I587172

(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 I587172 B**

(45)公告日： 中華民國 106 (2017) 年 06 月 11 日

(21)申請案號：104132537 (22)申請日： 中華民國 104 (2015) 年 10 月 02 日

(51)Int. Cl.： *G06F21/62 (2013.01)* *G06F21/64 (2013.01)*

(30)優先權：2014/11/06 美國 14/534,305

(71)申請人：英特爾公司 (美國) INTEL CORPORATION (US)
美國

(72)發明人：強森 西蒙P JOHNSON, SIMON P. (GB)；亞特曼 亞薛M ALTMAN, ASHER M. (US)；達斯 阿布希雪克DAS, ABHISHEK (IN)；史卡拉塔 文森R SCARLATA, VINCENT R. (US)

(74)代理人：惲軼群

(56)參考文獻：

US 20070094719A1 US 20090279699A1

US 20130036103A1 US 20130283056A1

US 20140317417A1

審查人員：何偉權

申請專利範圍項數：25 項 圖式數：5 共 44 頁

(54)名稱

用於建立安全工作空間的所有權之系統

SYSTEM FOR ESTABLISHING OWNERSHIP OF A SECURE WORKSPACE

(57)摘要

本申請案係有關於建立一安全工作空間(SW)之所有權。一用戶端裝置可將一 SW 資料結構(SWDS)提供至一 SW 配置器。一 SWDS 可包含一原始 SW 及一公開金鑰之一雜湊，且可藉由對應於該公開金鑰之一私密金鑰來簽署。該 SW 配置器可使得產生包括使用該 SWDS 起始之一 SW 之一執行容器(EC)。該用戶端裝置可使用連同該公開金鑰之一複本一起傳輸之一請求(藉由該私密金鑰簽署)主張 SW 所有權。可藉由一所有權判定模組來判定 SW 所有權，該所有權判定模組使用與該請求一起接收之該公開金鑰驗證該請求之簽章，判定該所接收公開金鑰之一雜湊且比較該所接收公開金鑰之該雜湊與該 SWDS 中的該公開金鑰之一雜湊。

The present application is directed to establishing ownership of a secure workspace (SW). A client device may provide a SW data structure (SWDS) to a SW configurator. A SWDS may comprise a hash of an original SW and a public key, and may be signed by a private key corresponding to the public key. The SW configurator may cause an execution container (EC) to be generated including a SW initiated using the SWDS. The client device may claim SW ownership using a request (signed by the private key) transmitted along with a copy of the public key. SW ownership may be determined by an ownership determination module that verifies the signature of the request using the public key received with the request, determines a hash of the received public key and compares the hash of the received public key to a hash of the public key in the SWDS.

指定代表圖：

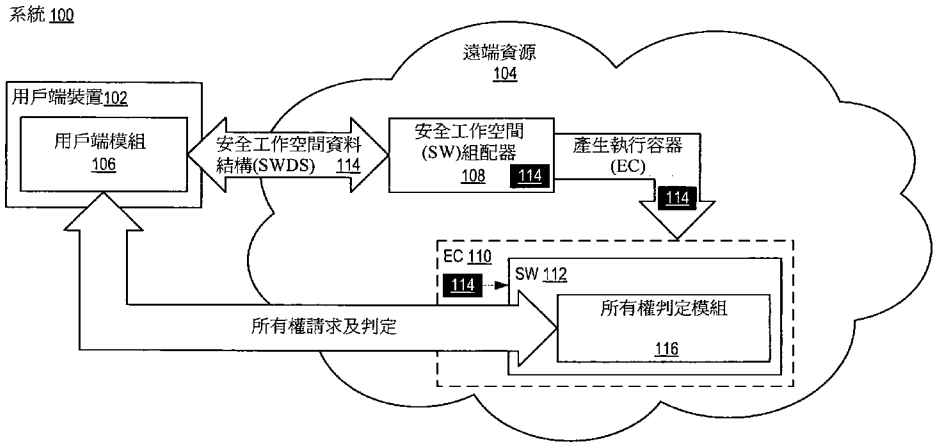

圖1

符號簡單說明：

100・・・系統

102・・・用戶端裝置

104・・・遠端資源

106・・・用戶端模組

108・・・SW 配置器

110・・・EC

112・・・SW

114・・・SWDS

116・・・所有權判定模組

I587172

發明摘要 公告本

※ 申請案號：104132537

※ 申請日：104.10.02 ※IPC 分類：G06F 21/62 (2013.01)
21/64 (2013.01)

【發明名稱】(中文/英文)

用於建立安全工作空間的所有權之系統

SYSTEM FOR ESTABLISHING OWNERSHIP OF A SECURE WORKSPACE

【中文】

本申請案係有關於建立一安全工作空間(SW)之所有權。一用戶端裝置可將一SW資料結構(SWDS)提供至一SW配置器。一SWDS可包含一原始SW及一公開金鑰之一雜湊，且可藉由對應於該公開金鑰之一私密金鑰來簽署。該SW配置器可使得產生包括使用該SWDS起始之一SW之一執行容器(EC)。該用戶端裝置可使用連同該公開金鑰之一複本一起傳輸之一請求(藉由該私密金鑰簽署)主張SW所有權。可藉由一所有權判定模組來判定SW所有權，該所有權判定模組使用與該請求一起接收之該公開金鑰驗證該請求之簽章，判定該所接收公開金鑰之一雜湊且比較該所接收公開金鑰之該雜湊與該SWDS中的該公開金鑰之一雜湊。

【英文】

The present application is directed to establishing ownership of a secure workspace (SW). A client device may provide a SW data structure (SWDS) to a SW configurator. A SWDS may comprise a hash of an original SW and a public key, and may be signed by a private key corresponding to the public key. The SW configurator may cause an execution container (EC) to be generated including a SW initiated using the SWDS. The client device may claim SW ownership using a request (signed by the private key) transmitted along with a copy of the public key. SW ownership may be determined by an ownership determination module that verifies the signature of the request using the public key received with the request, determines a hash of the received public key and compares the hash of the received public key to a hash of the public key in the SWDS.

【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...系統
102...用戶端裝置
104...遠端資源
106...用戶端模組
108...SW配置器
110...EC
112...SW
114...SWDS
116...所有權判定模組

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

用於建立安全工作空間的所有權之系統

SYSTEM FOR ESTABLISHING OWNERSHIP OF A SECURE WORKSPACE

【技術領域】

發明領域

[0001]本發明係關於系統安全，且更特定而言，係關於一種允許裝置建立位於遠端資源中之安全工作空間之所有權的系統。

【先前技術】

發明背景

[0002]基於現在可能電子地進行之多種增長的異動，防護電子資訊已變成重要問題。包括(例如)黑客、惡意軟體(例如，惡意程式碼)(諸如，病毒、隱匿程式(rootkits)等)之各種威脅可共用至少一個目的：避開現有保護措施以獲得對另一使用者之裝置之存取或控制。使用裝置執行日常異動之使用者可能並未察覺其裝置已受損害，且可能不知不覺地將敏感性個人、金融及/或專有資料提供給第三方。不斷地開發技術以抗擊此等類型之攻擊。然而，當新病毒保護策略顯現時，黑客設法攻擊裝置內之較低層級，從而在裝置中優先權高於保護軟體之層級獲得存取及/或控制。因此，裝置製造商正將安全措施建置至裝置之實際硬體中。舉例

而言，可在裝置初始化之初期實現此等安全特徵，且可藉由在將程式載入至裝置中時執行安全檢查而確保稍後載入之程式爲安全的。

[0003]舉例而言，在初始化期間，裝置可保留僅可供已知良好之程式存取的記憶體之一部分。以此方式，可保護儲存於記憶體之該部分中的敏感性及/或機密資料免受攻擊。然而，可能存在一種情況，其中已知良好之軟體並不常駐於與受保護之記憶體相同的裝置中。舉例而言，使用者裝置中的已知良好之程式(例如，「用戶端」程式)可能需要存取位於至少一個遠端計算裝置(例如，在雲端架構中操作)中的受保護記憶體之一部分。雖然可能需要用戶端程式能夠存取常駐於至少一個其他裝置中之受保護記憶體，但可保證受保護記憶體免於由受保護記憶體之「擁有者」以外的任何軟體存取，該「擁有者」可在(例如)第一次創建記憶體之受保護部分時進行指派。此要求可能嚴重地限制了此類型之安全技術可能適用的應用。

【發明內容】

[0004]依據本發明之一實施例，係特地提出一種包括至少一個裝置之裝置，其包含：一通訊模組，其用以與至少一用戶端裝置相互作用；以及一安全工作空間配置器，其用以：自該用戶端裝置接收一安全工作空間資料結構；及使一安全工作空間被包括在由遠端資源所產生之一執行容器內，該安全工作空間係基於該安全工作空間資料結構。

【圖式簡單說明】

[0005]所主張標的物之各種實施例的特徵及優點將在以下實施方式進行時且在參看圖式後變得顯而易見，其中相似編號指明相似部分，且其中：

圖1說明根據本發明之至少一個實施例的用於建立安全工作空間之所有權的實例系統；

圖2說明根據本發明之至少一個實施例的用於用戶端裝置及構成可用之遠端資源之至少一個裝置的實例組配；

圖3說明根據本發明之至少一個實施例的可能在用戶端模組、安全工作空間配置器及安全工作空間之間發生的實例相互作用；

圖4說明根據本發明之至少一個實施例的用於自用戶端裝置之角度建立安全工作空間之所有權的實例操作；及

圖5說明根據本發明之至少一個實施例的用於自遠端資源之角度建立安全工作空間之所有權的實例操作。

[0006]儘管以下實施方式將參考例示性實施例來進行，但其許多替代例、修改及變化對於熟習此項技術者而言將爲顯而易見的。

【實施方式】

較佳實施例之詳細說明

[0007]本申請案係有關於建立一安全工作空間(SW)之所有權。在至少一個實施例中，用戶端裝置可將SW資料結構(SWDS)提供至位於遠端資源中之SW配置器。一實例SWDS可包含一原始SW及一公開金鑰之一雜湊，且可使用對應於該公開金鑰之一私密金鑰來簽署。該SW配置器可接

