I827906

(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 I827906 B**

(45)公告日： 中華民國 113 (2024) 年 01 月 01 日

(21)申請案號：110103418 (22)申請日： 中華民國 110 (2021) 年 01 月 29 日

(51)Int. Cl.： ***H04L9/30*** ***(2006.01)*** ***H04L9/32*** ***(2006.01)***

G06F21/31 ***(2013.01)***

(71)申請人：銓安智慧科技股份有限公司 (中華民國) INFOKEYVAULT TECHNOLOGY CO., LTD. (TW)

臺北市文山區羅斯福路六段 218 號 4 樓

(72)發明人：劉許源 LIOU HSU, YUAN (TW) ；郭子昂 KUO, TZU-ANG (TW) ；林志宏 LIN, CHIHHUNG (TW)

(74)代理人：楊代強

(56)參考文獻：

TW	201902177A	CN	101807997B
US	7783884B2	US	2015/0358158A1

審查人員：許人偉

申請專利範圍項數：16 項 圖式數：6 共 42 頁

(54)名稱

訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組

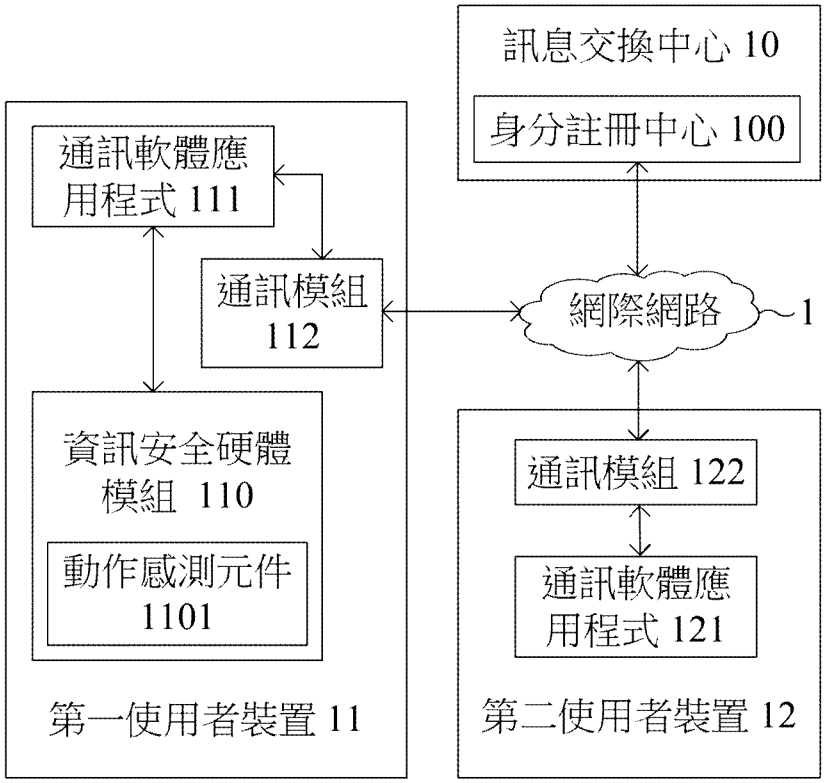
(57)摘要

本發明係有關於一種訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組，訊息傳輸系統包含：一訊息交換中心、一第一使用者裝置以及一第二使用者裝置。該資訊安全硬體模組安裝至第一使用者裝置的殼體中，該資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一公鑰-私鑰對之一第一密鑰建立組合，該第一公鑰-私鑰對中之該第一私鑰僅儲存於該資訊安全硬體模組中，而該第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心。該第二使用者裝置產生一共享密鑰，並運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文，然後傳送給該訊息交換中心後再傳送至該第一使用者裝置。收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。

The invention relates to a message transmitting system and a user device and a hardware security module for use therein. The message transmitting system includes: a message exchange center, a first user device and a second user device. The hardware security module is installed in the housing of the first user device, and the hardware security module generates a first key establishment combination including at least a first public-private key pair according to a key establishment algorithm. The first private key in the first public-private key pair is only stored in the hardware security module, and the first public key in the first public-private key pair is sent to the message exchange center, the second user device generates a shared key, and the shared key is used to encrypt a first message plaintext to obtain a first message ciphertext, which is sent to the message exchange center and then sent to the first user device. The first user device that received the first message ciphertext obtains the shared key through a shared key acquisition method, and uses the shared key to decrypt the first message ciphertext to get back the first message plaintext.

