I575403

(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 I575403 B**

(45)公告日： 中華民國 106 (2017) 年 03 月 21 日

(21)申請案號：102127658 (22)申請日： 中華民國 102 (2013) 年 08 月 01 日

(51)Int. Cl.： *G06F21/78 (2013.01)* *G06F21/60 (2013.01)*

(30)優先權：2012/08/01 歐洲專利局 12178889.7

(71)申請人：瑟卡內安全網路公司 (德國) SECUNET SECURITY NETWORKS AKTIENGESELLSCHAFT (DE)
德國

(72)發明人：瓦潘史密特 亞閔 WAPPENSCHMIDT, ARMIN (DE)

(74)代理人：陳長文

(56)參考文獻：

TW	201028854A	US	7565547B2
US	2003/0060234A1	US	2007/0016804A1
US	2009/0140040A1		

審查人員：彭智煇

申請專利範圍項數：13 項 圖式數：2 共 15 頁

(54)名稱

用於得到對一服務之安全存取之方法

METHOD OF GAINING SECURE ACCESS TO A SERVICE

(57)摘要

本發明揭示一種在一所定義可信任環境中得到對一服務之安全存取之方法。至少一個網路組件在該所定義可信任環境中，且將一密碼保存於該網路組件中。將一使用者裝置引入至該可信任環境中，且該使用者裝置連絡該網路組件且擷取保存於該網路組件中之該密碼。該使用者裝置將該密碼傳遞至該服務，且若儲存於該服務中之一密碼匹配已由該使用者裝置傳遞至該服務之該密碼，則針對該使用者裝置啟用該服務。

A method of gaining secure access to a service in a defined trustworthy environment. At least one network component is in the defined trustworthy environment, and a password is saved in the network component. A user device is introduced into the trustworthy environment, and the user device contacts the network component and retrieves the password that is saved in the network component. The user device communicates the password to the service, and the service is enabled for the user device if a password stored in the service matches the password that has been communicated by the user device to the service.

指定代表圖：

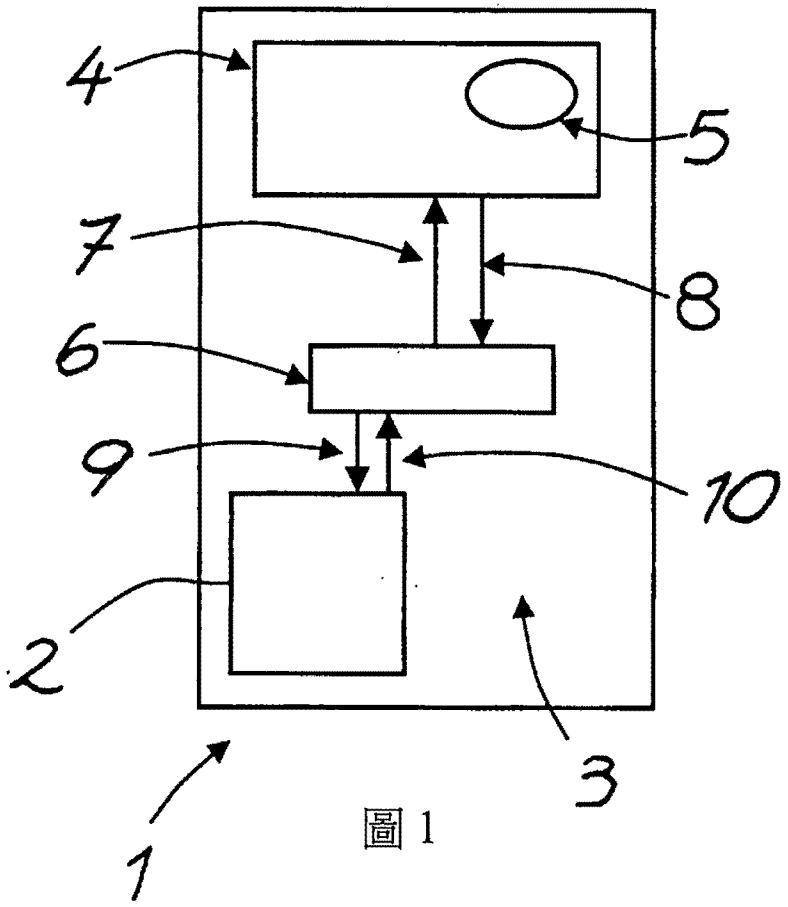

圖 1

符號簡單說明：

1・・・系統

2・・・網路附接儲存伺服器/服務

3・・・所定義可信任環境/可信任環境

4・・・網路組件

5・・・感測器

6・・・使用者裝置

7・・・箭頭/請求/密碼請求

8・・・箭頭

9・・・箭頭

10・・・箭頭

發明摘要

公告本

※ 申請案號：101127658

※ 申請日：102.8.1　　※IPC 分類：G06F 21/38 (2013.01)
21/60 (2013.01)