著使得產生包括基於該SWDS之一SW之一執行容器(EC)。用戶端裝置可稍後藉由向遠端資源傳輸請求而主張SW之所有權。該請求可藉由該私密金鑰來簽署，且可連同該公開金鑰之一複本一起傳輸。SW中之所有權判定模組可接著藉由(例如)以下操作判定用戶端裝置是否擁有SW：使用與該請求一起接收之公開金鑰驗證請求之簽章，判定與該請求一起接收之公開金鑰之雜湊，且接著比較與該請求一起接收之公開金鑰之雜湊與在SWDS中接收的公開金鑰之雜湊。若判定公開金鑰之雜湊匹配，則可允許用戶端裝置主張SW之所有權。

[0008]在至少一個實施例中，至少一個裝置可包含(例如)通訊模組及SW配置器。通訊模組可與至少一用戶端裝置相互作用。SW配置器最初可自用戶端裝置接收SWDS。SW配置器可接著使得將SW包括於由遠端資源產生之EC內，該SW係基於SWDS。

[0009]實例SWDS可包含關於SW之資料及公開金鑰，SWDS係在藉由對應於公開金鑰之私密金鑰簽署之訊息中接收。關於SW之資料可包含自SW量測之雜湊值。EC可進一步基於SWDS初始化SW，SW之初始化包括量測安全工作空間資料結構中之公開金鑰之雜湊值。

[0010]在至少一個實施例中，SW可進一步包含所有權判定模組以：經由通訊模組自用戶端裝置接收包括取得SW之所有權之至少一請求的經簽署訊息及公開金鑰，及至少基於該經簽署訊息及該SWDS判定用戶端裝置是否經授權

而取得SW之所有權。判定用戶端裝置是否經授權而取得SW之所有權的所有權判定模組可包含進行以下操作的所有權判定模組：利用與經簽署訊息一起接收之公開金鑰驗證經簽署訊息之簽章，藉由量測公開金鑰判定與經簽署訊息一起接收之公開金鑰的雜湊值，藉由比較與經簽署訊息一起接收之公開金鑰之雜湊與在初始化SW時判定的公開金鑰之雜湊而驗證SW之所有權，且在與經簽署訊息一起接收之公開金鑰之雜湊匹配在初始化SW時判定的公開金鑰之雜湊的情況下，將SW之所有權授與用戶端裝置。在至少一個實施例中，SW爲基於軟體防護擴展(SGX)技術之安全區域且SWDS爲SGX SIGSTRUCT資料結構。

[0011]與本發明一致之用戶端裝置可包含(例如)通訊模組及用戶端模組。通訊模組可與至少一遠端資源相互作用。用戶端模組可藉由量測用於產生新SW的SW之原始版本而判定SW之雜湊值，產生公開金鑰及對應私密金鑰，至少將該雜湊值及該公開金鑰置放至SWDS中，及將SWDS傳輸至遠端資源。可自(例如)遠端資源中之安全工作空間配置器接收SW之雜湊值。用戶端模組可進一步產生包含取得SW之所有權之請求的訊息，藉由私密金鑰簽署該訊息且將簽署訊息及公開金鑰傳輸至遠端資源。在至少一個實施例中，SW爲基於SGX技術之安全區域且SWDS爲SGX SIGSTRUCT資料結構。與本發明一致的用於建立SW之所有權之方法可包含(例如)在SW配置器處自用戶端裝置接收SWDS，該SW配置器常駐於遠端資源中且使得將SW包括於

由遠端資源產生之EC內，該SW係基於SWDS。

[0012]圖1說明根據本發明之至少一個實施例的用於建立安全工作空間之所有權的實例系統。系統100可包含(例如)至少用戶端裝置102及遠端資源104。用戶端裝置102之實例可包含(但不限於)：行動通訊裝置，諸如蜂巢式手機或智慧型手機，其基於來自Google公司之Android® OS、來自Apple公司之iOS®、來自Microsoft公司之Windows® OS、來自Apple公司之Mac OS、來自Linux Foundation之Tizen OS、來自Mozilla Project之Firefox OS、來自Blackberry公司之Blackberry® OS、來自Hewlett-Packard公司之Palm® OS、來自Symbian Foundation之Symbian® OS等；行動計算裝置，諸如平板電腦，如來自Apple公司之iPad®、來自Microsoft公司之Surface®、來自Samsung公司之Galaxy Tab®、來自Amazon公司之Kindle Fire®等；包括由Intel公司製造之低功率晶片組的Ultrabook®、迷你筆記型電腦、筆記型電腦、膝上型電腦、掌上型電腦等；通常固定之計算裝置，諸如桌上型電腦、智慧型電視、如來自Intel公司之下一代計算單元(NUC)平台的小型計算解決方案(例如，對於空間受限應用程式、TV機上盒等)；等等。遠端資源104可包含可供用戶端裝置102經由網路連接存取之至少一個計算裝置。實例網路可包括(但不限於)區域網路(LAN)、如網際網路之廣域網路(WAN)、全域網路(GAN)等。在至少一個實施例中，遠端資源104可包含作爲雲端計算架構之部分操作的至少一個資料伺服器。雲端計算架構可包含(例如)個別地或協調

地操作以爲用戶端裝置102提供各種資料處理相關服務之多個資料伺服器。

[0013]用戶端裝置102可包含(例如)至少用戶端模組106。用戶端模組106可包括可經組配以存取SW 112之設備及/或軟體。如本文所引用之「存取」可包括將資料儲存於SW 112中，自SW 112讀取資料，執行載入於SW 112中之程式等。出於解釋起見，與本發明一致之真實世界使用情況之實例可包含用戶端裝置102爲智慧型手機且用戶端模組106爲提供使用者介面以存取使用者之個人金融帳戶之應用程式，其中可將存取金融帳戶(例如，賬戶編號、使用者名稱、密碼等)所需之資訊儲存於遠端資源104中以保護用戶端裝置102從而免於丟失、被盜或以其他方式受損害。雖然此實例解決方案可保護免遭用戶端裝置102中之容易顯而易見的易損性，但當將存取資訊儲存於遠端資源104中時，尤其是在給定：遠端資源104可爲用於對應於大量使用者(例如，利用用戶端模組106之任何使用者)之存取資訊之儲存庫的情況下，存取資訊同樣可能易受攻擊，且因此，可能爲攻擊的有吸引力之目標。因此，以下情形可爲有益的：按可提供高等級安全之方式進一步保護儲存於遠端資源104中之資訊，該高等級安全之方式使得僅用戶端模組106可能能夠存取。

[0014]遠端資源104可包含(例如)可使得EC 110包括基於SWDS 114組配之至少SW 112的至少SW配置器108。如本文所引用，EC 110大體上可包含基於軟體之構築體，其可

能能夠仿真經類似組配的基於硬體之資料處理裝置的操作。EC 110之實例可包括(但不限於)諸如通常與來自Intel公司之虛擬化技術(VT)相關聯之虛擬機(VM)、如由Docker公司開發之Docker引擎、基於Linux核心之虛擬機(KVM)等。在至少一個實施例中，SW配置器108可包含用於進行以下操作之設備及/或軟體：用於儲存自用戶端裝置102接收之SWDS 114，及用於使得產生EC 110，包括可供EC 110用以產生SW 112之至少SWDS 114。SW 112可(例如)爲受信任執行環境(TEE)，在該環境中，可執行已知良好之程式，可按安全方式儲存機密資訊，等等。大體而言，SW 112可包含一組計算資源，該組計算資源爲安全的以使得在SW 112內執行之程式及與執行程式相關聯之任何資料爲隔離的。除了可開始或停止程式及可插入或刪除相關聯之資料以外，外部行動者在程式執行期間無法受SW 112內之程式/資料干擾或無法觀測到SW 112內之程式/資料。可按受控方式釋放離開SW 112之任何資料。與本發明一致，在SW 112內執行之至少一個已知良好之程式可執行本文關於SW 112所揭示之任何操作或所有操作。在一實例實施中，SW 112可使用由Intel公司開發之軟體防護擴展(SGX)技術。SGX可提供系統記憶體內之安全且硬體加密之計算及儲存區域，其內容無法藉由特許程式碼或甚至經由硬體探針至記憶體匯流排之施加來解密。當SW 112受SGX保護時，與本發明一致之實施例使得入侵者不可能解密SW 112之內容。受保護資料在SGX外部無法被觀測到，且因此，在SGX外部不可被

存取。

[0015]在使用SGX實施SW 112之實例實施中，可簽署程式之識別碼(例如，基於各程式之內容的密碼編譯雜湊量測結果)且將其儲存於各程式內部。當接著將程式載入至SW 112中時，處理器可驗證程式之量測結果(例如，如藉由處理器計算)與先前嵌入於程式內部之量測結果相同。用以簽署嵌入之量測結果的簽章亦爲可驗證的，此係因爲處理器可具備用以在程式載入時間驗證簽章之公開金鑰。此方式的惡意程式碼無法篡改程式，而且亦不會更改其可驗證之量測結果。惡意程式碼亦無法欺騙簽章，此係因爲簽署金鑰在程式之原創者處爲安全的。因此，任何惡意程式碼無法讀取軟體，寫入軟體或變更軟體。此外，亦可將資料保護於TEE模組106中。舉例而言，SW 112中之已知良好之程式可加密諸如金鑰、密碼、使用權等之資料，以使得僅經驗證之良好程式可解密此資料。在使用SGX之至少一個實施例中，SW 112可爲安全區域且SWDS 114可爲SIGSTRUCT資料結構。SIGSTRUCT資料結構可包含來自區域簽署者的關於區域之資訊，包括(例如)如SHA256之區域雜湊及四個3072-位整數(例如，模數、簽章、Q1及Q2)。雖然RSA簽章可能不需要Q1及Q2，但此等整數值可用以加速簽章驗證。與本發明一致，可改變SIGSTRUCT資料結構之內容中之一些內容或全部的用途以保持其他資訊(例如，公開金鑰)，如將關於圖3描述。

