之使用者 1 憑證 301 產生的密鑰 KLF。舉例而言，可自輸入指紋產生密鑰 KLF。鎖箱 F 312 之私用部分可含有用以解密使用者設定檔 320 之私用部分 322 的密鑰 KU1。應瞭解，儘

管兩個巢套鎖箱在圖 3 中經描繪為巢套，但可在不脫離本發明之範疇的情況下巢套總計兩個以上額外鎖箱。

[0026] 圖 4 中描繪例示性多因子鑑認程序。更特定言之，圖 4 描繪在本發明的實施例中由鑑認模組執行之步驟的例示性序列，所述步驟需要在提供對韌體服務之存取之前使用兩個憑證來鑑認使用者。在由計算裝置接收需要存取韌體服務之指示之後，序列以韌體經由第一憑證提供者接收使用者之第一憑證（步驟 402）開始。第一憑證提供者自第一憑證產生第 1 對稱密鑰（步驟 404）。所產生之第 1 對稱密鑰用以試圖解密含有第二資料容器之第一資料容器的私用部分（步驟 406）。若解密嘗試成功，則韌體接收第二憑證（步驟 408）。應瞭解，第二憑證（不限於此）可為來自相同使用者之第二憑證（諸如不同密碼）、相同使用者之第二類型之憑證（諸如指紋或視網膜掃描），或甚至在兩個個體需要進行授權之情形中來自不同使用者的第二憑證。第二憑證提供者自第二憑證之資料產生第 2 對稱密鑰（步驟 410），且所產生之第 2 對稱密鑰用以嘗試解密保存使用者設定檔密鑰之第 2 資料容器的私用部分（步驟 412）。若解密嘗試成功（步驟 413），則所擷取之使用者設定檔密鑰用以試圖解密相關聯的使用者設定檔資料容器之私用部分（步驟 414）。若使用者設定檔之私用部分的解密嘗試成功（步驟 415），則使用者由韌體鑑認，且被提供對使用者經授權之韌體服務之存取（步驟 416）。

[0027] 圖 5 描繪由本發明的實施例執行以使得能夠存取韌體服務而不用管丟失的使用者密碼之步驟之例示性序列。序列以韌體接收丟失的使用者密碼之指示（步驟 502）開始。舉例而言，在使用者忘記其密碼時，可選擇「忘記密碼？」連結或按鈕，所述連結或按鈕觸發恢復序列。恢復密碼的常見手段之一為詢問一個或多個安全性問題。若使用者能夠鍵入對安全性問題的正確回答，則使用者能夠獲得他/她的使用者設定檔，且重置他/她的密碼。在一個實施例中，在使用者的使用者設定檔之公用部分中編碼此等安全性問題。韌體自使用者設定檔之公用部分擷取安全性問題，且將其傳達給使用者（步驟 504）。呈現的問題數目為可組態策略。接著接收對一個或多個問題的回答（步驟 506）。將對一個或多個問題的一個或多個回答擴展至密碼中（步驟 508），且自所述密碼產生對稱密鑰（步驟 510）。韌體試圖解密保存使用者設定檔密鑰之相關聯鎖箱的私用部分，所述使用者設定檔密鑰可用以存取使用者設定檔容器之私用部分（步驟 512）。若解密成功（步驟 513），則所擷取使用者設定檔密鑰用以試圖解密相關聯使用者設定檔之私用部分（步驟 514。若嘗試成功（步驟 515），則允許使用者存取他或她的經授權韌體服務（步驟 516）。

[0028] 利用憑證導出之對稱密鑰之上文所描述的技術亦可用以改變密碼。圖 6 描繪由本發明的實施例執行以改變密碼之步驟的例示性序列。所述序列假設存在當前作

用中使用者設定檔，且此使用者設定檔具有改變其自身密碼的特權。一些使用者設定檔（諸如「客體」設定檔）不具有此等特權。接收當前使用者的輸入項及相關聯的密碼（步驟 602）。亦接收使用者鍵入的新密碼（步驟 604），且識別與使用者及密碼憑證提供者相關聯的鎖箱（步驟 606）。對稱密鑰自當前密碼產生（步驟 608），且用以試圖解密鎖箱之私用部分（保存使用者設定檔密鑰）（步驟 610）。若嘗試成功（步驟 611），則接著利用自新密碼產生之對稱密鑰重新加密鎖箱之私用部分（步驟 612）。若成功，則密碼已改變，因為僅新密碼將在將來產生解密重新加密之鎖箱所需要的對稱密鑰。在所述序列結束之前，自新及舊密碼產生之兩個密鑰接著皆被捨棄（步驟 614），如輸入密碼資料一樣。

[0029] 為了使本文中已描述的技術起作用，與使用者相關聯的使用者設定檔容器及鎖箱容器首先被建立，且使用相同對稱密鑰加密，所述對稱密鑰稍後將用以對所述容器進行解密。圖 7 描繪由本發明的實施例執行以最初創建新使用者設定檔之步驟的例示性序列。序列以識別使用者（步驟 702）及檢查當前使用者設定檔（若存在在作用中之使用者設定檔）是否允許新使用者登記（步驟 703）。新使用者登記常常為指派給特定使用者或特定類別之使用者的特權。若當前使用者設定檔不允許新使用者登記，則退出所述程序。假設允許新使用者登記（步驟 703），則接收特定使用者之密碼（步驟 704）。此步驟