TW I827906 B

指定代表圖：



【圖 1】

符號簡單說明：

1:網際網路

10:訊息交換中心

100:身分註冊中心

11:第一使用者裝置

12:第二使用者裝置

111、121:通訊軟體應用程式

112、122:通訊模組

110:資訊安全硬體模組

1101:動作感測元件

公告本

I827906

【發明摘要】

【中文發明名稱】訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組

【英文發明名稱】Message transmitting system, user device and hardware security module for use therein

【中文】本發明係有關於一種訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組，訊息傳輸系統包含：一訊息交換中心、一第一使用者裝置以及一第二使用者裝置。該資訊安全硬體模組安裝至第一使用者裝置的殼體中，該資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一公鑰-私鑰對之一第一密鑰建立組合，該第一公鑰-私鑰對中之該第一私鑰僅儲存於該資訊安全硬體模組中，而該第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心。該第二使用者裝置產生一共享密鑰，並運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文，然後傳送給該訊息交換中心後再傳送至該第一使用者裝置。收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。

【英文】

The invention relates to a message transmitting system and a user device and a hardware security module for use therein. The message transmitting system includes: a message exchange center, a first user device and a second user device.

The hardware security module is installed in the housing of the first user device, and the hardware security module generates a first key establishment combination including at least a first public-private key pair according to a key establishment algorithm. The first private key in the first public-private key pair is only stored in the hardware security module, and the first public key in the first public-private key pair is sent to the message exchange center, the second user device generates a shared key, and the shared key is used to encrypt a first message plaintext to obtain a first message ciphertext, which is sent to the message exchange center and then sent to the first user device. The first user device that received the first message ciphertext obtains the shared key through a shared key acquisition method, and uses the shared key to decrypt the first message ciphertext to get back the first message plaintext.

【指定代表圖】　　圖1

【代表圖之符號簡單說明】

1：網際網路

10：訊息交換中心

100：身分註冊中心

11：第一使用者裝置

12：第二使用者裝置

111、121：通訊軟體應用程式

112、122：通訊模組

110：資訊安全硬體模組

1101：動作感測元件

【發明說明書】

【中文發明名稱】 訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組

【英文發明名稱】Message transmitting system, user device and hardware security module for use therein

【技術領域】

【0001】 本案係為一種訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組，尤指應用於行動通訊網路的訊息傳輸系統以及應用其中之使用者裝置與資訊安全硬體模組。

【先前技術】

【0002】 隨著行動通訊系統的不斷進展，資料傳輸頻寬大幅增加，使用者幾乎已改用即時通訊軟體進行語音交談以及文字訊息與圖片資料的傳輸。但以目前主流的即時通訊軟體的架構可以看出，使用者互相傳送的文字訊息與圖片資料必然通過一訊息交換中心來進行轉傳，而且文字訊息與圖片資料的備份會被儲存在業者所設置的資料伺服器中達一段時間甚至完全不會刪除。

【0003】 隨著使用者對於即時通訊軟體的大量使用以及對於資訊安全的高度要求，不想被公開的隱私實際卻被儲存在雲端，這種傳統的即時通訊軟體已無法滿足使用者對於資料保密的需求，因此，如Signal、Telegram等各式的私密即時

通訊軟體便應運而生。此等私密即時通訊軟體傳送的訊息會被加密後再送出，即使傳輸過程中被攔截或是從雲端資料庫中被竊取也無法被有效解讀，其中Signal還強調不會將任何文字訊息與圖片資料儲存在業者的資料伺服器中，不想被公開的隱私也就不會有被儲存在雲端的問題。