[0016]在一操作實例中，用戶端裝置102中之用戶端模

組106可與SW配置器108相互作用以建立SWDS 114。相互作用可包括(例如)判定用於包含於SW配置器108中之SW 112之原始版本的雜湊，產生公開金鑰及對應私密金鑰，將SW 112之雜湊及公開金鑰之複本置放於SWDS 114中，及將SWDS 114傳輸至SW配置器108。在至少一個實施例中，可藉由SW配置器108判定SW 112之雜湊且將其傳輸至用戶端模組106。可根據公開金鑰密碼編譯方法產生公開金鑰及私密金鑰，該等公開金鑰密碼編譯方法包括(例如)RSA、Diffie-Hellman、數位簽章演算法(DSA)等。可藉由私密金鑰簽署SWDS 114，之後將其傳輸至遠端資源104。私密/公開金鑰對可基於(例如)客戶之偏好而表示客戶(例如，用戶端裝置102)或SW 112。當在遠端資源104中產生EC 110時，SW配置器108可使得將SWDS 114置放至EC 110中(例如，除其他投與憑證之外)。當初始化SW 112時，EC 110可接著利用SWDS 114。在至少一個實施例中，在初始化期間，可經由SWDS 114中之公開金鑰判定雜湊，當判定SW 112之擁有者時，公開金鑰之雜湊爲重要的。

[0017]用戶端模組106可接著試圖主張SW 112之所有權，該情形可包括用戶端模組106使得裝置102向遠端資源104傳輸針對SW 112之所有權的請求。該請求可使用私密金鑰來簽署且可包括公開金鑰之複本。在至少一個實施例中，可在EC 110中由所有權判定模組116接收請求。所有權判定模組116可接著(例如)使用與請求一起接收之公開金鑰驗證關於請求之簽章，且可判定與請求一起接收之公開金鑰是

否與包括於SWDS 114中之公開金鑰相同。若判定金鑰匹配，則所有權判定模組116可授與針對所有權之請求。用戶端模組106可接著被告知其爲SW 112之擁有者且可能能夠存取SW 112。重要的是應注意，當所有權判定模組116經展示爲常駐於SW 112內時，所有權判定模組116亦有可能常駐於EC 110內之其他處或甚至遠端資源104內之其他處。

[0018]圖2說明根據本發明之至少一個實施例的用於用戶端裝置102及構成可用之遠端資源104之至少一個裝置的實例組配。詳言之，用戶端裝置102'及/或遠端資源104'可能能夠執行諸如圖1中所揭示之實例功能性。然而，用戶端裝置102'及遠端資源104'僅意欲作爲可在與本發明一致之實施例中使用的裝置之實例，但並不意欲將此等各種實施例限於實施之任何特定方式。

[0019]用戶端裝置102'可包含(例如)經組配以管理裝置操作之系統模組200。系統模組200可包括(例如)處理模組202、記憶體模組204、電力模組206、使用者介面模組208及通訊介面模組210。用戶端裝置102'亦可包括通訊模組212。雖然將通訊模組212說明爲與系統模組200分離，但圖2中所展示之實例實施僅係出於解釋起見而提供。可將與通訊模組212相關聯之功能性中之一些功能性或全部併入至系統模組200中。

[0020]在用戶端裝置102'中，處理模組202可包含位於單獨組件中之一或多個處理器，或替代地，在單一組件中體現之一或多個處理核心(例如，在系統單晶片(SoC)組配中)

及任何處理器相關支援電路系統(例如，橋接介面等)。實例處理器可包括(但不限於)可購自Intel公司之各種基於x86之微處理器，包括Pentium、Xeon、Itanium、Celeron、Atom、核心i-系列產品系列中之彼等微處理器、進階RISC (例如，精簡指令集計算)機器或「ARM」處理器等。支援電路系統之實例可包括經組配以提供介面之晶片組(例如，可購自Intel公司之北橋、南橋等)，處理模組202可經由該介面與用戶端裝置102'中的可按不同速度、在不同匯流排上等操作之其他系統組件相互作用。通常與支援電路系統相關聯之功能性中之一些功能性或全部亦可包括於與處理器相同之實體封裝中(例如，諸如在可購自Intel公司之Sandy Bridge處理器系列中)。

[0021]處理模組202可經組配以執行用戶端裝置102'中之各種指令。指令可包括經組配以使得處理模組202執行與讀取資料、寫入資料、處理資料、制定資料、轉換資料、變換資料等有關之活動的程式碼。可將資訊(例如，指令、資料等)儲存於記憶體模組204中。記憶體模組204可包含呈固定或抽取式格式之隨機存取記憶體(RAM)或唯讀記憶體(ROM)。RAM可包括經組配以在用戶端裝置102'之操作期間保持資訊之依電性記憶體，諸如靜態RAM (SRAM)或動態RAM (DRAM)。ROM可包括基於BIOS、UEFI等組配以在啓動用戶端裝置102'時提供指令的非依電性(NV)記憶體模組、諸如電子可規劃ROM (EPROM)之可規劃記憶體、快閃記憶體等。其他固定/抽取式記憶體可包括(但不限於)：磁

性記憶體，諸如軟碟、硬碟機等；電子記憶體，諸如固態快閃記憶體(例如，嵌入式多媒體卡(eMMC)等)；抽取式記憶卡或棒(例如，微儲存裝置(uSD)、USB等)；光學記憶體，諸如基於緊密光碟之ROM (CD-ROM)、數位影音光碟(DVD)、藍光光碟等。

[0022]電力模組206可包括內部電源(例如，電池組、燃料電池等)及/或外部電源(例如，機電或太陽能產生器、電網、燃料電池等)，及經組配以向用戶端裝置102'供應操作所需之電力的相關電路系統。使用者介面模組208可包括硬體及/或軟體以允許使用者與用戶端裝置102'相互作用，諸如各種輸入機構(例如，麥克風、開關、按鈕、把手、鍵盤、揚聲器、觸敏表面、經組配以俘獲影像及/或感測接近性、距離、運動、示意動作、定向等之一或多個感測器)及各種輸出機構(例如，揚聲器、顯示器、照亮/閃光指示器、用於振動、運動等之機電組件)。使用者介面模組208中之硬體可併入於用戶端裝置102'內及/或可經由有線或無線通訊媒體耦接至用戶端裝置102'。

[0023]通訊介面模組210可經組配以管理封包投送及通訊模組212之其他控制功能，該通訊模組可包括經組配以支援有線及/或無線通訊之資源。在一些情況下，用戶端裝置102'可包含皆由集中式通訊介面模組210管理之一個以上通訊模組212 (例如，包括用於有線協定及/或無線電之單獨實體介面模組)。有線通訊可包括串列及並列有線媒體，諸如乙太網路、通用串列匯流排(USB)、Firewire、數位視訊介

面(DVI)、高清晰度多媒體介面(HDMI)等。無線通訊可包括(例如)緊密近接無線媒體(例如，諸如基於近場通訊(NFC)標準之射頻(RF)、紅外線(IR)等)、短程無線媒體(例如，藍芽、WLAN、Wi-Fi等)、遠程無線媒體(例如，蜂巢式廣域無線電通訊技術、基於衛星之通訊等)，或經由聲波之電子通訊。在一實施例中，通訊介面模組210可經組配以防止通訊模組212中處於作用中之無線通訊彼此干擾。在執行此功能時，通訊介面模組210可基於(例如)等待傳輸之訊息之相對優先權來排程通訊模組212之活動。雖然圖2中所揭示之實施例說明通訊介面模組210與通訊模組212分離，但通訊介面模組210及通訊模組212之功能性亦可能有可能併入至同一模組中。

[0024]與本發明一致，記憶體模組204可包含用戶端模組106'之至少部分。用戶端模組106'亦可能有可能包含可與載入至記憶體模組204中之可執行碼及/或資料合作的基於硬體之部分。在至少一個實施例中，用戶端模組106'可經由上文所描述之模組及/或匯流排與通訊模組212相互作用。作爲此相互作用之部分，用戶端模組106'可使得通訊模組212將資訊傳輸至遠端資源104'及/或自遠端資源104'接收資訊。將遠端資源104'揭示爲單一裝置，但其實際上可爲經組配以個別地或協調地操作以處理資料之多個裝置，諸如在雲端計算架構之情況下。遠端資源104'可包含分別對應於模組200至212之模組200'至212'，如關於用戶端裝置102'所揭示，且因此，此等兩個模組群組可經類似地組配及/或執行

類似功能性。一些差異通常可存在於用戶端裝置102'與遠端資源104'之間的組配中，其中(例如)使用者介面模組210'可爲視情況選用的以使得資料伺服器(例如，安裝於機架組配中)可能並不包含使用者介面設備且實際上可依賴於用於使用者介面功能性之遠端用戶端台。在至少一個實施例中，記憶體模組204'可包含EC 110'。EC110'可能能夠經由上文所揭示之模組及/或匯流排與通訊模組212'相互作用，且可使得通訊模組212'經由用戶端裝置102'中之通訊模組212自用戶端模組106'接收資訊及/或將資訊傳輸至用戶端模組106'。