包含收集填充使用者設定檔所需要的任何其他初始資訊（諸如使用者名稱），且可包含複製含有所要預設特權及使用者識別策略之範本使用者設定檔，且接著接收新使用者之密碼。在此階段亦加強了密碼複雜度。例如，密碼含有大寫及小寫以及數字及標點符號或不重複先前密碼之要求。接著利用使用者名稱及含有基本使用者特權資訊之範本創建基本使用者設定檔（公用及私用）。範本可與當前使用者有關，可由當前使用者選擇或可為通用預設。接著使用隨機產生之對稱使用者設定檔密鑰來加密使用者設定檔之私用部分（步驟 706）隨機產生對稱密鑰之手段係熟知的。將鎖箱劃分成公用（未加密）部分及私用（加密）部分。公用部分含有使用者憑證識別符（將其與使用者憑證驅動程式相關聯）及使用者識別符（將其與在步驟 706 中創建之使用者設定檔相關聯）。將用以加密使用者設定檔之私用部分的使用者設定檔密鑰儲存於鎖箱之私用部分中（步驟 708）。在一個實施例中，使用者設定檔密鑰連同用以驗證解密之鹽值一起被儲存。使用者憑證提供者自所接收密碼產生對稱密鑰（步驟 710），且試圖加密新鎖箱之私用部分（步驟 712）。若加密成功（步驟 713），則建立使用者設定檔，且由韌體捨棄使用者設定檔密鑰之複本及自密碼產生之對稱密鑰。以此方式，後續鑑認程序不需要將所儲存密碼與輸入密碼匹配，因此限制安全性風險。應瞭解，此相同程序亦適用於其他類型之非密碼憑證。

[0030] 圖 8 描繪適合本發明的實施例使用之例示性計算裝置 800。計算裝置 800 可為伺服器、桌上型計算裝置、平板計算裝置、膝上型電腦、智慧型電話或裝備有處理器之某一類型之其他電子裝置。計算裝置 800 包含一個或多個處理器，諸如 CPU 804 及記憶體 806。記憶體 806 可為隨機存取記憶體（RAM）。計算裝置 800 可包含保存作業系統 808 之硬碟驅動機（HDD）807，在計算裝置之啟動程序期間由韌體 810 將所述作業系統裝載至記憶體 806 中。計算裝置 800 亦包含唯讀記憶體（ROM）810。ROM 810 可為（但不限於）ROM、PROM、EPROM、EEPROM 及快閃記憶體 ROM。ROM 810 儲存包含鑑認模組 830 之韌體 820，所述鑑認模組用以使用憑證導出之密鑰執行使用者鑑認及如上文所描述之其他功能性。鑑認模組 830 可與如上文所描述之憑證提供者 831a...n、鎖箱 832a...n 及使用者設定檔 833a...n 互動，以在允許存取韌體服務之前鑑認使用者。使用者 802 可經由輸入裝置 A 及 B（801A、801B）與計算裝置 800 互動。舉例而言，輸入裝置 A（801A）可為使用者 802 可鍵入密碼之鍵盤，所述密碼被用作憑證提供者之輸入以產生對稱密鑰。類似地，輸入裝置 B（801B）可為指紋或視網膜掃描儀，使用者 802 可藉由所述指紋或視網膜掃描儀鍵入憑證，所述憑證被用作憑證提供者之輸入以產生對稱密鑰。計算裝置 800 可包含適合在網路上通信之顯示器 840 及通信介面 850。

[0031] 可將本發明實施例中的部分或所有提供為體

現於一個或多個非暫時性媒體上或媒體中的一個或多個電腦可讀程式或程式碼。媒體可為（但不限於）硬碟、光碟、數位影音光碟、ROM、PROM、EPROM、EEPROM、快閃記憶體、RAM 或磁帶。大體而言，可以任何計算語言實施電腦可讀程式或程式碼。

[0032] 由於可在不脫離本發明的範疇的情況下作出某些改變，因此希望將上文描述中所含有或隨附圖式中所展示的所有物質解釋為說明性而非字面意義。習此相關技藝之人士將認識到可在不脫離本發明的範疇的情況下，變更圖式中所描繪的步驟序列以及架構，且本文中所含有的說明為本發明的眾多可能描繪的單數實例。

[0033] 本發明的實例實施例之前述描述提供說明以及描述，但並不意欲為窮盡性的或將本發明限為所揭示之精確形式。有可能根據上文教示進行修改以及變化或可自本發明的實踐獲得修改以及變化。舉例而言，雖然已描述一系列動作，但可在與本發明原理一致的其他實施中修改動作的次序。另外，可並行地執行非相依性動作。

【符號說明】

[0034]

100：第一使用者 1 憑證

101：第二類型之使用者 1 憑證

102：憑證提供者 C1

104：憑證提供者 C2

110：鎖箱 A

112：鎖箱 B

114：鎖箱 C

116：鎖箱 D

121：使用者設定檔容器/使用者設定檔 1

122：未加密部分

123：加密部分/私用部分

124：使用者設定檔容器/使用者設定檔 2

125：未加密部分

126：加密部分/私用部分

127：使用者設定檔容器/使用者設定檔 3

128：未加密部分

129：加密部分/私用部分

300：第一使用者 1 憑證

301：第二/第二類型之使用者 1 憑證

302：韌體憑證提供者 C1

304：憑證提供者 C2

310：鎖箱 E

312：鎖箱 F

320：使用者設定檔

322：私用部分

800：計算裝置

801A：輸入裝置 A

801B：輸入裝置 B

802：使用者

804：CPU

806：記憶體

807：硬碟驅動機（HDD）

808：作業系統

810：韌體

820：韌體

830：鑑認模組

831a...n：憑證提供者

832a...n：鎖箱

833a...n：使用者設定檔

840：顯示器

850：通信介面

公告本

I684890

發明摘要

※申請案號：105104313

※申請日：105 年 02 月 15 日　　※IPC 分類：

【發明名稱】(中文/英文)

使用憑證導出之加密密鑰改良韌體服務安全性的計算裝置之系統及方法

System and method for computing device with improved firmware service security using credential-derived encryption key

【中文】

論述一種基於韌體之技術，其用於使用自一個或多個使用者憑證產生之一個或多個對稱密鑰來解密使用者設定檔資訊，且在允許存取韌體提供之服務之前鑑認使用者。

【英文】

A firmware-based technique for using one or more symmetric keys generated from one or more user credentials to decrypt user profile information and authenticate the user before allowing access to firmware-provided services is discussed.