【發明名稱】

用於得到對一服務之安全存取之方法

METHOD OF GAINING SECURE ACCESS TO A SERVICE

【中文】

本發明揭示一種在一所定義可信任環境中得到對一服務之安全存取之方法。至少一個網路組件在該所定義可信任環境中，且將一密碼保存於該網路組件中。將一使用者裝置引入至該可信任環境中，且該使用者裝置連絡該網路組件且擷取保存於該網路組件中之該密碼。該使用者裝置將該密碼傳遞至該服務，且若儲存於該服務中之一密碼匹配已由該使用者裝置傳遞至該服務之該密碼，則針對該使用者裝置啓用該服務。

【英文】

A method of gaining secure access to a service in a defined trustworthy environment. At least one network component is in the defined trustworthy environment, and a password is saved in the network component. A user device is introduced into the trustworthy environment, and the user device contacts the network component and retrieves the password that is saved in the network component. The user device communicates the password to the service, and the service is enabled for the user device if a password stored in the service matches the password that has been communicated by the user device to the service.

【代表圖】

【本案指定代表圖】：第（1）圖。

【本代表圖之符號簡單說明】：

1 系統

2 網路附接儲存伺服器/服務

3 所定義可信任環境/可信任環境

4 網路組件

5 感測器

6 使用者裝置

7 箭頭/請求/密碼請求

8 箭頭

9 箭頭

10 箭頭

【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】

用於得到對一服務之安全存取之方法

METHOD OF GAINING SECURE ACCESS TO A SERVICE

本發明係關於一種在一所定義可信任環境中得到對一服務之安全存取之方法。

上文所闡述之類型之方法在實務上眾所周知。安全相關要求通常指示，在存取特定服務或經加密資料之前必須啓用服務或必須解密經加密資料。特定而言，每當在一所定義可信任環境之外操作此等裝置時保護特定服務或資料係必要的。可通常在一可信任環境中省略封鎖或加密資料，此乃因對服務或資料之存取唯由可信任經授權實體或使用者實現。在此情形中在實務上已知之方法中固有的缺點係，若在可信任環境之外存取服務或在可信任環境之外使用資料，則服務或資料將不被保護之事實。因此，在實務上用以避免此問題情形之方法係採用可藉由其保護服務或資料免受未經授權使用之一密碼。然而，在一特定週期之在使用服務或存取資料上之不活動之後，必須再輸入密碼，且此意指服務或資料之利用在某種程度上係對使用者較不友好的。

因此，本發明之目的係提供一種由易用性而亦由一高安全位準表徵之上文所闡述之類型之方法。本發明之另一目的係提供一對應系統。

爲了達成此目的，本發明教示一種在一所定義可信任環境中得到對一服務之安全存取之方法，其中

至少一個網路組件在該所定義可信任環境中，

將一密碼保存於該網路組件中，其中將一使用者裝置整合至該可信任環境中，

該使用者裝置連絡該網路組件且擷取保存於該網路組件中之該密碼，

該使用者裝置將該密碼傳遞至該服務，且

若儲存於該服務中之一密碼匹配已由該使用者裝置傳遞至該服務之該密碼，則針對該使用者裝置啓用該服務。

在本發明之範疇內，安全存取指代保護對該服務之存取免受由一未經授權實體達成之事實。舉例而言，該服務係一網際網路服務，較佳地，一網頁郵件服務。可能以較佳地在一本端裝置(舉例而言，一電腦(PC))上對一使用者帳戶之存取之形式在可信任環境中提供服務。在一項實施例中，該服務係一大容量儲存媒體，舉例而言，包含一較佳地經加密檔案系統之一檔案伺服器及/或一網路附接儲存伺服器(NAS伺服器)。每當針對該使用者裝置啓用安全存取時，較佳地解密該經加密檔案系統以使用該大容量儲存媒體。每當在該可信任環境之外使用該大容量儲存媒體時，有利地加密該大容量儲存媒體之該檔案系統。藉由建議之方式，該可信任環境係(較佳地)藉由一路由器與公用網際網路分離之一網路。可能藉由一電腦單元(電腦)提供網路。