【0004】 但是，私密即時通訊軟體加密所需的密鑰(keys)，在現今的技術中都是由使用者裝置的中央處理器(CPU)所生成，生成後之密鑰(keys)被儲存在使用者裝置中所規劃的特定資料儲存區域中。因此，一旦使用者裝置被外來者駭入而取得使用者裝置核心(例如是運行其上的作業系統)的主導權時，存放在由使用者裝置的作業系統所管理的特定資料儲存區域中的密鑰(keys)，將會被輕易取得而使加密後的訊息內容會被輕易解讀，形成資訊安全上的漏洞。而如何改善此一問題，提供更佳的資訊安全方案，係為發展本案之主要目的。

【發明內容】

【0005】 本發明係有關於一種訊息傳輸系統，其包含：一訊息交換中心；一第一使用者裝置，信號連接至該訊息交換中心，該第一使用者裝置中安裝有一第一資訊安全硬體模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第一資訊安全硬體模組中，而該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心；以及一第二使用者裝置，信號連接至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一

訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文。

【0006】 本案之另一方面係為一種訊息傳輸系統，其包含：一第一使用者裝置，信號連接至網際網路，該第一使用者裝置中安裝有一第一資訊安全硬體模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第一資訊安全硬體模組中；以及一第二使用者裝置，信號連接至網際網路，當該第二使用者裝置對該第一使用者裝置發起一訊息傳輸動作時，該第二使用者裝置直接將其網路位址發給第一使用者裝置而建立一點對點的連線，該第二使用者裝置產生一共享密鑰，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文，該第二使用者裝置利用已建立之點對點的連線，將該第一訊息密文傳送至該第一使用者裝置，而收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文。

【0007】 本案之再一方面係為一種第一使用者裝置，其應用於一訊息交換中心與一第二使用者裝置之間，該第一使用者裝置包含：一通訊模組，信號連接至該訊息交換中心；以及一第一資訊安全硬體模組，信號連接至該通訊模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該

第一私鑰僅儲存於該第一資訊安全硬體模組中，而該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文。

【0008】 根據上述構想，本案所述之該第二使用者裝置依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對之一第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二使用者裝置中，而該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，該第二使用者裝置至少運用該第一使用者之第一公鑰及第二使用者之第一私鑰來進行密鑰建立而產生該共享密鑰，而該共享密鑰獲取手段則是該第一使用者自該訊息交換中心取得該第二使用者之第一公鑰，並使該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立而得出該共享密鑰。

【0009】 根據上述構想，本案所述之該訊息交換中心中包含一身分註冊中心而且該第二使用者裝置中安裝有一第二資訊安全硬體模組，該第二資訊安全硬體模組依據該密鑰建立演算法生成該第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二資訊安全硬體模組中，該第一使用者

之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第一使用者裝置屬於該第一使用者，同樣地，該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第二使用者裝置屬於該第二使用者，該第一資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第一使用者裝置中或該第二資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第二使用者裝置中。

【0010】 根據上述構想，本案所述之該第二使用者裝置自該身分註冊中心取得第一使用者之第一公鑰，運用至少包含該第一使用者之第一公鑰及第二使用者之第一私鑰，進行密鑰建立而獲得一共享秘密，然後再基於該共享秘密衍生出該共享密鑰，該第一使用者裝置，自身分註冊中心取得第二使用者之第一公鑰，並利用該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立並獲得該共享秘密並儲存於該第一資訊安全硬體模組中，該第一資訊安全硬體模組基於該共享秘密衍生出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。

【0011】 根據上述構想，本案所述之該第一使用者裝置進行完身份註冊後便對應產生一第一數位簽章，該第一數位簽章使用該第一使用者之該第一私鑰或一第二私鑰進行簽章，簽章的訊息是與該第一使用者裝置的相關公開資訊，然後該第一使用者裝置將該第一數位簽章傳送至該訊息交換中心，該第二使用者裝置自訊息交換中心拿到該第一數位簽章後，使用該第一使用者裝置的相關公開資訊進行驗章，若通過才接著使用至少包含第二使用者之第一私鑰、第一使用者之第一公鑰進行密鑰建立。