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：

100：第一使用者 1 憑證

101：第二類型之使用者 1 憑證

102：憑證提供者 C1

104：憑證提供者 C2

110：鎖箱 A

112：鎖箱 B

114：鎖箱 C

116：鎖箱 D

121：使用者設定檔容器/使用者設定檔 1

122：未加密部分

123：加密部分/私用部分

124：使用者設定檔容器/使用者設定檔 2

125：未加密部分

126：加密部分/私用部分

127：使用者設定檔容器/使用者設定檔 3

128：未加密部分

129：加密部分/私用部分

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

申請專利範圍

1. 一種用於增強一計算裝置中之韌體提供之服務的安全性之方法，所述計算裝置經組態有韌體，所述韌體在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述解密部分保存一第二對稱使用者設定檔密鑰，所述第二對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第二資料容器的一私用部分，所述第一及第二資料容器儲存於非揮發性儲存器中；

使用所述第二對稱使用者設定檔密鑰解密所述第二資料容器之所述私用部分；

基於所述第二資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

2. 如申請專利範圍第 1 項所述的方法，其中所述使用者憑證先前暫時與所述計算裝置中之韌體共用，以創建等同於所述第一對稱密鑰之一對稱密鑰，等同於所述第一對稱密鑰之所述對稱密鑰用以加密所述第一資料容器，且接著由所述韌體捨棄。

3. 如申請專利範圍第 1 項所述的方法，其中所述韌體之所述執行使所述計算裝置：

基於所述第二資料容器之所述私用部分中含有的一已知鹽值來判定所述成功解密。

4. 如申請專利範圍第 1 項所述的方法，其中所述使用者憑證為一密碼。

5. 如申請專利範圍第 1 項所述的方法，其中所述使用者憑證為一指紋掃描或視網膜掃描。

6. 如申請專利範圍第 1 項所述的方法，其中所述使用者憑證為來自一智慧卡之資料。

7. 如申請專利範圍第 1 項所述的方法，其中所述韌體之所述執行在用於所述計算裝置的一作業系統至記憶體中之一加載之前發生。

8. 如申請專利範圍第 1 項所述的方法，其中所述韌體之所述執行進一步使所述計算裝置：

自保存所述使用者設定檔之所述第二資料容器的一公用部分擷取一密碼恢復問題，且向所述使用者傳達所述恢復問題；

使用一使用者憑證驅動程式將對所述密碼恢復問題之一正確回答擴展至一回答密碼中；

自所述回答密碼創建一第三對稱密鑰；及

利用所述第三對稱密鑰解密保存所述第二對稱使用者設定檔密鑰之一複本的一第三資料容器的至少一部分；

使用所述第二對稱使用者設定檔密鑰之所述複本解密所述第二資料容器之所述私用部分；

基於所述第二資料容器之所述私用部分的一成功解密

之一判定鑑認所述使用者；及

在所述鑑認之後提供對一韌體服務之存取。

9. 如申請專利範圍第 1 項所述的方法，其中所述使用者憑證為一密碼，且提供存取之所述韌體服務為一密碼改變服務，且其中所述韌體之所述執行進一步使所述計算裝置：

自所述使用者接收一第二密碼；

自所述第二密碼產生一第三對稱密鑰；及

使用所述第三對稱密鑰加密保存所述使用者設定檔密鑰之所述第一資料容器的所述私用部分，所述第一資料容器之所述私用部分先前利用所述第一對稱密鑰解密。

10. 一種用於增強一計算裝置中之韌體提供之服務的安全性之方法，所述計算裝置經組態有韌體，所述韌體在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述第一資料容器儲存於非揮發性儲存器中；

利用一第二使用者憑證驅動程式接收一第二使用者憑證；

利用所述第二使用者憑證驅動程式自所述第二使用者憑證產生一第二對稱密鑰；

利用所述第二對稱密鑰解密一第二資料容器的至少一

部分，所述解密部分保存一第三對稱使用者設定檔密鑰，所述第三對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第三資料容器的一私用部分，所述第二及第三資料容器儲存於非揮發性儲存器中；

使用所述第三對稱使用者設定檔密鑰解密所述第三資料容器之所述私用部分；

基於所述第三資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

11. 如申請專利範圍第 10 項所述的方法，其中所述第二使用者憑證為一類型與所述第一使用者憑證不同之使用者憑證。

12. 一種非暫時性媒體，其保存用於增強一計算裝置中之韌體提供之服務的安全性之電腦可執行韌體指令，所述韌體在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述解密部分保存一第二對稱使用者設定檔密鑰，所述第二對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第二資料容器的一私用部分，所述第一及第二資料容器儲存於非揮發性儲存器中；

使用所述第二對稱使用者設定檔密鑰解密所述第二資

料容器之所述私用部分；

基於所述第二資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

13. 如申請專利範圍第 12 項所述的媒體，其中所述使用者憑證先前暫時與所述計算裝置中之韌體共用，以創建等同於所述第一對稱密鑰之一對稱密鑰，等同於所述第一對稱密鑰之所述對稱密鑰用以加密所述第一資料容器，且接著由所述韌體捨棄。

14. 如申請專利範圍第 12 項所述的媒體，其中所述指令在執行時進一步使所述計算裝置：

基於所述第二資料容器之所述私用部分中含有的一已知鹽值來判定所述成功解密。

15. 如申請專利範圍第 12 項所述的媒體，其中所述使用者憑證為一密碼。

16. 如申請專利範圍第 12 項所述的媒體，其中所述使用者憑證為一指紋掃描或視網膜掃描。

17. 如申請專利範圍第 12 項所述的媒體，其中所述使用者憑證為來自一智慧卡之資料。

18. 如申請專利範圍第 12 項所述的媒體，其中所述韌體指令在將用於所述計算裝置之一作業系統加載至記憶體中之前執行。

19. 如申請專利範圍第 12 項所述的媒體，其中所述指令在執行時進一步使所述計算裝置：

在保存所述使用者設定檔之所述第二資料容器的一公用部分中提供一密碼恢復問題；

使用一使用者憑證驅動程式將對所述密碼恢復問題之一正確回答擴展至一回答密碼中；

自所述回答密碼創建一第三對稱密鑰；及

利用所述第三對稱密鑰解密保存所述第二對稱使用者設定檔密鑰之一複本的一第三資料容器的至少一部分；

使用所述第二對稱使用者設定檔密鑰之所述複本解密所述第二資料容器之所述私用部分；

基於所述第二資料容器之所述私用部分的一成功解密之一判定鑑認所述使用者；及

在所述鑑認之後提供對一韌體服務之存取。

20. 如申請專利範圍第 12 項所述的媒體，其中所述使用者憑證為一密碼，且提供存取的所述韌體服務為一密碼改變服務，且其中所述指令在執行時進一步使所述計算裝置：

自所述使用者接收一第二密碼；

自所述第二密碼產生一第三對稱密鑰；及

使用所述第三對稱密鑰加密保存所述使用者設定檔密鑰之所述第一資料容器的所述私用部分，所述第一資料容器之所述私用部分先前利用所述第一對稱密鑰解密。

21. 一種非暫時性媒體，其保存用於增強一計算裝置中之韌體提供之服務的安全性之電腦可執行韌體指令，所述韌體在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述第一資料容器儲存於非揮發性儲存器中；