建議基於含有至少一個資料組之一參考資料組定義該可信任環境，該至少一個資料組由由以下項組成之群組構成：位置資料(GPS資料)、LAN資料、藍芽資料、網路位址、GSM無線資料、氣象資料。本發明之範疇內之位置資料指代可信任環境之座標或空間範圍。本發明之範疇內之LAN資料(區域網路資料)指代在可信任環境中之至少一個組件且較佳地複數個或所有組件。在原則上LAN可能包括一無線網路(無線LAN、WLAN)或者呈一無線網路或WLAN之形式。在一項實施例中，LAN資料包括整合於WLAN中之組件之可接收外部

WLAN信號及/或信號強度及/或網路識別符。可接收外部WLAN信號包括可在可信任環境內接收且不各自構成係可信任環境之一部分之任何組件之來自網路之信號。本發明之範疇內之信號強度指代可由外部WLAN接收之信號及/或指代可由來自可信任環境之組件接收之信號。本發明之範疇內之網路位址包含在可信任環境中之組件之位址。舉例而言，本發明之範疇內之GMS資料指代可由GSM無線小區存取之位於可信任環境中之一支援GSM裝置之識別碼。舉例而言，氣象資料係當前溫度及/或一過去溫度曲線。藍芽資料包括在可信任環境中之至少一個支援藍芽之裝置之連絡資料。

爲了將網路組件定位於可信任環境中，較佳地比較定義可信任環境之資料組與由網路組件供應之一整合資料組且僅在參考資料組與整合資料組之間的一所規定最大偏差下降至低於一特定位準情況下才將該等網路組件專有地整合於可信任環境中。該整合資料組包括至少一個資料組，該資料組選自由以下項組成之群組：位置資料(GPS資料)、LAN資料、藍芽資料、網路位址、GSM無線資料、氣象資料。在一尤佳方法中，該整合資料組中所含有之該資料組亦係該參考資料組之一構成部分。該最大偏差係較佳地經規定或可規定的，藉此允許調整根據本發明之方法之安全位準。隨著可允許之偏差變得較高，安全位準相應地變得較低。根據本發明之方法之安全位準隨著該參考資料組與該整合資料組之間的可允許之偏差變得較小而增大。若由該網路組件供應之該整合資料組與該參考資料組係相同的，則該網路組件較佳地在可信任環境中或整合至可信任環境中。在一項實施例中，若該整合資料組不匹配該參考資料組，或超過該整合資料組與該參考資料組之間的一所規定偏差，則將該網路組件視爲係一外部網路組件，或不將其視爲屬於該可信任環境。在此情形中，該網路組件不是該可信任環境之一構成部分。該網路組件有利地具有至少一個感測器，該

感測器可偵測或判定該整合資料組-較佳地，該整合資料組中所含有之該等資料組或該整合資料組中所含有之該資料組。在一項實施例中，該感測器係一GPS感測器。

爲了將該使用者裝置引入至該可信任環境中，建議比較定義該可信任環境之參考資料組與自該使用者裝置所偵測之項目資料，且僅在該參考資料組與該項目資料之間的一所規定最大偏差下降至低於一特定值之情況下才將該使用者裝置視爲專屬於該可信任環境。該項目資料尤佳地匹配該參考資料組。自該使用者裝置所偵測之該項目資料包括該參考資料組中所含有之至少一個資料組。舉例而言，該項目資料包含選自由以下項組成之群組之至少一個資料組：位置資料(GPS資料)、LAN資料、藍芽資料、網路位址、GSM無線資料、氣象資料。建議該使用者裝置具有可偵測或判定該項目資料之至少一個感測器單元。該感測器單元有利地係一GPS感測器。一經證實方法係將定義該可信任環境之資料組儲存於該網路組件及/或該使用者裝置中。在一尤佳態樣中，該網路組件使用保存於該網路組件中以前瞻性地判定是否該網路組件屬於該可信任環境之該整合資料組及該參考資料。