【0012】根據上述構想，本案所述之該第一資訊安全硬體模組更提供一身份認證功能，該第一使用者裝置通過該身份認證程序後，才能驅動該第一資訊安全硬體模組提供該第一私鑰來將該第一訊息密文解密而還原出該第一訊息。

【0013】根據上述構想，本案所述之該身份認證功能為手動輸入一密碼、一生物特徵或兩者的組合，該第一資訊安全硬體模組驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置通過該身份認證程序。

【0014】根據上述構想，本案所述之該第一資訊安全硬體模組中包含一動作感測元件，用以偵測手動輸入該密碼或該生物特徵時對該第一使用者裝置所產生之震動，進而判斷出為使用者是否以手動方式輸入，當該動作感測元件未能偵測到震動時則判斷為不合法輸入。

【0015】根據上述構想，本案所述之該第一使用者裝置於成功收到該第一訊息密文後，便發出一確認信號給該訊息交換中心，該訊息交換中心於收到該確認信號後，便將該第一訊息密文刪除。

【0016】根據上述構想，本案所述之該第一資訊安全硬體模組包含一安全晶片，該安全晶片生成一主密鑰，該主密鑰用以加密該第一使用者之第一私鑰而產生一加密結果，該加密結果被傳出該安全晶片外，只留下該主密鑰存在該安全晶片內並將該加密結果刪除，當需要該第一使用者之第一私鑰時，再將該加密結果傳回該安全晶片，使用該安全晶片內部之該主密鑰解密而得回該第一使用者之第一私鑰，而該安全晶片生成該主密鑰之方式包含下列中之一：亂數生成該主密鑰、選用在該安全晶片中所儲存之一固定值以及將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出。

【0017】根據上述構想，本案所述之該第二使用者裝置生成該共享密鑰之方式包含下列中之一：亂數生成該共享密鑰、選用在該第二使用者裝置中所儲存之一固定值為該共享密鑰以及將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出該共享密鑰，而該共享密鑰獲取手段則包含下列步驟：該第二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，運用該第一使用者之第一公鑰對該共享密鑰進行加密而形成一加密後之共享密鑰，然後將該加密後之共享密鑰傳送給該第一使用者裝置，該第一使用者裝置利用該第一資訊安全硬體模組中所儲存之該第一使用者之第一私鑰來對該加密後之共享密鑰進行解密，進而得回該共享密鑰。

【0018】本案之又一方面係為一種資訊安全硬體模組，安裝至一第一使用者裝置的殼體中，該第一使用者裝置、一第二使用者裝置皆信號連接至一訊息交換中心構成一訊息傳輸系統，該資訊安全硬體模組電性連接至該第一使用者裝置，該資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一公鑰-私鑰對之一第一密鑰建立組合，該第一公鑰-私鑰對中之該第一私鑰僅儲存於該資訊安全硬體模組中，而該第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。

【0019】 為了能對本發明之上述構想有更清楚的理解，下文特舉出多個實施例，並配合對應圖式詳細說明如下。

【圖式簡單說明】

【0020】 圖1，其係本案所發展出來關於一種訊息傳輸系統的較佳實施例功能方塊示意圖。

圖2，其係本案所發展出來關於訊息傳輸系統中之加解密方法流程圖。

圖3，其係本案所發展出來執行在點對點多媒體加密通訊上之實施例方法流程圖。

圖4a與圖4b，其係本案中資訊安全硬體模組的兩種實施例示意圖。

圖5，其係本案所發展出來關於訊息傳輸系統中之另一加解密方法之實施例流程圖。

圖6，其係本案所發展出來關於訊息傳輸系統中之加解密方法的又一較佳實施例方法流程圖。

【實施方式】

【0021】 請參見圖1，其係本案所發展出來關於一種訊息傳輸系統的較佳實施例功能方塊示意圖，訊息傳輸系統中包含有訊息交換中心10、第一使用者裝置11以及第二使用者裝置12，設置有通訊模組112之第一使用者裝置11以及設置有