[0025]圖3說明根據本發明之至少一個實施例的可能在用戶端模組106、SW配置器108及SW 112之間發生的實例相互作用。最初，雖然圖3中所揭示之實例相互作用可能引用與SGX技術相關聯之各種術語、結構、方法等，但與本發明一致之實施例不限於僅使用SGX之實施。本文所揭示之實施例亦可使用替代安全技術來實施。如300處所展示，用戶端模組106可使用指令(例如，SGX EREPORT指令)來判定SW 112之雜湊。可自「原始」SW 112量測雜湊，該「原始」SW 112用作SW配置器108中之「主控器」以在EC 110中產生SW 112。可由用戶端模組106或SW配置器108來執行雜湊之實際判定且接著將其傳輸至用戶端模組106。用戶端模組106可接著產生公開金鑰及私密金鑰，如302處所展示，將公開金鑰之複本及SW 112之先前所判定之雜湊置放至SWDS 114 (例如，SGX SIGSTRUCT資料結構)中，如304處

所展示。在306處，可由用戶端模組106使用私密金鑰來簽署SIGSTRUCT且接著在308處將其傳輸至SW配置器108。在310處，當產生EC 110時，SW配置器108可將SIGSTRUCT之複本置放至EC 110中。在312處，EC 110可接著基於SIGSTRUCT初始化SW 112，其中初始化可包括由用戶端模組106在314處計算置放於SIGSTRUCT中的公開金鑰之雜湊(例如，使用SGX EINIT指令)。

[0026]當主張SW 112之所有權時，用戶端模組106可使得用戶端裝置102傳輸藉由私密金鑰簽署的主張SW 112之所有權之請求，連同公開金鑰之複本，如316處所展示。在318處，SW 112且更特定而言所有權判定模組116最初可使用連同請求一起提供之公開金鑰驗證關於自用戶端模組106接收的主張所有權之請求之簽章。若簽章爲有效的，則在320處，SW 112可接著使用指令(例如，SGX EREPORT指令)來判定先前儲存於SIGSTRUCT中之公開金鑰之雜湊，可判定連同請求一起提供之公開金鑰之雜湊且可接著比較連同請求一起提供之公開金鑰之雜湊與SIGSTRUCT中的公開金鑰之先前所判定的雜湊。在至少一個實例實施中，可藉由SW 112 (例如，支援SW 112之SGX硬體)將SIGSTRUCT內的至少一個欄位中之公開金鑰之雜湊值置放至EREPORT.MRSIGNER中。可接著比較EREPORT.MRSIGNER之值與與所有權請求一起接收之公開金鑰之雜湊以判定SW 112之所有權。若判定雜湊匹配，則SW 112可接著在322處向用戶端模組106通告已驗證用戶

端模組106對SW 112之所有權。

[0027]圖4說明根據本發明之至少一個實施例的用於自用戶端裝置之角度建立安全工作空間之所有權的實例操作。實例操作400至406大體上可關於組配SW產生。最初，在操作400中，連同公開金鑰及私密金鑰一起判定受信任SW (例如，稍後將主張所有權之SW)之雜湊。可接著在操作402中將SW雜湊及公開金鑰置放至SWDS中。可在操作404中在SWDS上計算簽章(例如，利用私密金鑰)且可在操作406中傳輸經簽署SWDS (例如，傳輸至SW配置器)。實例操作408及410大體上可關於取得SW之所有權。在操作408中，可傳輸針對SW之所有權的請求(例如，傳輸至包含SW之遠端資源)。在操作410中，可接收對請求之回應。舉例而言，對請求之回應可指示驗證了請求且請求者爲SW之擁有者(例如，可能能夠存取SW)，或替代地，可能並未驗證請求且並不准許請求者存取SW。

[0028]圖5說明根據本發明之至少一個實施例的用於自遠端資源之角度建立安全工作空間之所有權的實例操作。實例操作500至504大體上可關於在遠端資源中產生SW。在操作500中，可接收SWDS (例如，在SW配置器中)。可接著在操作502中產生包括SWDS之EC。EC可接著在操作504中利用SWDS初始化SW。在至少一個實施例中，SW之初始化可包含判定包括於SWDS內之公開金鑰之雜湊。實例操作506至516大體上可關於驗證SW之所有權。在操作506中，可連同公開金鑰一起接收主張SW之所有權之請求。可簽署

請求，且在操作508中，可使用連同請求一起提供之公開金鑰驗證請求之簽章。假定能夠在操作508中驗證簽章，則在操作510中，可至少針對連同主張SW之所有權之請求一起接收的公開金鑰判定雜湊值。可接著在操作512中做出關於連同請求一起接收之公開金鑰之雜湊是否匹配在SWDS中接收的公開金鑰之雜湊的判定。若在操作中判定雜湊並不匹配，則在操作514中，可拒絕主張SW之所有權之請求。另一方面，若在操作512中判定雜湊匹配，則在操作516中，可授與主張SW之所有權之請求。在至少一個實施例中，可接著向請求者告知授與該請求且現在准許存取SW。

[0029] 雖然圖4及圖5說明根據不同實施例之操作，但應理解，並非圖4及圖5中所描繪之所有操作爲其他實施例所必要的。實際上，本文中充分預期到，在本發明之其他實施例中，圖4及圖5中所描繪之操作及/或本文所描述的其他操作可以任何圖式中未具體展示的方式組合，但仍與本發明充分一致。因此，針對一個圖式中並未準確展示之特徵及/或操作的申請專利範圍被視爲在本發明之範疇及內容內。

[0030] 如在本申請案中及在申請專利範圍中所使用，藉由術語「及/或」接合之項目之清單可意謂所列項目之任何組合。舉例而言，片語「A、B及/或C」可意謂A；B；C；A及B；A及C；B及C；或A、B及C。如在本申請案中及在申請專利範圍中所使用，藉由術語「中之至少一者」接合之項目之清單可意謂所列項目之任何組合。舉例而言，片

語「A、B或C中之至少一者」可意謂A；B；C；A及B；A及C；B及C；或A、B及C。

[0031]如本文中之任何實施例中所使用，術語「模組」可指經組配以執行前述操作中之任一者的軟體、韌體及/或電路系統。軟體可體現爲套裝軟體、程式碼、指令、指令集及/或記錄於非暫時性電腦可讀儲存媒體上之資料。韌體可體現爲程式碼、指令或指令集及/或經硬寫碼(例如，非依電性)於記憶體裝置中之資料。如本文中之任何實施例中所使用之「電路系統」可(例如)單獨或以任何組合包含固線式電路系統、諸如包含一或多個個別指令處理核心之電腦處理器的可規劃電路系統、狀態機電路系統，及/或儲存由可規劃電路系統執行之指令的韌體。該等模組可共同地或個別地體現爲形成大型系統(例如，積體電路(IC)、系統單晶片(SoC)、桌上型電腦、膝上型電腦、平板電腦、伺服器、智慧型手機等)之部分的電路系統。

[0032]本文中所描述之操作中之任一者可實施於一系統中，該系統包括一或多個儲存媒體(例如，非暫時性儲存媒體)，該一或多個儲存媒體具有個別地或組合地儲存於其上之指令，該等指令在由一或多個處理器執行時執行該等方法。因此，處理器可包括(例如)伺服器CPU、行動裝置CPU及/或其他可規劃電路系統。又，預期可跨越多個實體裝置散佈本文中所描述之操作，諸如在一個以上不同實體位置處之處理結構。儲存媒體可包括任何類型之有形媒體，例如，任何類型之磁碟，包括硬碟、軟碟、光學光碟、緊密

光碟唯讀記憶體(CD-ROM)、可重寫緊密光碟(CD-RW)及磁光碟；半導體裝置，諸如唯讀記憶體(ROM)、諸如動態及靜態隨機存取記憶體(RAM)之RAM、可抹除可規劃唯讀記憶體(EPROM)、電可抹除可規劃唯讀記憶體(EEPROM)、快閃記憶體、固態磁碟(SSD)、嵌入式多媒體卡(eMMC)、安全數位輸入/輸出(SDIO)卡、磁性或光學卡，或適合於儲存電子指令之任何類型之媒體。其他實施例可實施爲由可規劃控制裝置執行之軟體模組。

[0033]因此，本申請案係有關於建立一安全工作空間(SW)之所有權。一用戶端裝置可將一SW資料結構(SWDS)提供至一SW配置器。一SWDS可包含一原始SW及一公開金鑰之一雜湊，且可藉由對應於該公開金鑰之一私密金鑰來簽署。該SW配置器可使得產生包括使用該SWDS起始之一SW之一執行容器(EC)。該用戶端裝置可使用連同該公開金鑰之一複本一起傳輸之一請求(藉由該私密金鑰簽署)主張SW所有權。可藉由一所有權判定模組來判定SW所有權，該所有權判定模組使用與該請求一起接收之該公開金鑰驗證該請求之簽章，判定該所接收公開金鑰之一雜湊且比較該所接收公開金鑰之該雜湊與該SWDS中的該公開金鑰之一雜湊。

[0034]以下實例關於其他實施例。本發明之以下實例可包含諸如以下各者之標的物：裝置、方法、用於儲存指令之至少一個機器可讀媒體(該等指令在經執行時使得一機器基於方法執行動作)、用於基於方法執行動作之構件及/

或用於建立安全工作空間之所有權之系統，如下文所提供。

[0035]根據實例1，提供至少一個裝置。該至少一個裝置可包含：一通訊模組，其與至少一用戶端裝置相互作用；一安全工作空間配置器，其自該用戶端裝置接收一安全工作空間資料結構且使得將一安全工作空間包括於由遠端資源產生之一執行容器內，該安全工作空間係基於該安全工作空間資料結構。

[0036]實例2可包括如實例1之元件，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在藉由對應於該公開金鑰之一私密金鑰簽署之一訊息中接收。

[0037]實例3可包括如實例2之元件，其中關於該安全工作空間之該資料包含自該安全工作空間量測之一雜湊值。

[0038]實例4可包括如實例2至3中任一項之元件，其中該執行容器進一步基於該安全工作空間資料結構初始化該安全工作空間，該安全工作空間之初始化包括量測該安全工作空間資料結構中之該公開金鑰之一雜湊值。