在一尤佳態樣中，每當該使用者裝置位於該可信任環境之外時該網路組件拒絕允許該使用者裝置擷取儲存於該網路組件中之密碼。僅當已將該使用者裝置引入至或整合至該可信任環境中時，該網路組件才有利地對來自該使用者裝置之一密碼請求做出響應。有利地，無密碼保存於該使用者裝置中。舉例而言，每當該使用者裝置位於該可信任環境之外時，需要該使用者輸入該密碼以便使用該使用者裝置來獲得對該可信任環境及/或對該服務之安全存取。根據本發明，若該網路組件位於該可信任環境之外，則該網路組件拒絕允許該使用者裝置擷取儲存於該網路組件中之該密碼。每當由該網路組件判定之該整合資料組超出與該參考資料組之一所規定偏差時，該網路組件拒絕揭

示該密碼。

已發現若至少兩個且較佳地複數個網路組件在該可信任環境中、該密碼之一各別部分儲存於可信任環境中之至少兩個網路組件中之每一者中係有利的。該密碼之一部分較佳地保存於該可信任環境之每一網路組件中。保存於該等個別網路組件中之該密碼之各部分有利地彼此不同。該密碼之至少兩個部分可能係同樣的且視情況該密碼之所有部分可能係同樣的或相同的。該網路組件之位址可能用作該密碼。對該服務之存取可藉助該密碼進行。在一項實施例中，藉由較佳地用作解密密鑰之密碼實現檔案系統之解密。

該使用者裝置有利地自其中儲存該密碼之各部分之彼等網路組件擷取該密碼之該等部分。建議組合由該使用者裝置擷取之該密碼之該等部分以在該使用者裝置中形成該密碼。在一尤佳實施例中，該密碼不保存於或僅暫時保存於該使用者裝置中。欲連絡之網路組件或各網路組件之位址較佳地儲存於該使用者裝置中，自該網路組件擷取該密碼或自該網路組件擷取該密碼之各部分。根據本發明，一旦已將該使用者裝置有利地引入至該可信任環境中或至該服務中，便藉由該使用者裝置前瞻性地實現該密碼或該密碼之該等部分之擷取。若尚未將該使用者裝置引入至該可信任環境中及/或若其中儲存該密碼之部分之一網路組件不在該可信任環境中，則根據本發明不可藉由該使用者裝置前瞻性地建立對該服務之存取。在本發明之範疇內，前瞻性地意指就一密碼之擷取而言該使用者裝置自動地連絡該可信任環境中之該網路組件及/或該可信任環境中之該等網路組件以便擷取儲存於該網路組件中之該密碼或儲存於該等個別網路組件中之該密碼之該等部分。該使用者裝置僅在該使用者裝置在該可信任環境中之情況下才可能前瞻性地實現該密碼之一擷取。建議該網路組件或該等網路組件各自前瞻性地或獨立地判定是否其屬於該可信任環境。

另外，本發明教示一種用於達成本發明之目的之系統，可藉由該系統在一所定義可信任環境中安全地存取一服務，其中該所定義可信任環境包括至少一個網路組件，一密碼保存於該網路組件中，其中一使用者裝置可引入至或整合至該可信任環境中，其中在整合於該可信任環境中之該使用者裝置與該網路組件之間實現一通信，其中可由整合至該可信任環境中之該使用者裝置擷取保存於該網路組件中之該密碼，其中該使用者裝置將該密碼傳遞至該服務，且其中若儲存於該服務中之一密碼匹配由該使用者裝置傳遞之該密碼，則針對該使用者裝置啓用該服務。

建議該可信任環境較佳地係一私人網路。在本發明之範疇內，私人網路指代一私人住所及/或一電腦中心中之一公司網路及/或一網路。建議該網路組件係一被動網路組件。舉例而言，該網路組件係一DSL切換器、一過濾器、一放大器或諸如此類。特定而言，在本發明之範疇內，被動網路組件指代此網路組件不產生任何資料或信號之事實。

該網路組件可能係一主動網路組件。該主動網路組件係選自由以下項組成之群組之至少一個組件：伺服器、NAS伺服器、藍芽裝置、印表機、大容量儲存構件。該使用者裝置有利地係一支援網路之裝置。在一項實施例中，該使用者裝置選自由以下項組成之群組：可攜式電腦(筆記型電腦)、行動電話、智慧電話、平板PC。