利用一第二使用者憑證驅動程式接收一第二使用者憑證；

利用所述第二使用者憑證驅動程式自所述第二使用者憑證產生一第二對稱密鑰；

利用所述第二對稱密鑰解密一第二資料容器的至少一部分，所述解密部分保存一第三對稱使用者設定檔密鑰，所述第三對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第三資料容器的一私用部分，所述第二及第三資料容器儲存於非揮發性儲存器中；

使用所述第三對稱使用者設定檔密鑰解密所述第三資料容器之所述私用部分；

基於所述第三資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

22. 如申請專利範圍第 21 項所述的媒體，其中所述第二使用者憑證為一類型與所述第一使用者憑證不同之使用者憑證。

23. 一種計算裝置，其提供用於韌體提供之服務之使用者鑑認的增強的安全性，所述計算裝置包括：

一處理器；

一輸入裝置；及

韌體，所述韌體包含一鑑認模組，所述鑑認模組在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述解密部分保存一第二對稱使用者設定檔密鑰，所述第二對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第二資料容器的一私用部分，所述第一及第二資料容器儲存於非揮發性儲存器中；

使用所述第二對稱使用者設定檔密鑰解密所述第二資料容器之所述私用部分；

基於所述第二資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

24. 如申請專利範圍第 23 項所述的計算裝置，其中所述使用者憑證先前暫時與所述計算裝置中之韌體共用，以創建等同於所述第一對稱密鑰之一對稱密鑰，等同於所述第一對稱密鑰之所述對稱密鑰用以加密所述第一資料容器，且接著由所述韌體捨棄。

25. 如申請專利範圍第 23 項所述的計算裝置，其中所述輸入裝置為一指紋讀取器，且所述使用者憑證為一指

紋。

26. 如申請專利範圍第 23 項所述的計算裝置，其中所述輸入裝置為一視網膜掃描讀取器，且所述使用者憑證為一視網膜掃描。

27. 如申請專利範圍第 23 項所述的計算裝置，其中所述韌體在將用於所述計算裝置之一作業系統加載至記憶體中之前執行。

28. 一種計算裝置，其提供用於韌體提供之服務之使用者鑑認的增強的安全性，所述計算裝置包括：

一處理器；

一輸入裝置；及

韌體，所述韌體包含一鑑認模組，所述鑑認模組在執行時使所述計算裝置：

利用一使用者憑證驅動程式接收一使用者憑證；

利用所述使用者憑證驅動程式自所述使用者憑證產生一第一對稱密鑰；

利用所述第一對稱密鑰解密一第一資料容器的至少一部分，所述第一資料容器儲存於非揮發性儲存器中；

利用一第二使用者憑證驅動程式接收一第二使用者憑證；

利用所述第二使用者憑證驅動程式自所述第二使用者憑證產生一第二對稱密鑰；

利用所述第二對稱密鑰解密一第二資料容器的至少一部分，所述解密部分保存一第三對稱使用者設定檔密鑰，

所述第三對稱使用者設定檔密鑰先前用以加密保存一使用者設定檔之一第三資料容器的一私用部分，所述第二及第三資料容器儲存於非揮發性儲存器中；

使用所述第三對稱使用者設定檔密鑰解密所述第三資料容器之所述私用部分；

基於所述第三資料容器之所述私用部分的一成功解密之一判定鑑認使用者；及

在所述鑑認之後提供對一韌體服務之存取。

29. 如申請專利範圍第 28 項所述的計算裝置，其中所述使用者憑證先前暫時與所述計算裝置中之韌體共用，以創建等同於所述第一對稱密鑰之一對稱密鑰，等同於所述第一對稱密鑰之所述對稱密鑰用以加密所述第一資料容器，且接著由所述韌體捨棄。