通訊模組122之第二使用者裝置12皆信號連接至該訊息交換中心10，例如透過圖中之網際網路1來完成彼此的信號連接。上述之通訊模組112與通訊模組122可以是廣泛裝設智慧型手機上之行動通訊晶片。至於第一使用者裝置11以及第二使用者裝置12則可以分別是可以執行應用程式並具有數據通訊能力的智慧型手機、平板電腦、車用電腦或是個人電腦等資訊處理裝置，以下則以其上運行有通訊軟體應用程式之智慧型手機為主要範例來進行說明 。

【0022】 為能達到有效的資料保密，本案在其上運行有通訊軟體應用程式111(例如Signal、Telegram等各式的私密即時通訊軟體)之該第一使用者裝置11中，另外安裝有一資訊安全硬體模組110，其可信號連接至該通訊軟體應用程式111與該通訊模組112，而如圖2所示之加解密方法流程圖則執行在此訊息傳輸系統之上。首先，步驟21為該資訊安全硬體模組110依據一密鑰建立演算法(例如橢圓曲線上之密鑰建立演算法)生成至少包含一第一使用者之第一公鑰-私鑰對(USER_1-Keypair_1)之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰(USER_1-Private_key_1)僅儲存於該資訊安全硬體模組110中，而不會被儲存在該資訊安全硬體模組110的外部，用以確保該第一使用者之第一私鑰(USER_1-Private_key_1)不會被任意盜取。又因為可以將該資訊安全硬體模組110設定成不被使用者裝置核心(例如是運行其上的作業系統)可以任意存取，因此存放在該資訊安全硬體模組110中的密鑰(keys)將無法被輕易取得而使加密後的訊息內容會被輕易解讀。

【0023】 至於步驟22則是將該第一使用者之第一公鑰-私鑰對中之該第一公鑰(USER_1-Public_key_1)傳送至該訊息交換中心10中之身分註冊中心100進行身份註冊。舉例來說，身份註冊可利用該訊息交換中心10以另一管道來協助完成，

例如使用手機簡訊管道，以第一使用者的電話號碼來發送一認證碼給該第一使用者裝置11，讓第一使用者利用該第一使用者裝置11上之輸入該認證碼傳回該訊息交換中心10，用以確認第一使用者裝置11確實屬於該第一使用者而未遭冒用。而包含有身分註冊中心100之訊息交換中心10則可以是該通訊軟體應用程式111之伺服器(例如Signal、Telegram等各式的私密即時通訊軟體的伺服器)。至於信號連接至該訊息交換中心10之另一使用者裝置(第二使用者裝置12)，其上也是運行有通訊軟體應用程式121。通訊軟體應用程式111、通訊軟體應用程式121與訊息交換中心10可以是屬於同一程式開發商所發行的同一套系統組合。至於第二使用者裝置12也可以同樣利用類似步驟21、22的方式，依據上述之密鑰建立演算法(與第一使用者裝置11的密鑰建立演算法是一樣的)生成至少包含一第二使用者之第一公鑰-私鑰對(USER_2-Keypair_1)之一第二密鑰建立組合，而第二使用者之第一公鑰-私鑰對(USER_2-Keypair_1)中之第一公鑰(USER_2-Public_key_1)被傳送至該身分註冊中心100進行身份註冊，讓該身分註冊中心100可以確認該第二使用者裝置屬於該第二使用者。而該第二使用者裝置12中可以設有另一資訊安全硬體模組(本圖未示出)，也可以未設置資訊安全硬體模組，同樣可以完成身份註冊而繼續進行下列步驟。

【0024】步驟23判斷該第二使用者裝置12是否利用通訊軟體應用程式121對該訊息交換中心10發起對象為該第一使用者裝置11的一訊息傳輸動作，當該第二使用者裝置12利用通訊軟體應用程式121對該訊息交換中心10發起對象為該第一使用者裝置11之訊息傳輸動作(例如寫一段文字訊息、貼一張圖片、發一段語音訊息或發一段影音訊息)時，進入步驟24，其中該第二使用者裝置12自該訊息交換中心取得該第一使用者之第一公鑰(USER_1-Public_key_1)，該第二使用者裝