[0039]實例5可包括如實例4之元件，其中該安全工作空間進一步包含一所有權判定模組，該所有權判定模組經由該通訊模組自該用戶端裝置接收包括取得該安全工作空間之所有權之至少一請求的一經簽署訊息及該公開金鑰，且至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權。

[0040] 實例6可包括如實例5之元件，其中用以判定該用戶端裝置是否經授權而取得該安全工作空間之所有權的該所有權判定模組包含用以進行以下操作之該所有權判定模組：利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章，藉由量測該公開金鑰判定與該經簽署訊息一起接收的該公開金鑰之一雜湊值，藉由比較與該經簽署訊息一起接收的該公開金鑰之該雜湊與在初始化該安全工作空間時判定的該公開金鑰之該雜湊驗證該安全工作空間之所有權，且在與該經簽署訊息一起接收之該公開金鑰之該雜湊匹配在初始化該安全工作空間時判定的該公開金鑰之該雜湊的情況下，將該安全工作空間之所有權授與該用戶端裝置。

[0041] 實例7可包括如實例6之元件，其中比較與該經簽署訊息一起接收之該公開金鑰之該雜湊與在初始化該安全工作空間時判定的該公開金鑰之該雜湊包含將自一軟體防護擴展(SGX) SIGSTRUCT資料結構內之一欄位讀取的一雜湊值置放至一SGX EREPORT.MRSIGNER資料結構中，及比較該EREPORT.MRSIGNER之值與與該經簽署訊息一起接收之該公開金鑰之該雜湊。

[0042] 實例8可包括如實例1至7中任一項之元件，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

[0043] 實例9可包括如實例1至8中任一項之元件，其中

該安全工作空間資料結構包含自該安全工作空間量測之一雜湊值及一公開金鑰，該安全工作空間資料結構係在藉由對應於該公開金鑰之一私密金鑰簽署之一訊息中接收。

[0044]實例10可包括如實例1至9中任一項之元件，其中該至少一個裝置爲經組配以在一雲端計算架構中操作之至少一個伺服器。

[0045]實例11可包括如實例1至10中任一項之元件，其中該執行容器包含一虛擬機。

[0046]根據實例12，提供一種用戶端裝置。該用戶端裝置可包含：一通訊模組，其與至少一遠端資源相互作用；及一用戶端模組，其藉由量測待用於產生新安全工作空間之一安全工作空間之一原始版本而判定該安全工作空間之一雜湊值，產生一公開金鑰及一對應私密金鑰，將至少該雜湊值及該公開金鑰置放至一安全工作空間資料結構中，及將該安全工作空間資料結構傳輸至該遠端資源。

[0047]實例13可包括如實例12之元件，其中該安全工作空間之該雜湊值係自該遠端資源中之一安全工作空間配置器接收。

[0048]實例14可包括如實例12至13中任一項之元件，其中該用戶端模組進一步產生包含取得一安全工作空間之所有權之一請求的一訊息，藉由該私密金鑰簽署該訊息，及將該經簽署訊息及該公開金鑰傳輸至該遠端資源。

[0049]實例15可包括如實例12至14中任一項之元件，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安

全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

[0050]根據實例16，提供一種用於建立一安全工作空間之所有權之方法。該方法可包含在一安全工作空間配置器處自一用戶端裝置接收一安全工作空間資料結構，該安全工作空間配置器常駐於一遠端資源中且使得將一安全工作空間包括於藉由該遠端資源產生之一執行容器內，該安全工作空間係基於該安全工作空間資料結構。

[0051]實例17可包括如實例16之元件，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在藉由對應於該公開金鑰之一私密金鑰簽署之一訊息中接收。

[0052]實例18可包括如實例16至17中任一項之元件，其中關於該安全工作空間之該資料包含自該安全工作空間量測之一雜湊值。

[0053]實例19可包括如實例18之元件，且更進一步包含基於該安全工作空間資料結構初始化該安全工作空間，其中初始化該安全工作空間包括量測該安全工作空間資料結構中之該公開金鑰之一雜湊值。

[0054]實例20可包括如實例19之元件，且更進一步包含自該用戶端裝置接收包括取得該安全工作空間之所有權之至少一請求的一經簽署訊息及該公開金鑰，及至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權。

[0055]實例21可包括如實例20之元件，其中判定該用戶端裝置是否經授權而取得該安全工作空間之所有權可包含利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章，藉由量測該公開金鑰判定與該經簽署訊息一起接收之該公開金鑰之一雜湊值，藉由比較與該經簽署訊息一起接收之該公開金鑰之該雜湊與在初始化該安全工作空間時判定的該公開金鑰之雜湊檢驗該安全工作空間之所有權，及在與該經簽署訊息一起接收之該公開金鑰之該雜湊匹配在初始化該安全工作空間時判定的該公開金鑰之該雜湊的情況下，將該安全工作空間之所有權授與該用戶端裝置。

[0056]實例22可包括如實例21之元件，其中比較與該經簽署訊息一起接收之該公開金鑰之該雜湊與在初始化該安全工作空間時判定的該公開金鑰之該雜湊包含將自一軟體防護擴展(SGX) SIGSTRUCT資料結構內之一欄位讀取的一雜湊值置放至一SGX EREPORT.MRSIGNER資料結構中，及比較該EREPORT.MRSIGNER之值與與該經簽署訊息一起接收之該公開金鑰之該雜湊。

[0057]實例23可包括如實例16至22中任一項之元件，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

[0058]實例24可包括如實例16至23中任一項之元件，其中該安全工作空間資料結構包含自該安全工作空間量測之

一雜湊值及一公開金鑰，該安全工作空間資料結構係在藉由對應於該公開金鑰之一私密金鑰簽署之一訊息中接收。

[0059]實例25可包括如實例16至24中任一項之元件，其中該遠端資源包含經組配以在一雲端計算架構中操作之至少一個伺服器。

[0060]實例26可包括如實例16至25中任一項之元件，其中該執行容器包含一虛擬機。

[0061]根據實例27，提供一種用於主張一安全工作空間之所有權之方法。該方法可包含藉由量測待用於產生新安全工作空間之一安全工作空間之一原始版本判定一遠端資源中的該安全工作空間之一雜湊值，產生一公開金鑰及一對應私密金鑰，將至少該雜湊值及該公開金鑰置放至一安全工作空間資料結構中，及將該安全工作空間資料結構傳輸至該遠端資源。

[0062]實例28可包括如實例27之元件，其中該安全工作空間之該雜湊值係自該遠端資源中之一安全工作空間配置器接收。

[0063]實例29可包括如實例27至28中任一項之元件，且可進一步包含產生包含取得一安全工作空間之所有權之一請求的一訊息，藉由該私密金鑰簽署該訊息，及將該經簽署訊息及該公開金鑰傳輸至該遠端資源。

[0064]實例30可包括如實例27至29中任一項之元件，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT

資料結構。

[0065]根據實例31，提供一種包括至少一裝置及一遠端資源之系統，該系統經配置以執行如上述實例16至30中任一項之方法。

[0066]根據實例32，提供一種經配置以執行如上述實例16至30中任一項之方法的晶片組。

[0067]根據實例33，提供至少一個機器可讀媒體，其包含多個指令，該等多個指令回應於在一計算裝置上執行而使得該計算裝置執行如上述實例16至30中任一項之方法。

[0068]根據實例34，提供一種經組配以用於建立一安全工作空間之所有權之裝置，該裝置經配置以執行如上述實例16至30中任一項之方法。

[0069]根據實例35，提供一種用於建立一安全工作空間之所有權之系統。該系統可包含用於在一安全工作空間配置器處自一用戶端裝置接收一安全工作空間資料結構之構件，該安全工作空間配置器常駐於一遠端資源中，及用於使得將一安全工作空間包括於藉由該遠端資源產生之一執行容器內的構件，該安全工作空間係基於該安全工作空間資料結構。

[0070]實例36可包括如實例35之元件，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在藉由對應於該公開金鑰之一私密金鑰簽署之一訊息中接收。

[0071]實例37可包括如實例36之元件，其中關於該安全

工作空間之該資料包含自該安全工作空間量測之一雜湊值。

[0072]實例38可包括如實例36至37中任一項之元件，且可進一步包含用於基於該安全工作空間資料結構初始化該安全工作空間之構件，其中初始化該安全工作空間包括量測該安全工作空間資料結構中之該公開金鑰之一雜湊值。

[0073]實例39可包括如實例38之元件，且可進一步包含用於自該用戶端裝置接收包括取得該安全工作空間之所有權之至少一請求的一經簽署訊息及該公開金鑰的構件，及用於至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權的構件。

[0074]實例40可包括如實例39之元件，其中用於判定該用戶端裝置是否經授權而取得該安全工作空間之所有權的該構件包含用於進行以下操作的構件：利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章，藉由量測該公開金鑰判定與該經簽署訊息一起接收的該公開金鑰之一雜湊值，藉由比較與該經簽署訊息一起接收之該公開金鑰之該雜湊與在初始化該安全工作空間時判定的該公開金鑰之雜湊驗證該安全工作空間之所有權，及在與該經簽署訊息一起接收之該公開金鑰之該雜湊匹配在初始化該安全工作空間時判定的該公開金鑰之該雜湊的情況下，將該安全工作空間之所有權授與該用戶端裝置。

[0075]實例41可包括如實例36至40中任一項之元件，其

中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

[0076]根據實例42，提供一種用於主張一安全工作空間之所有權之系統。該系統可包含用於藉由量測待用於產生新安全工作空間之一安全工作空間之一原始版本而判定一遠端資源中的該安全工作空間之一雜湊值的構件、用於產生一公開金鑰及一對應私密金鑰之構件，用於將至少該雜湊值及該公開金鑰置放至一安全工作空間資料結構中之構件，及用於將該安全工作空間資料結構傳輸至該遠端資源之構件。