圖式

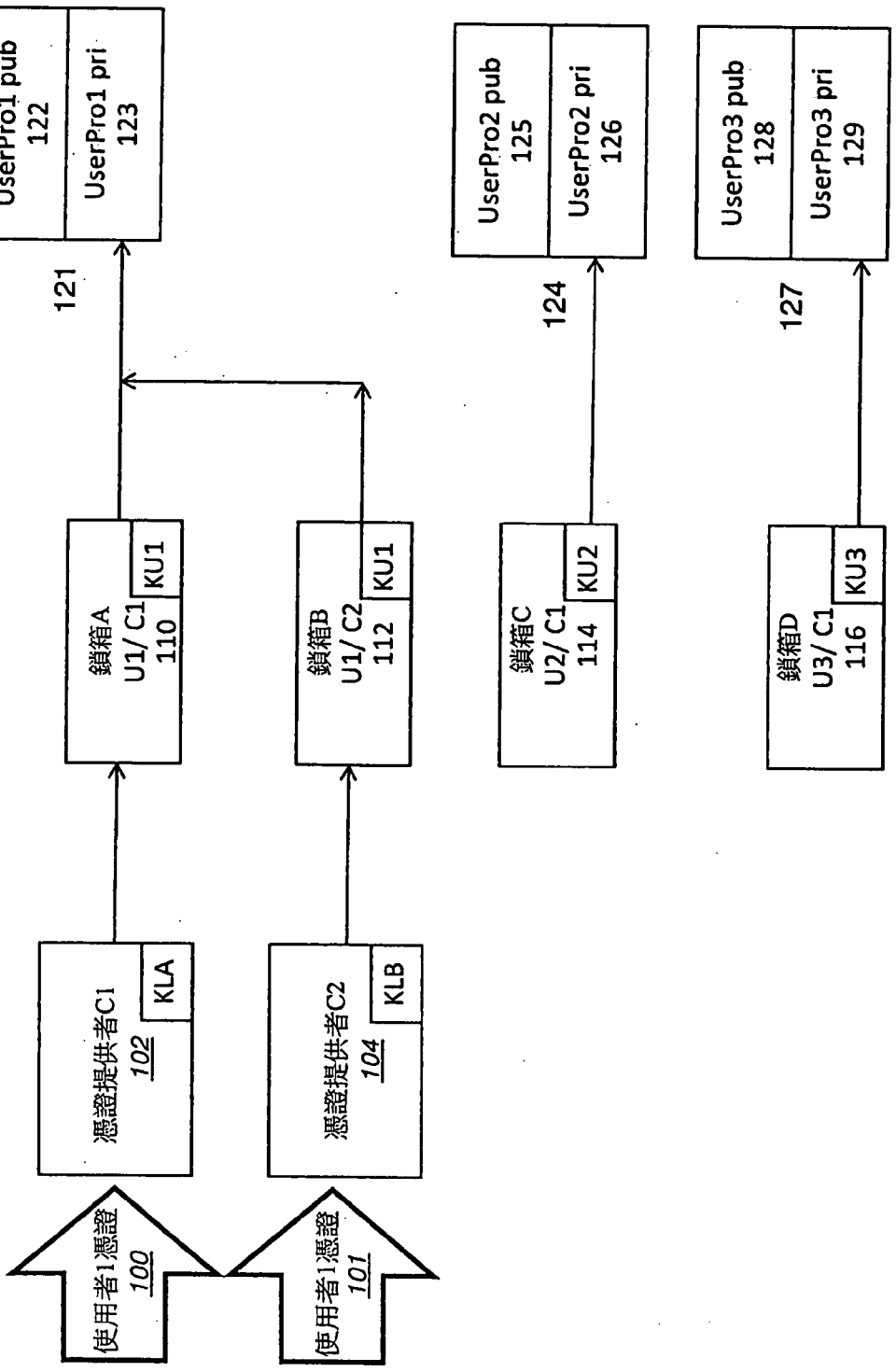
使用者1憑證
100
使用者1憑證
101
憑證提供者C1
102
KLA
憑證提供者C2
104
KLB
鎖箱A
U1/ C1
110
KU1
鎖箱B
U1/ C2
112
KU1
鎖箱C
U2/ C1
114
KU2
鎖箱D
U3/ C1
116
KU3
121
124
127
UserPro1 pub
122
UserPro1 pri
123
UserPro2 pub
125
UserPro2 pri
126
UserPro3 pub
128
UserPro3 pri
129

圖1

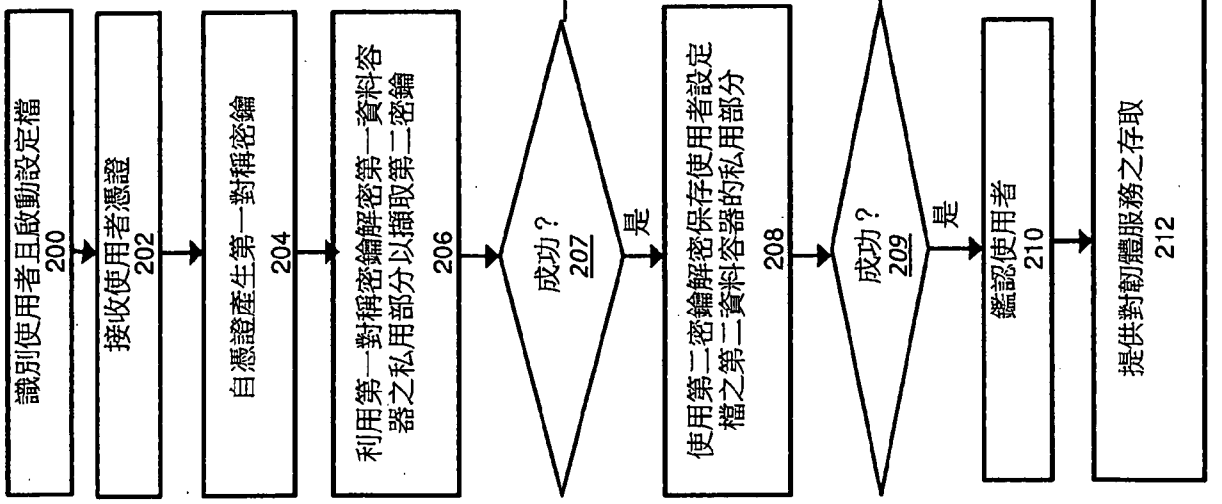
識別使用者且啟動設定檔
200
接收使用者憑證
202
自憑證產生第一對稱密鑰
204
利用第一對稱密鑰解密第一資料容器之私用部分以擷取第二密鑰
206
成功？
207
否
是
鑑認失敗
使用第二密鑰解密保存使用者設定檔之第二資料容器的私用部分
208
成功？
209
否
是
鑑認使用者
210
提供對韌體服務之存取
212