已發現密碼含有該可信任環境中之一網路組件之一網路位址及/或一網路位址之一部分係有利的。此方法確保在其中必須儲存該密碼之該網路組件或該等網路組件中不需要額外記憶體。密碼可能由整合至該可信任環境中之該等個別網路組件之該等網路位址或由該等網路位址之各部分構成。

本發明係基於根據本發明之方法及根據本發明之系統由一驚人

易用性及高使用者友好度表徵之理念。藉由根據本發明之方法將頻繁輸入一密碼以啓用對一服務之存取限制於其中該使用者裝置不在一可信任環境中之情形。根據本發明之方法使得每當該使用者裝置位於該可信任環境中時可能在不危及安全之情況下消除對輸入一密碼之需要。由於啓用對該服務之存取之個別組件儲存於該可信任環境中之事實，可將該使用者裝置設計爲不具有任何特別安全之記憶體。由於一未經授權第三方不知曉關於在何處且如何在根據本發明之方法中或在根據本發明之系統中獲得密碼，因此對該服務之未經授權存取係不可能的或僅藉由昂貴構件係可能的。因此，根據本發明之方法由一高安全位準及驚人易用性表徵。

以下論述基於僅繪示一項所圖解說明之實施例之一圖式詳細闡述本發明。

圖1展示其中呈一NAS伺服器(網路附接儲存伺服器) 2形式之一服務在一所定義可信任環境3中之一系統1。如圖1中所指示，一網路組件4在可信任環境3中。網路組件4各自具有一感測器5，該感測器可判定與儲存於網路組件4中之一參考資料組進行比較之整合資料。此處，感測器5判定網路組件4之一位置且比較所獲得位置資料與參考資料組中所含有之位置資料。此處且在圖1及圖2中，由感測器5獲得之位置資料及儲存於參考資料組中之位置資料匹配，結果係網路組件4判定其屬於可信任環境3中且整合至可信任環境3中。

此外，圖1亦展示已將一使用者裝置6引入至可信任環境3中，且較佳地且在圖1中使用者裝置6藉由所進行之使用由使用者裝置6判定之項目資料與儲存於使用者裝置6中之參考資料組之一比較判定其屬於可信任環境3中。在圖1中之實施例中，使用者裝置6判定其係可信任環境3之一構成部分。整合至可信任環境3中之使用者裝置現在可將一密碼請求發送至網路組件4。

箭頭7指示使用者裝置6正在將該密碼請求發送至網路組件4以擷取儲存於網路組件4中之一密碼。由於網路組件4與使用者裝置6兩者皆在可信任環境3中，因此網路組件4藉由將儲存於網路組件4中之一密碼發送至使用者裝置6而對請求7做出響應，如由箭頭8所圖解說明。使用自網路組件4獲得之密碼，使用者裝置6如由箭頭9所展示登入至NAS伺服器2。

此處，若如圖1中所圖解說明儲存於NAS伺服器2之檔案系統中之密碼匹配由使用者裝置6傳遞至NAS伺服器2之密碼，則NAS伺服器2解密儲存於NAS伺服器2之未圖解說明之檔案系統中之檔案。箭頭10表示NAS伺服器2與使用者裝置6之間的資料傳送。

圖2展示使用者裝置6在可信任環境3之外。使用者裝置6比較由使用者裝置6判定之項目資料與儲存於使用者裝置6中之參考資料組且在如此做時發現無匹配。由於圖2中之使用者裝置6在可信任環境3之外，因此密碼請求7之結果係裝置不能到達可信任環境3中之網路組件4。因此，使用者裝置6不可能藉助於密碼請求7來請求存取NAS伺服器2所需之密碼。圖2圖解說明在藉由使用者裝置6之一失敗之前瞻性密碼請求之後不可能實現對NAS伺服器2之存取。圖2未圖解說明可藉由在使用者裝置6中人工輸入一密碼建立對NAS伺服器2之存取。