置12至少運用該第一使用者之第一公鑰(USER_1-Public_key_1)及第二使用者之第一私鑰(USER_2-Private_key_1)來進行密鑰交換與建立（例如是進行迪菲-赫爾曼密鑰交換(Diffie–Hellman key exchange)）而產生一共享密鑰，該第二使用者裝置12運用該共享密鑰將一第一訊息明文(文字訊息、圖片、語音訊息或影音訊息)進行加密而得出一第一訊息密文之後傳送給該訊息交換中心10。當然，為能減少系統資源的負擔，該第二使用者裝置12與該第一使用者裝置11完成第一次通訊時所產生之該共享密鑰，可以在往後幾次的通訊時繼續使用，直到一預設時間或達一預設次數後再重新產生另一共享密鑰即可。

【0025】步驟 25 則是該訊息交換中心 10 將該第一訊息密文傳送至該第一使用者裝置 11，而收到該第一訊息密文之該第一使用者裝置 11 所執行之共享密鑰獲取手段則是，自該訊息交換中心 10 取得該第二使用者之第一公鑰(USER_2-Public_key_1)，並使該資訊安全硬體模組 110 運用至少包含該第二使用者之第一公鑰(USER_2-Public_key_1)及第一使用者之第一私鑰 (USER_1-Private_key_1)來進行密鑰交換與建立，進而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文(步驟 26)。如此一來，通訊軟體應用程式 111 與通訊軟體應用程式 121 便可以透過訊息交換中心 10 進行安全的訊息轉傳。

【0026】而上述第一使用者裝置11之第一私鑰係僅被儲存於該資訊安全硬體模組110中，因此較安全的做法可以是：讓該第一使用者裝置11需要通過安全認證程序後，才能驅動該資訊安全硬體模組110提供該第一私鑰。也就是通過安全認證程序後該第一私鑰才會從該資訊安全硬體模組110被取出，讓第一使用者裝置11對接收到的該加密後訊息來進行解密，並可於解密完成後將該第一私鑰予以刪除而不留存在資訊安全硬體模組110之外。當然，資訊安全硬體模組110也可

以定期(每隔一段固定時間)或定量(達一定的資料量後)的來重新生成新的第一公鑰-私鑰對，用以降低第一私鑰被竊取的風險。或者，若是該資訊安全硬體模組110的運算能力足夠，也可以將該第一訊息密文直接送入該資訊安全硬體模組110中進行該第一訊息密文之解密而得回該第一訊息，如此第一私鑰將完全不會被資訊安全硬體模組110傳出。

【0027】 至於該安全認證程序可以是輸入一預設驗證密碼或生物特徵(例如指紋)來進行比對，該預設驗證密碼或生物特徵係可於使用者將通訊軟體應用程式111安裝至具有該資訊安全硬體模組110之第一使用者裝置11的過程中，將該通訊軟體應用程式111與該資訊安全硬體模組110完成綁定連結時，可由使用者來輸入設定，並可於每次登入通訊軟體應用程式111時，需要再輸入一次。另外，為了避免被駭客由遠端進行攻擊，該身份認證程序可以是需要使用者手動輸入該預設驗證密碼、該生物特徵或兩者的組合，該資訊安全硬體模組驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置11通過該身份認證程序。而該第一使用者裝置11中更設置一動作感測元件1101，用以偵測手動輸入該密碼或該生物特徵時對該第一使用者裝置11所產生之震動，進而判斷出為使用者是否以手動方式輸入，當該動作感測元件1101未能偵測到震動時則判斷為不合法輸入。而該動作感測元件1101的較佳作法可以是設置於該資訊安全硬體模組110中，確保該動作感測元件1101的正確運作且不被駭客從遠端操控。

【0028】 而上述由該第二使用者裝置12至少運用該第一使用者之第一公鑰(USER_1-Public_key_1)及第二使用者之第一私鑰(USER_2-Private_key_1)來進行密鑰建立之步驟24中，可以進行密鑰建立先獲得一共享秘密（shared secret），然後再基於該共享秘密衍生出該共享密鑰。同樣地，在該第一使用者裝置11使該資