[0077]實例43可包括如實例42之元件，其中該安全工作空間之該雜湊值係自該遠端資源中之一安全工作空間配置器接收。

[0078]實例44可包括如實例42至43中任一項之元件，且可進一步包含用於產生包含取得一安全工作空間之所有權之一請求的一訊息的構件、用於藉由該私密金鑰簽署該訊息之構件，及用於將該經簽署訊息及該公開金鑰傳輸至該遠端資源之構件。

[0079]實例45可包括如實例42至44中任一項之元件，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

[0080]已在本文中使用之術語及表達用作描述而非限

制之術語，且在使用此等術語及表達時並不意欲排除所展示及描述之特徵的任何等效物(或其部分)，且應認識到，在申請專利範圍之範疇內，各種修改爲可能的。因此，申請專利範圍意欲涵蓋所有此等等效物。

【符號說明】

100...系統

102、102'...用戶端裝置

104、104'...遠端資源

106、106'...用戶端模組

108...SW配置器

110、110'...EC

112...SW

114...SWDS

116...所有權判定模組

200、200'...系統模組

202、202'...處理模組

204、204'...記憶體模組

206、206'...電力模組

208、208'、210'...使用者介面模組

210...通訊介面模組

212、212'...通訊模組

400、402、404、406、408、410、500、502、504、506、508、510、512、514、516...實例操作

申請專利範圍

1. 一種包括至少一個裝置之裝置，其包含：

一通訊模組，其用以與至少一用戶端裝置相互作用；以及

一安全工作空間配置器，其用以：

自該用戶端裝置接收一安全工作空間資料結構；及

使一安全工作空間被包括在由遠端資源所產生之一執行容器內，該安全工作空間係基於該安全工作空間資料結構。

2. 如請求項1之至少一個裝置，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在用對應於該公開金鑰之一私密金鑰簽署的一訊息中接收。

3. 如請求項2之至少一個裝置，其中關於該安全工作空間之該資料包含自該安全工作空間量測之一雜湊值。

4. 如請求項2之至少一個裝置，其中該執行容器進一步基於該安全工作空間資料結構初始化該安全工作空間，該安全工作空間之初始化包括量測該安全工作空間資料結構中的該公開金鑰之一雜湊值。

5. 如請求項4之至少一個裝置，其中該安全工作空間進一步包含一所有權判定模組以：

經由該通訊模組自該用戶端裝置接收包括取得該

安全工作空間之所有權之至少一請求及該公開金鑰的一簽署訊息；以及

至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權。

6. 如請求項5之至少一個裝置，其中係用以判定該用戶端裝置是否經授權而取得包含該所有權判定模組的該安全工作空間之所有權的該所有權判定模組係用以：

利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章；

藉由量測該公開金鑰判定與該經簽署訊息一起接收之該公開金鑰之一雜湊值；

藉由比較與該經簽署訊息一起接收之該公開金鑰之雜湊與在初始化該安全工作空間時判定的該公開金鑰之雜湊驗證該安全工作空間之所有權；以及

如果與該經簽署訊息一起接收之該公開金鑰之雜湊與初始化該安全工作空間時判定的該公開金鑰之雜湊匹配，則將該安全工作空間之所有權授與該用戶端裝置。

7. 如請求項1之至少一個裝置，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

8. 一種用戶端裝置，其包含：

一通訊模組，其與至少一遠端資源相互作用；以及

一用戶端模組，其用以：

藉由量測要被用於產生新安全工作空間之該安全工作空間之一原始版本判定該安全工作空間之一雜湊值；

產生一公開金鑰及一對應私密金鑰；

將至少該雜湊值及該公開金鑰置放至一安全工作空間資料結構中；以及

將該安全工作空間資料結構傳輸至該遠端資源。

9. 如請求項8之用戶端裝置，其中該安全工作空間之該雜湊值係自該遠端資源中之一安全工作空間配置器所接收。

10. 如請求項8之用戶端裝置，其中該用戶端模組係進一步用以：

產生包含取得一安全工作空間之所有權之一請求的一訊息；

以該私密金鑰簽署該訊息；以及

將經簽署之該訊息及該公開金鑰傳輸至該遠端資源。

11. 如請求項8之用戶端裝置，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

12. 一種用於建立一安全工作空間之所有權之方法，其包含：

自一用戶端裝置在一安全工作空間配置器接收一安全工作空間資料結構，該安全工作空間配置器常駐於一遠端資源中；以及

致使一安全工作空間用以被包括在由該遠端資源所產生之一執行容器內，該安全工作空間係基於該安全工作空間資料結構。

13. 如請求項12之方法，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在以對應於該公開金鑰之一私密金鑰所簽署的一訊息中被接收。

14. 如請求項13之方法，其中關於該安全工作空間之該資料包含自該安全工作空間所量測之一雜湊值。

15. 如請求項13之方法，其進一步包含：

基於該安全工作空間資料結構初始化該安全工作空間，其中初始化該安全工作空間包括量測該安全工作空間資料結構中的該公開金鑰之一雜湊值。

16. 如請求項15之方法，其進一步包含：

自該用戶端裝置接收包括取得該安全工作空間之所有權之至少一請求及該公開金鑰的一經簽署訊息；以及

至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權。

17. 如請求項16之方法，其中判定該用戶端裝置是否經授權

而取得該安全工作空間之所有權包含：

利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章；

藉由量測該公開金鑰判定與該經簽署訊息一起接收之該公開金鑰之一雜湊值；

藉由比較與該經簽署訊息一起接收之該公開金鑰之雜湊與在初始化該安全工作空間時判定的該公開金鑰之雜湊驗證該安全工作空間之所有權；以及

如果與該經簽署訊息一起接收之該公開金鑰之雜湊與初始化該安全工作空間時判定的該公開金鑰之雜湊匹配，則將該安全工作空間之所有權授與該用戶端裝置。

18. 如請求項11之方法，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

19. 一種具有個別地或組合地儲存於其上的指令之至少一個機器可讀取儲存媒體，用於建立一安全工作空間之所有權的該等指令在由一或多個處理器所執行時，致使該一或多個處理器：

自一用戶端裝置在一安全工作空間配置器接收一安全工作空間資料結構，該安全工作空間配置器常駐於一遠端資源中；以及

致使一安全工作空間用以被包括在由該遠端資源所產生之一執行容器內，該安全工作空間係基於該安全

工作空間資料結構。

20. 如請求項19之媒體，其中該安全工作空間資料結構包含關於該安全工作空間之資料及一公開金鑰，該安全工作空間資料結構係在以對應於該公開金鑰之一私密金鑰所簽署的一訊息中被接收。