【圖式簡單說明】

圖1展示其中一使用者裝置在一可信任環境中之用於實施根據本發明之方法之根據本發明之一系統；且

圖2展示其中使用者裝置在可信任環境之外之用於實施根據本發明之方法之根據本發明之一系統。

【符號說明】

1　系統

2　網路附接儲存伺服器/服務

3	所定義可信任環境/可信任環境
4	網路組件
5	感測器
6	使用者裝置
7	箭頭/請求/密碼請求
8	箭頭
9	箭頭
10	箭頭

第 102127658 號專利申請案
中文申請專利範圍替換本(105 年 1 月 25 日)
年 月 日修正本

申請專利範圍

1. 一種在容納至少一個網路組件(4)之一所定義可信任環境(3)中得到對一服務(2)之安全存取之方法，其特徵在於，

基於一參考資料組而定義該可信任環境(3)，且

該參考資料組含有選自由以下各項所組成之群組中之至少一個資料組：LAN資料、藍芽資料及網路位址，

將一密碼保存於該網路組件(4)及該服務(2)中，

將一使用者裝置(6)引入至該可信任環境(3)中，其中

比較定義該可信任環境(3)之該參考資料組與來自該使用者裝置(6)之項目資料以便將該使用者裝置(6)引入至該可信任環境(3)中，且

僅在該參考資料組與該項目資料之間的一所規定最大偏差下降至低於一特定值之情況下，將該使用者裝置(6)視為專屬於該可信任環境(3)，

該使用者裝置(6)連絡該網路組件(4)，

該使用者裝置(6)擷取保存於該網路組件(4)中之該密碼，

該使用者裝置(6)將該密碼傳遞至該服務(2)，且

若儲存於該服務(2)中之一密碼匹配已由該使用者裝置(6)傳遞至該服務(2)之該密碼，則針對該使用者裝置(6)啟用該服務(2)。

2. 如請求項1之方法，其中比較定義該可信任環境(3)之該參考資料組與由該網路組件(4)供應之整合資料以便將該網路組件(4)定位於該可信任環境(3)中，且僅在該參考資料組與該整合資料之間的一所規定最大偏差下降至低於一特定值之情況下將該網路組件(4)視為屬於該可信任環境(3)。

3. 如請求項1或2之方法，其中若該使用者裝置(6)位於該可信任環

境(3)之外，則該網路組件(4)拒絕允許該使用者裝置(6)擷取儲存於該網路組件(4)中之該密碼。

4. 如請求項1或2之方法，其中若該網路組件(4)位於該可信任環境之外，則該網路組件(4)拒絕允許該使用者裝置(6)擷取儲存於該網路組件(4)中之該密碼。

5. 如請求項1或2之方法，其中至少兩個且較佳地複數個網路組件在該可信任環境(3)中，該密碼之一部分儲存於該可信任環境(3)之該至少兩個網路組件(4)中之每一者中。