訊安全硬體模組110運用至少包含該第二使用者之第一公鑰(USER_2-Public_key_1)及第一使用者之第一私鑰 (USER_1-Private_key_1)進行密鑰建立之步驟26中，可以進行密鑰建立先獲得一共享秘密，然後再基於該共享秘密衍生出該共享密鑰，得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。由於該共享密鑰可以根據該共享秘密以及一衍生函數來生成，因此可以根據該共享秘密與該衍生函數來定期更新該共享密鑰，降低該共享密鑰被破解的機會。而基於該共享秘密來衍生出該共享密鑰的方式可以是常見的各種金鑰衍生函數（key derivation function，簡稱KDF），如此便可以利用該共享秘密衍生出不同的共享密鑰。

【0029】 另外，包含有資訊安全硬體模組110之本案系統與方法也可以運用至點對點多媒體加密通訊的應用中，也就是將上述圖1訊息傳輸系統中之訊息交換中心10省去之另一應用環境。如此一來，當該第一使用者12裝置欲發起多媒體（聲音、影像與文字）通訊時，該第二使用者裝置12便可基於前述之加密訊息發送方式但跳過訊息交換中心10之轉傳，直接利用網際網路1將其網路位址發給第一使用者裝置11，而兩者便可透過網際網路1建立點對點的連線。連線建立後，第一使用者裝置11利用資訊安全硬體模組110產生會談所需之公鑰-私鑰對，並與第二使用者裝置12進行密鑰建立協議，用以獲得一把會談用密鑰（為能降低加解密所需資源，本例之會談加密密鑰、會談解密密鑰可以是同一把共享密鑰）並儲存於資訊安全硬體模組110中。然後，第二使用者裝置12運用資訊安全硬體模組110，利用會談加密密鑰來加密欲傳送至第一使用者裝置11之多媒體封包明文，而第一使用者裝置11也運用資訊安全硬體模組110，利用會談解密密鑰，對來自第二使用者裝置之多媒體封包密文進行解密，進而得回該多媒體封包明文。同理，

連線建立後，第二使用者裝置12也可利用相同方法來進行會談加密與解密動作，故不再贅述。當然也可以改用會談加密密鑰、會談解密密鑰互為公鑰-私鑰對之會談用密鑰對，可以視系統的運算能力來選用。

【0030】 如圖3所示之加解密方法流程圖，其便是執行在點對點多媒體加密通訊上之實施例方法流程圖，首先，步驟31為其上運行有通訊軟體應用程式111之第一使用者裝置11中之該資訊安全硬體模組110依據一密鑰建立演算法(例如是橢圓曲線上之密鑰建立演算法)生成至少包含一第一使用者之第一公鑰-私鑰對(USER_1-Keypair_1)之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰(USER_1-Private_key_1)僅儲存於該資訊安全硬體模組110中，而不會被儲存在該資訊安全硬體模組110的外部，用以確保該第一使用者之第一私鑰(USER_1-Private_key_1)不會被任意盜取。

【0031】 至於步驟32則是信號連接至網際網路1之另一使用者裝置(第二使用者裝置12)依據該密鑰建立演算法(與第一使用者裝置11的密鑰建立演算法是一樣的)生成至少包含一第二使用者之第一公鑰-私鑰對(USER_2-Keypair_1)之一第二密鑰建立組合，其上也是運行有通訊軟體應用程式121。通訊軟體應用程式111、通訊軟體應用程式121是屬於同一程式開發商所發行的同一套系統組合。而該第二使用者裝置12中可以設有另一資訊安全硬體模組(本圖未示出)，也可以未設置資訊安全硬體模組。

【0032】 步驟33判斷該第二使用者裝置12是否利用通訊軟體應用程式121發起對象為該第一使用者裝置11的一訊息傳輸動作，當該第二使用者裝置12利用通訊軟體應用程式121發起對象為該第一使用者裝置11之訊息傳輸動作(例如寫一段文字訊息、貼一張圖片、發一段語音訊息或發一段影音訊息)時，進入步驟