圖2

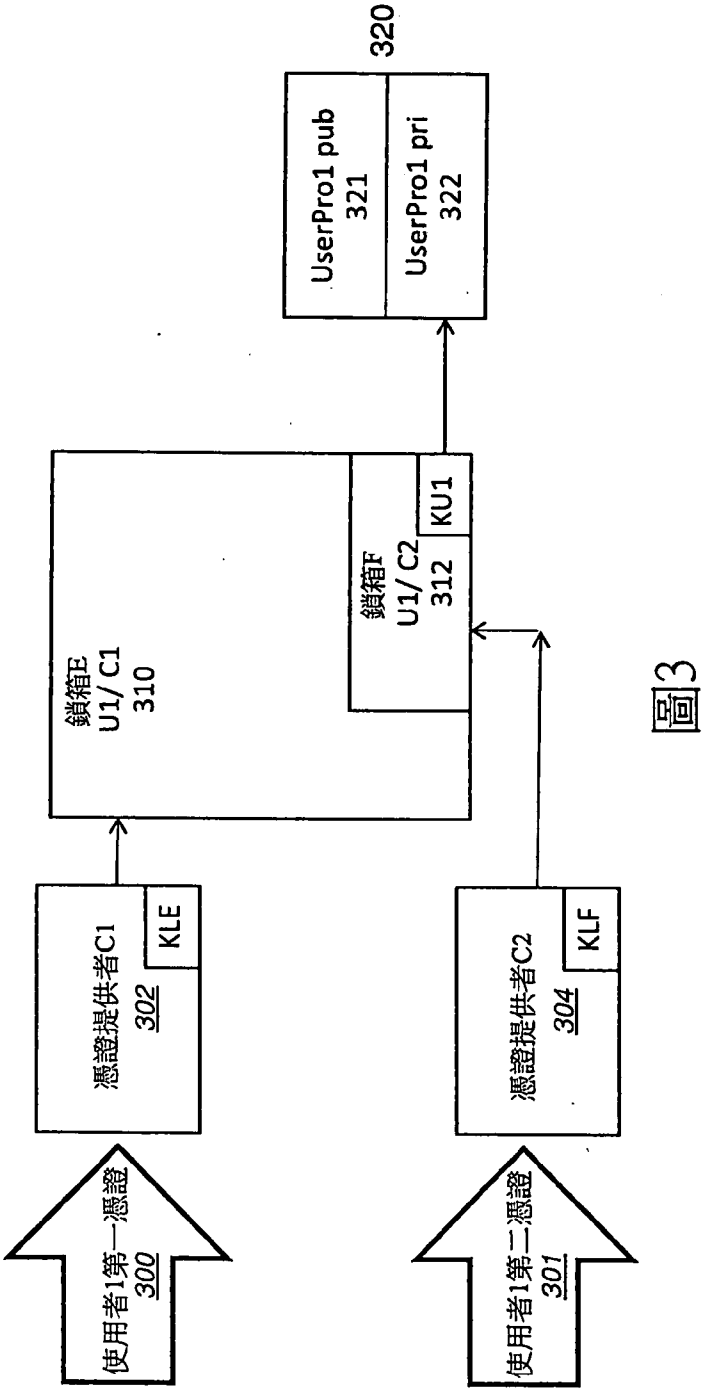
使用者1第一憑證
300
憑證提供者C1
302
KLE
使用者1第二憑證
301
憑證提供者C2
304
KLF
鎖箱E
U1/ C1
310
鎖箱F
U1/ C2
312
KU1
UserPro1 pub
321
UserPro1 pri
322
320

圖3

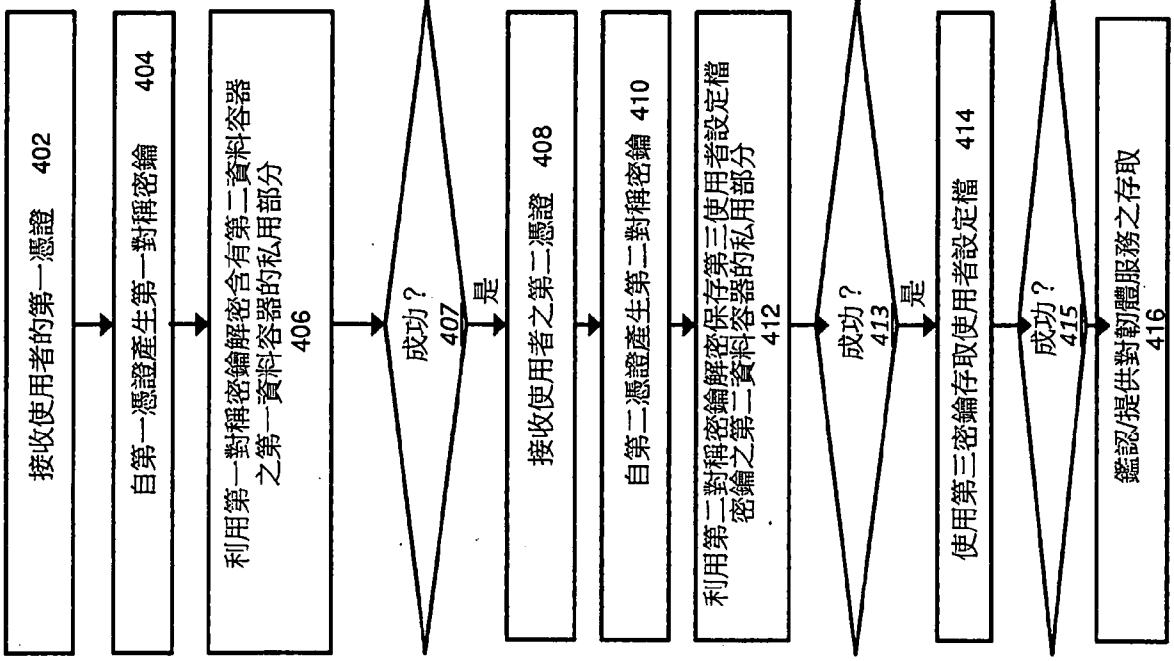
接收使用者的第一憑證 402
自第一憑證產生第一對稱密鑰 404
利用第一對稱密鑰解密含有第二資料容器之第一資料容器的私用部分 406
成功？ 407
否
是
接收使用者之第二憑證 408
自第二憑證產生第二對稱密鑰 410
利用第二對稱密鑰解密保存第三使用者設定檔密鑰之第二資料容器的私用部分 412
成功？ 413
否
是
使用第三密鑰存取使用者設定檔 414
成功？ 415
否
鑑認失敗
鑑認/提供對軀體服務之存取 416