6. 如請求項5之方法，其中該使用者裝置(6)自其中儲存該密碼之該等部分之該等網路組件(4)擷取該密碼之各別部分。

7. 如請求項6之方法，其中組合由該使用者裝置(6)擷取之該密碼之該等部分以在該使用者裝置(6)中形成該密碼。

8. 一種用於實施如請求項1至7中任一項之方法之系統，可藉由該系統在一所定義可信任環境(3)中安全地存取一服務(2)，其中

該所定義可信任環境(3)包含至少一個網路組件(4)，其特徵在於，

基於一參考資料組而定義該可信任環境(3)，且

該參考資料組含有選自由以下各項所組成之群組中之至少一個資料組：位置資料(GPS資料)、LAN資料、藍芽資料、網路位址、GSM無線資料、氣象資料，

將一密碼保存於該網路組件(4)及該服務(2)中，

可將一使用者裝置(6)引入至或整合至該可信任環境(3)中，其中

比較定義該可信任環境(3)之該參考資料組與來自該使用者裝置(6)之項目資料以便將該使用者裝置(6)引入至該可信任環境(3)中，且

僅在該參考資料組與該項目資料之間的一所規定最大偏差下降至低於一特定值之情況下，將該使用者裝置(6)視為專屬於該可信任環境(3)，

在整合至該可信任環境(3)中之該使用者裝置(6)與該網路組件(4)之間實現一通信，

可由整合至可信任環境(3)中之該使用者裝置(6)擷取保存於該網路組件(4)中之該密碼，

該使用者裝置(6)將該密碼傳遞至該服務(2)，且

若儲存於該服務(2)中之一密碼匹配已由該使用者裝置(6)傳遞之該密碼，則針對該使用者裝置(6)啟用該服務(2)。

9. 如請求項8之系統，其中該可信任環境(3)較佳地係一私人網路。

10. 如請求項8或9之系統，其中該網路組件(4)係一被動網路組件。

11. 如請求項8或9之系統，其中該網路組件(4)係一主動網路組件。

12. 如請求項8或9之系統，其中該使用者裝置(6)係一支援網路之裝置。

13. 如請求項8或9之系統，其中該密碼含有在該可信任環境(3)中之一網路組件之一位址。

圖式

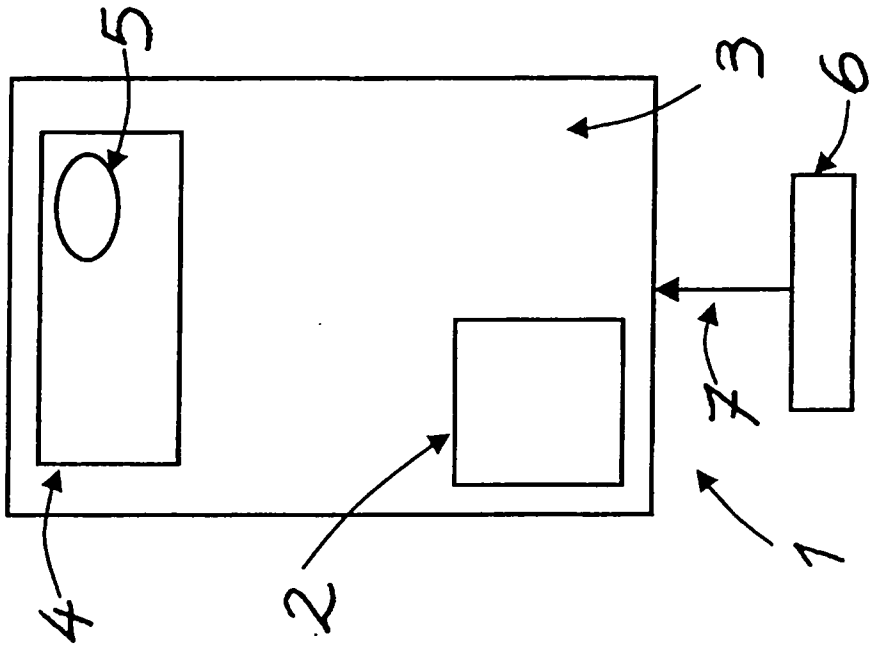

圖 2

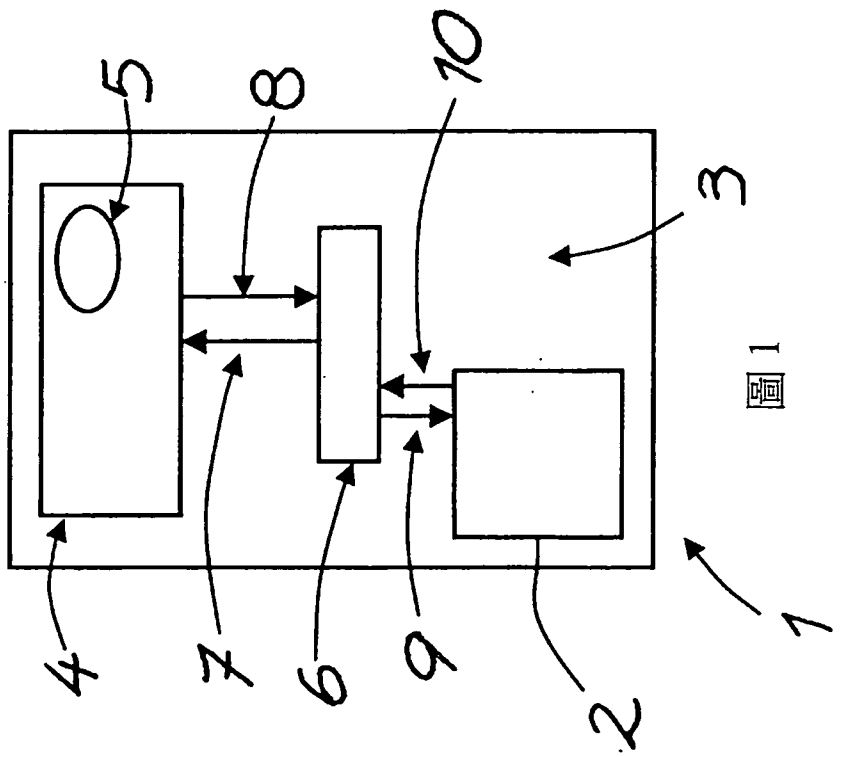

圖 1