21. 如請求項20之媒體，其中關於該安全工作空間之該資料包含自該安全工作空間所量測之一雜湊值。

22. 如請求項20之媒體，其進一步包含指令，該等指令在由一或多個處理器所執行時，致使該一或多個處理器：

基於該安全工作空間資料結構初始化該安全工作空間，其中初始化該安全工作空間包括量測該安全工作空間資料結構中的該公開金鑰之一雜湊值。

23. 如請求項22之媒體，其進一步包含指令，該等指令在由一或多個處理器所執行時，致使該一或多個處理器：

自該用戶端裝置接收包括取得該安全工作空間之所有權之至少一請求及該公開金鑰的一簽署訊息；以及

至少基於該經簽署訊息及該安全工作空間資料結構判定該用戶端裝置是否經授權而取得該安全工作空間之所有權。

24. 如請求項23之媒體，其中用於判定該用戶端裝置是否經授權而取得該安全工作空間之所有權的該等指令包含致使該一或多個處理器用以進行以下操作之指令：

利用與該經簽署訊息一起接收之該公開金鑰驗證該經簽署訊息之簽章；

藉由量測該公開金鑰判定與該經簽署訊息一起接收之該公開金鑰之一雜湊值；

藉由比較與該經簽署訊息一起接收之該公開金鑰之雜湊與在初始化該安全工作空間時判定的該公開金鑰之雜湊驗證該安全工作空間之所有權；以及

如果與該經簽署訊息一起接收之該公開金鑰之雜湊與初始化該安全工作空間時判定的該公開金鑰之雜湊匹配，則將該安全工作空間之所有權授與該用戶端器件。

25. 如請求項19之媒體，其中該安全工作空間爲基於軟體防護擴展(SGX)技術之一安全區域且該安全工作空間資料結構爲一SGX SIGSTRUCT資料結構。

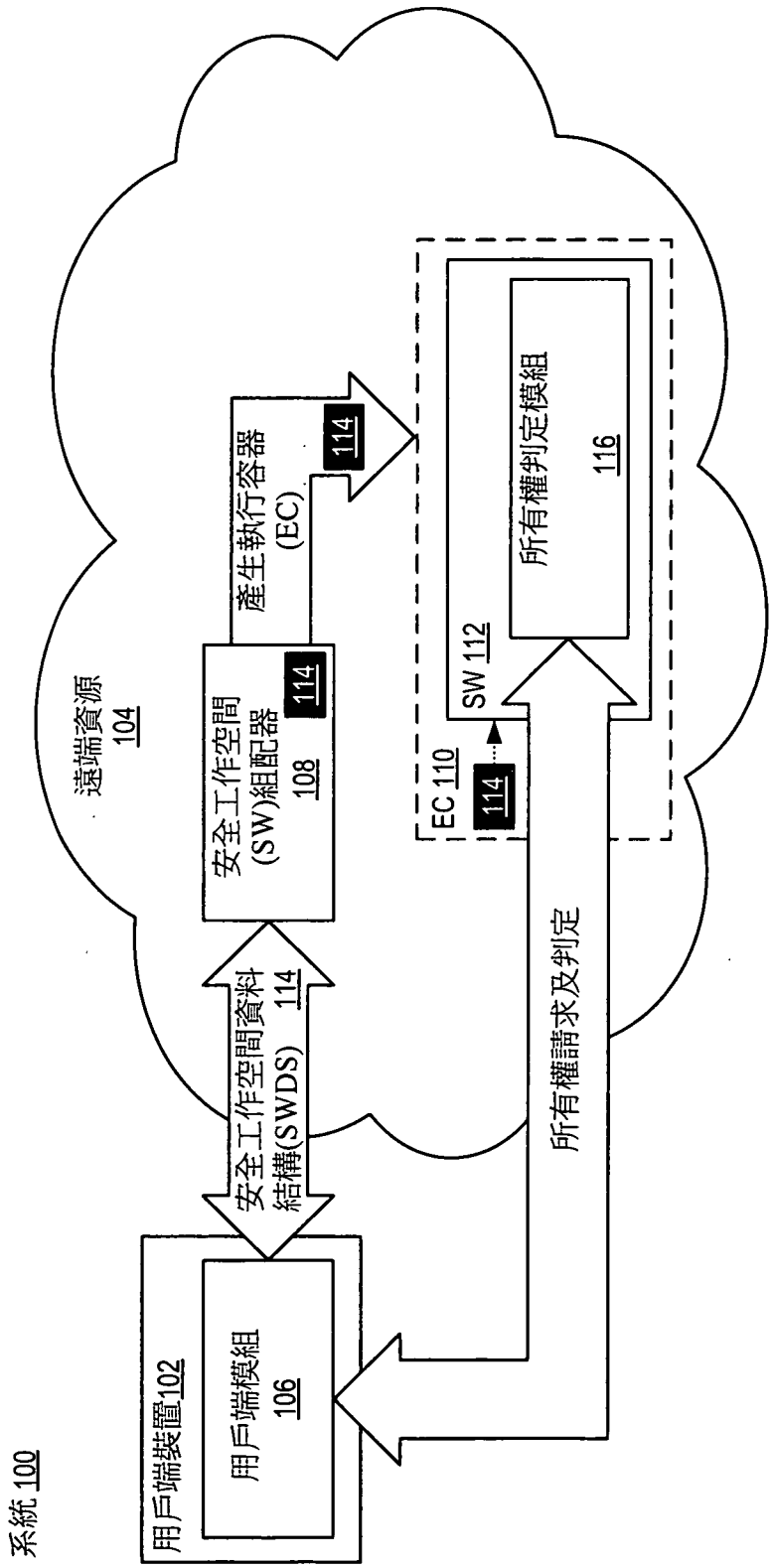
系統 100
用戶端裝置102
用戶端模組
106
安全工作空間資料
結構(SWDS) 114
遠端資源
104
安全工作空間
(SW)組配器
108
114
產生執行容器
(EC)
114
EC 110
114
SW 112
所有權判定模組
116
所有權請求及判定

圖1

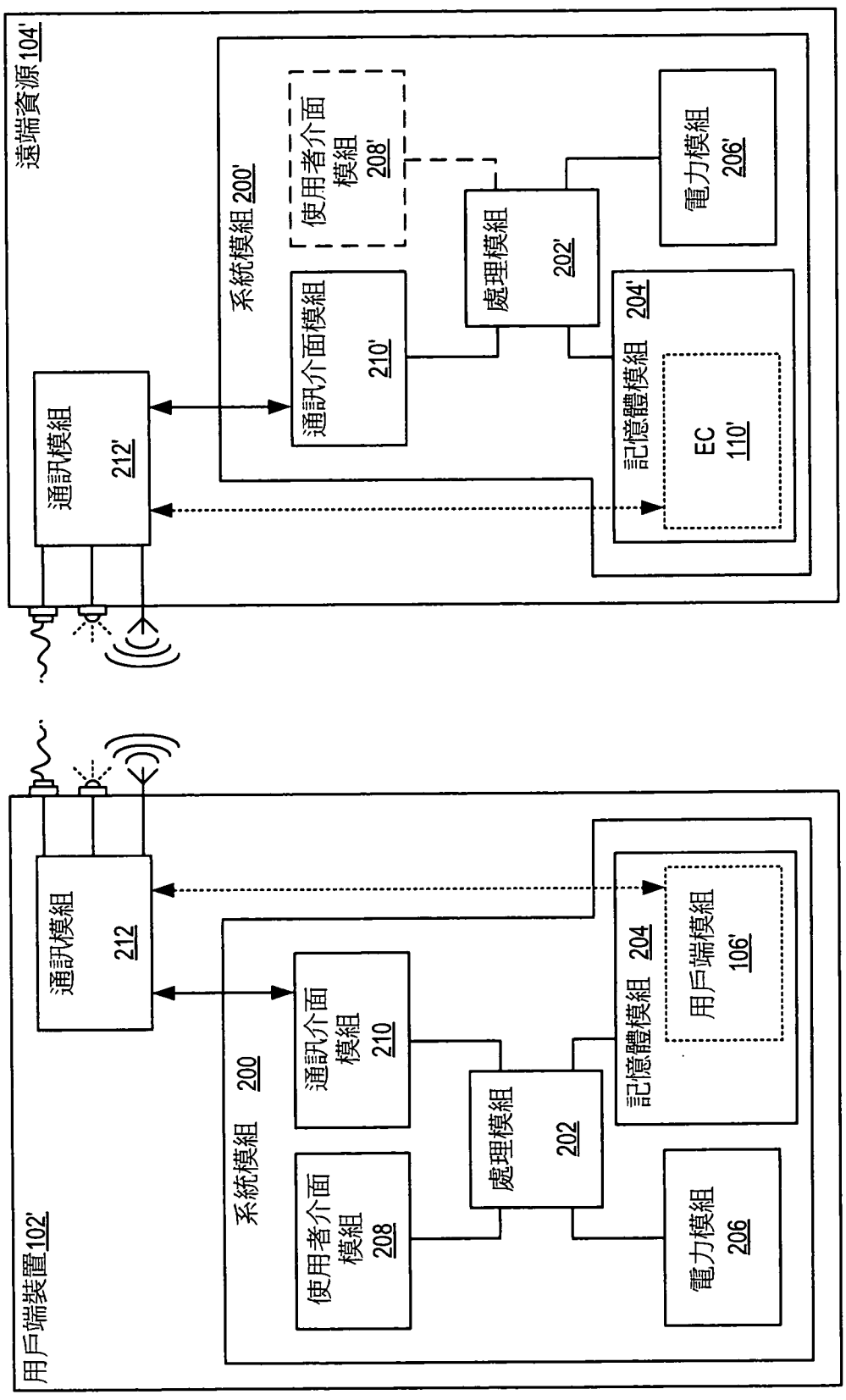
遠端資源 104'
系統模組 200'
通訊介面模組 210'
使用者介面模組 208'
處理模組 202'
記憶體模組 204'
EC 110'
電力模組 206'
通訊模組 212'
用戶端裝置 102'
系統模組 200
通訊介面模組 210
使用者介面模組 208
處理模組 202
記憶體模組 204
用戶端模組 106'
電力模組 206
通訊模組 212

圖2

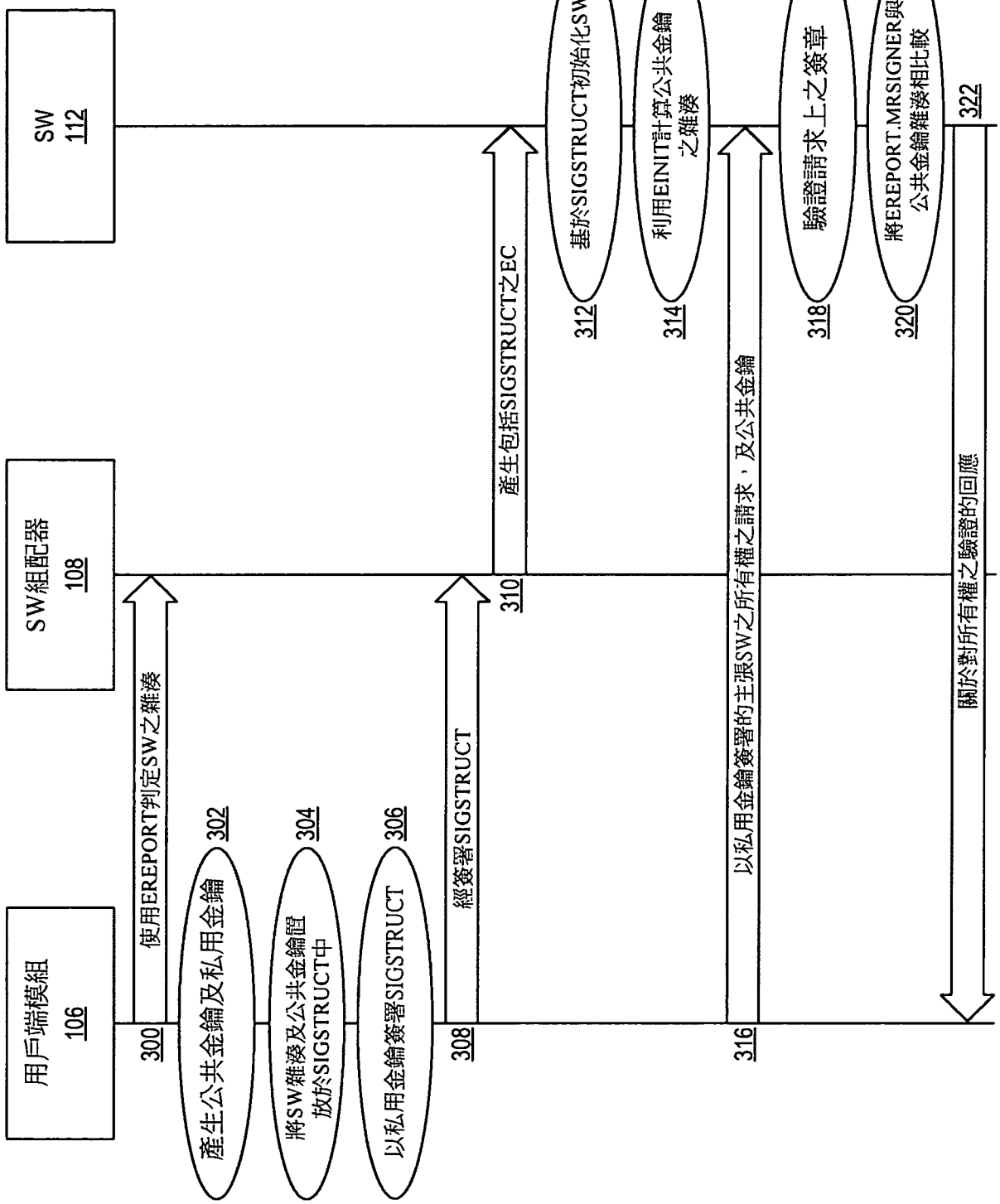
用戶端模組
106
SW組配器
108
SW
112
300
使用EREPORT判定SW之雜湊
302
產生公共金鑰及私用金鑰
304
將SW雜湊及公共金鑰置
放於SIGSTRUCT中
306
以私用金鑰簽署SIGSTRUCT
308
經簽署SIGSTRUCT
310
產生包括SIGSTRUCT之EC
312
基於SIGSTRUCT初始化SW
314
利用EINIT計算公共金鑰
之雜湊
316
以私用金鑰簽署的主張SW之所有權之請求，及公共金鑰
318
驗證請求上之簽章
320
將EREPORT.MRSIGNER與
公共金鑰雜湊相比較
322
關於對所有權之驗證的回應