圖4

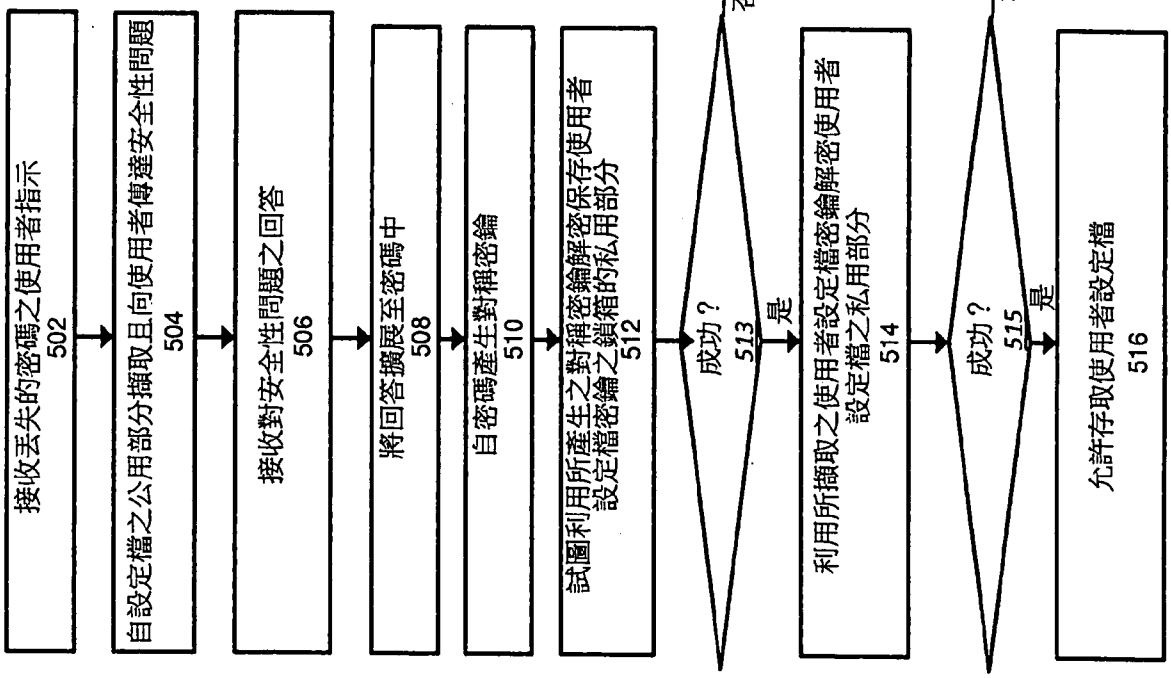
接收丟失的密碼之使用者指示
502
自設定檔之公用部分擷取且向使用者傳達安全性問題
504
接收對安全性問題之回答
506
將回答擴展至密碼中
508
自密碼產生對稱密鑰
510
試圖利用所產生之對稱密鑰解密保存使用者設定檔密鑰之鎖箱的私用部分
512
成功？
513
否
是
利用所擷取之使用者設定檔密鑰解密使用者設定檔之私用部分
514
成功？
515
否
是
失敗
允許存取使用者設定檔
516

圖5

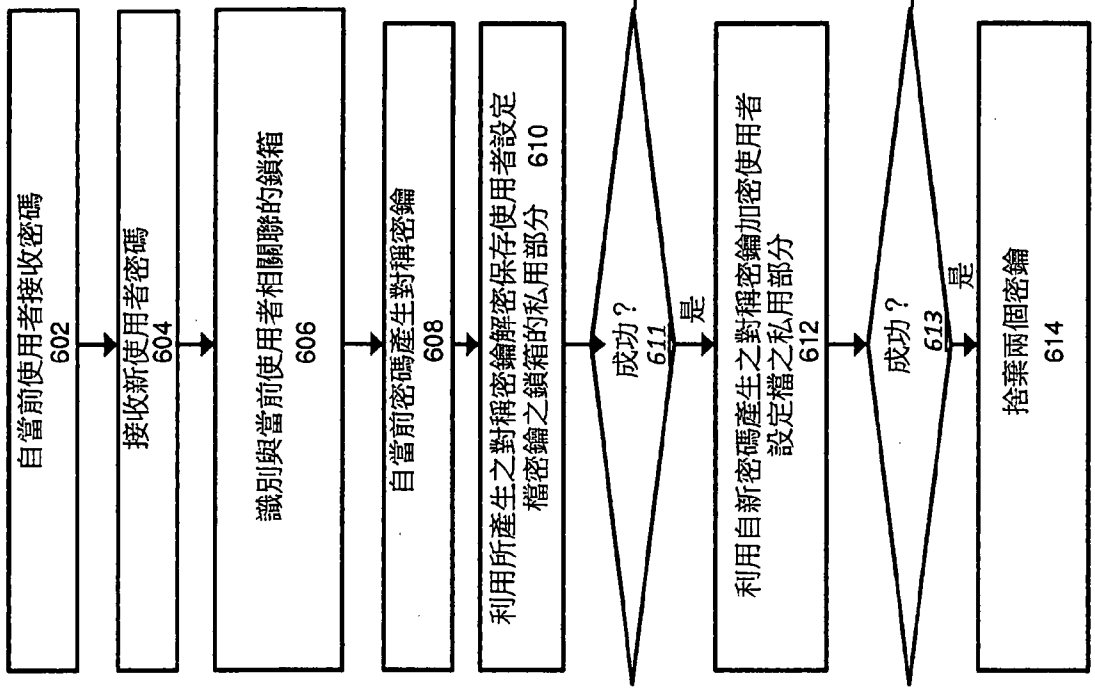
自當前使用者接收密碼
602
接收新使用者密碼
604
識別與當前使用者相關聯的鎖箱
606
自當前密碼產生對稱密鑰
608
利用所產生之對稱密鑰解密保存使用者設定檔密鑰之鎖箱的私用部分 610
成功？
611
否
是
利用自新密碼產生之對稱密鑰加密使用者設定檔之私用部分
612
成功？
613
否
是
捨棄兩個密鑰
614
失敗