圖3

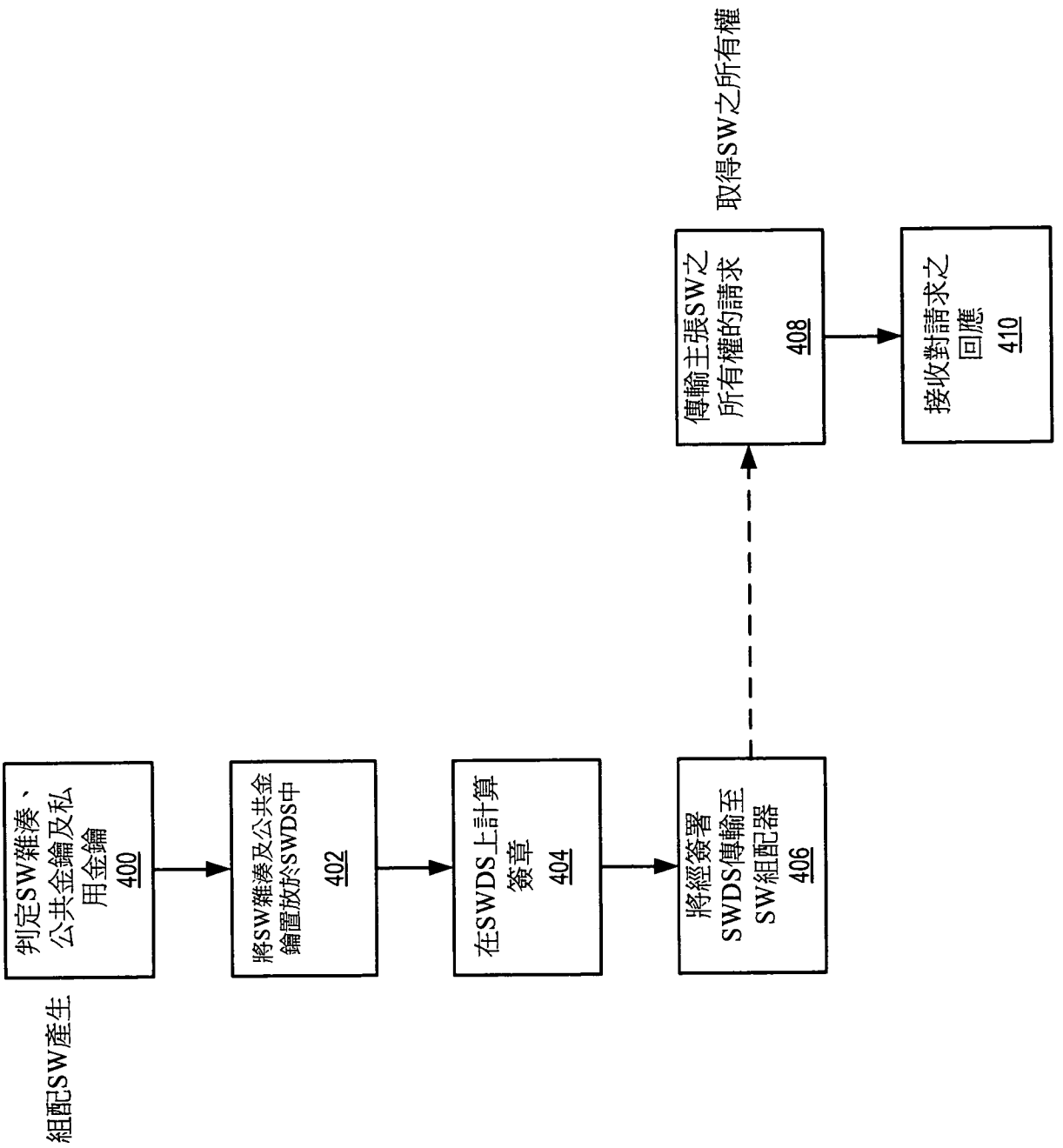
組配SW產生
判定SW雜湊、公共金鑰及私用金鑰 400
將SW雜湊及公共金鑰置放於SWDS中 402
在SWDS上計算簽章 404
將經簽署SWDS傳輸至SW組配器 406
傳輸主張SW之所有權的請求 408
取得SW之所有權
接收對請求之回應 410

圖4

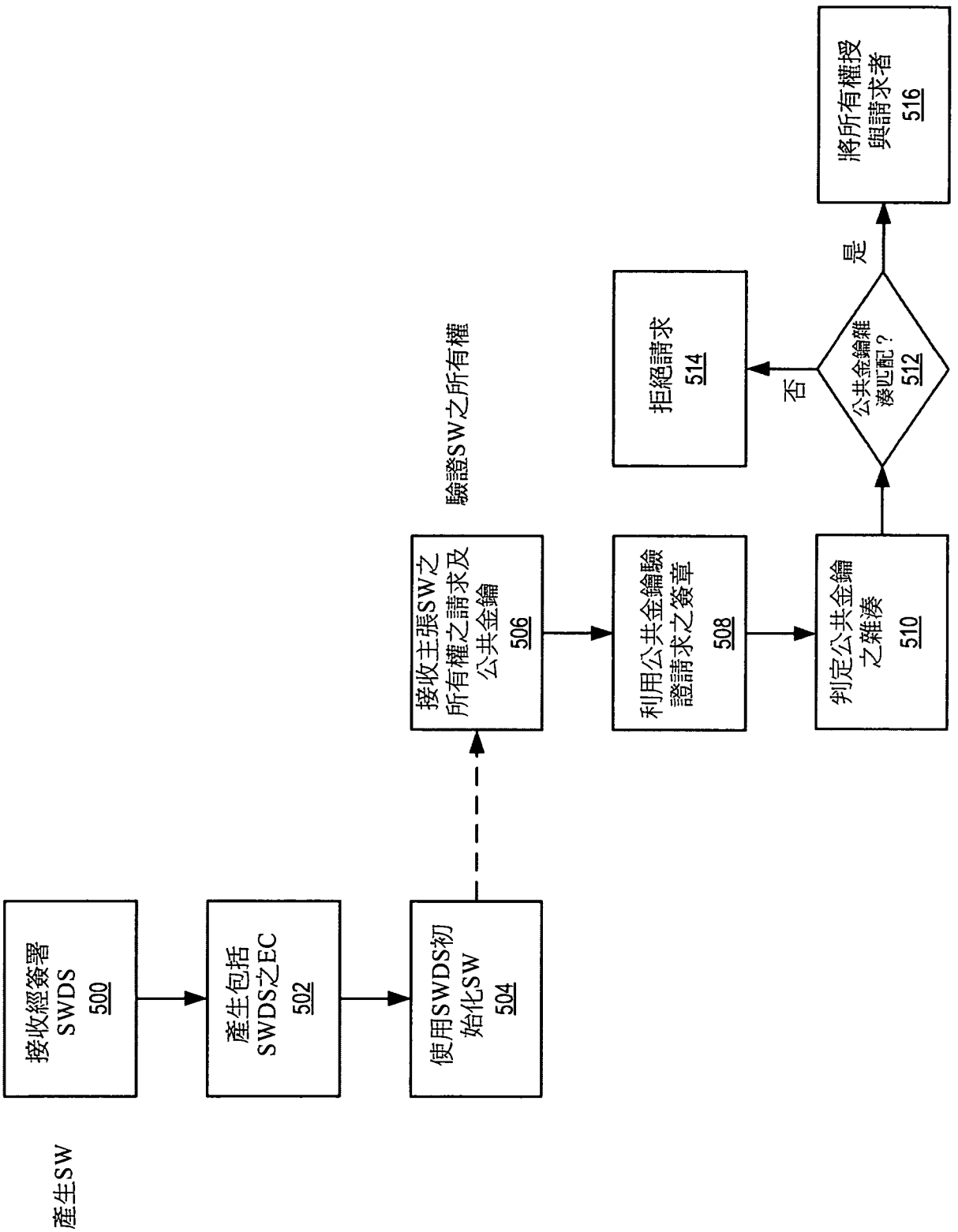
產生SW
接收經簽署SWDS 500
產生包括SWDS之EC 502
使用SWDS初始化SW 504
驗證SW之所有權
接收主張SW之所有權之請求及公共金鑰 506
利用公共金鑰驗證請求之簽章 508
判定公共金鑰之雜湊 510
公共金鑰雜湊匹配？ 512
否
拒絕請求 514
是
將所有權授與請求者 516

圖5