圖6

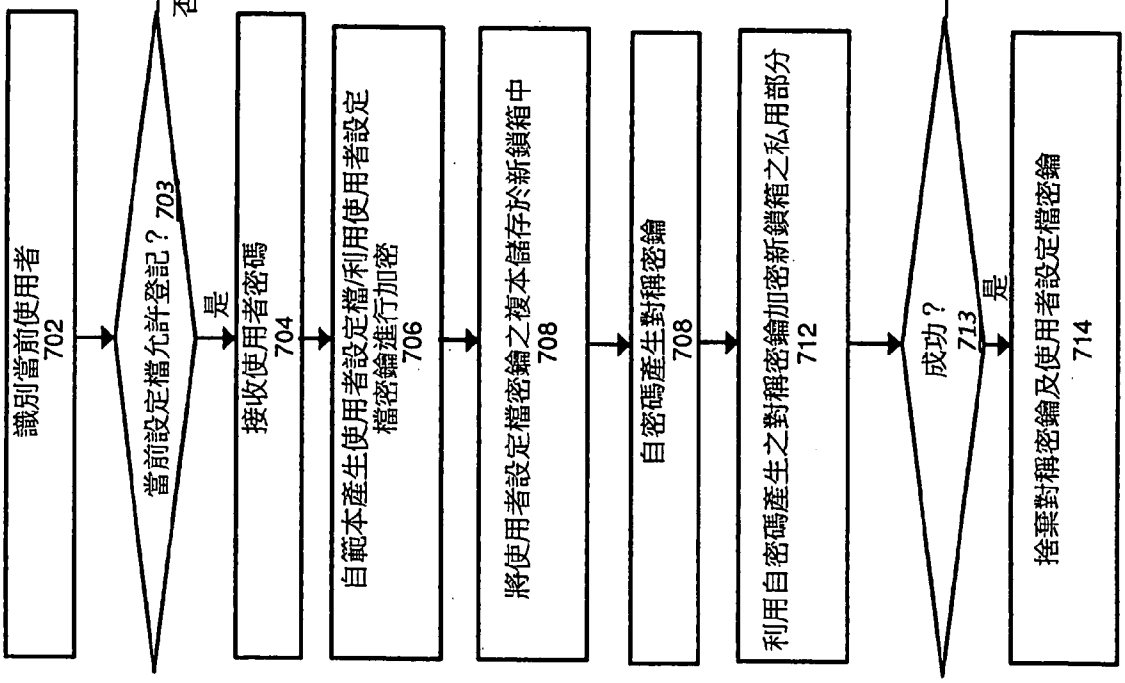
識別當前使用者
702
當前設定檔允許登記？ 703
否
是
失敗
接收使用者密碼
704
自範本產生使用者設定檔/利用使用者設定檔密鑰進行加密
706
將使用者設定檔密鑰之複本儲存於新鎖箱中
708
自密碼產生對稱密鑰
708
利用自密碼產生之對稱密鑰加密新鎖箱之私用部分
712
成功？ 713
否
是
捨棄對稱密鑰及使用者設定檔密鑰
714

圖7

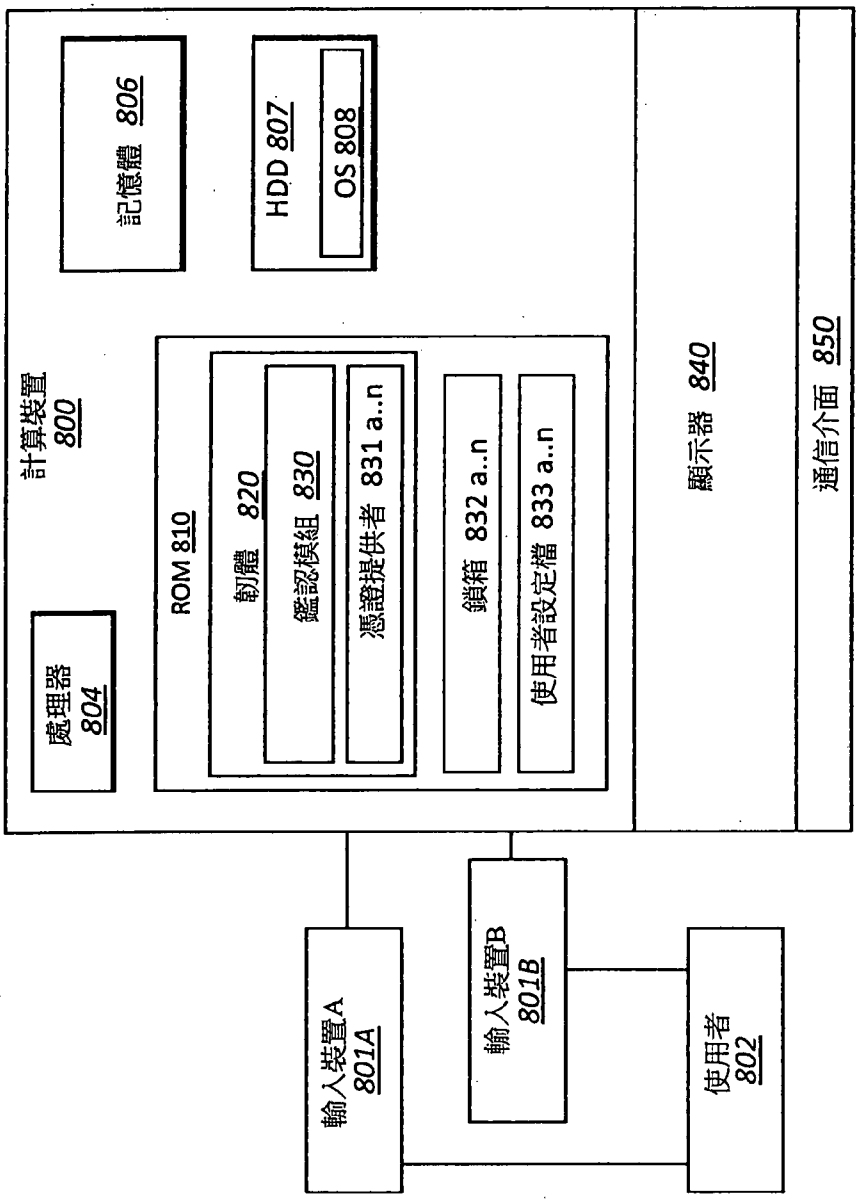
計算裝置
800
處理器
804
記憶體 806
ROM 810
韌體 820
鑑認模組 830
憑證提供者 831 a..n
鎖箱 832 a..n
使用者設定檔 833 a..n
HDD 807
OS 808
顯示器 840
通信介面 850
輸入裝置A
801A
輸入裝置B
801B
使用者
802

圖8