34，其中該第二使用者裝置12直接將其網路位址發給第一使用者裝置11，而兩者便可成功建立一點對點的連線，該第二使用者裝置12並自第一使用者裝置11透過該點對點的連線取得該第一使用者之第一公鑰(USER_1-Public_key_1)，該第二使用者裝置12至少運用該第一使用者之第一公鑰(USER_1-Public_key_1)及第二使用者之第一私鑰(USER_2-Private_key_1)來進行密鑰建立（例如是遵從迪菲-赫爾曼密鑰交換的協定來建立）而產生一共享密鑰，該第二使用者裝置12運用該共享密鑰將一第一訊息明文(文字訊息、圖片、語音訊息或影音訊息)進行加密而得出一第一訊息密文。

【0033】步驟35則是第二使用者裝置12利用已建立之點對點的連線，將該第一訊息密文傳送至該第一使用者裝置11，而收到該第一訊息密文之該第一使用者裝置11所執行之共享密鑰獲取手段則是，透過該點對點的連線自該第二使用者裝置12取得該第二使用者之第一公鑰(USER_2-Public_key_1)，並使該資訊安全硬體模組110運用至少包含該第二使用者之第一公鑰(USER_2-Public_key_1)及第一使用者之第一私鑰 (USER_1-Private_key_1)來進行密鑰建立而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文(步驟36)。如此一來，通訊軟體應用程式111與通訊軟體應用程式121便可以透過點對點的連線進行安全的訊息轉傳。

【0034】而上述資訊安全硬體模組 110 的基礎架構可以是一般常見的硬體安全模組（Hardware security module， HSM），為能增強其性能，如圖 4a 與圖 4b 之所示，本案於該資訊安全硬體模組 110 中除了該動作感測元件 1101 與殼體 1100 外，還可增設一安全晶片 1102，資訊安全硬體模組 110 的殼體 1100 外型的較佳實施例可以是一外接式記憶卡裝置，以目前常見的應用例，該外接式記憶卡

裝置可以是安全數位記憶卡(Secure Digital Memory Card)，而且可以選用不同的尺寸類型，例如安全數位記憶卡(Secure Digital Memory Card)的標準尺寸(32.0×24.0×2.1 mm）、Mini 尺寸:(21.5×20.0×1.4 mm）以及 Micro 尺寸(15.0×11.0×1.0 mm)，其中以 Micro 尺寸的安全數位記憶卡最適用於現今的智慧手機。當然，本案的技術手段也可以延用至其他記憶卡規格，例如記憶棒(Memory Stick)等，故在此不予贅述。根據上述技術說明可知，本案的資訊安全硬體模組 110 可以具有以下功能：(1)依據密鑰建立演算法產生一組或多組的公鑰-私鑰對之密鑰建立組合，並保存於硬體模組中。(2)利用保存於硬體模組中之密鑰建立組合進行密鑰建立，產生共享秘密並保存於硬體模組中。(3)利用保存於硬體模組中之共享秘密，衍生出共享密鑰，並保存於硬體中。(4)利用共享密鑰進行訊息明文加密以獲得訊息密文，或進行訊息密文解密以獲得訊息明文。(5)可根據安全認證程序的結果來選擇性地匯出共享秘密或共享密鑰。而上述的訊息明文可以是各種的數位資料，例如是文件檔案、影像檔案、聲音檔案或是混合有上述內容的多媒體檔案。

【0035】 上述之安全晶片1102可設置於該殼體1100中，該安全晶片1102可用以生成上述之公鑰-私鑰對以及進行身份認證程序等工作，安全晶片1102通常需要具備以下條件：內建密碼演算法 (Cryptographic Algorithm)、抗外力入侵(Tamper Resistant)、安全作業系統 (Secure OS) 、具有偵測各種侵入式或非侵入式攻擊的感應器(Sensors)以及用以儲存金鑰(Cryptographic Keys)的安全存儲空間等。而圖4a是將動作感測元件1101設於安全晶片1102之外的實施例，其不需要特殊規格的安全晶片。而圖4b則是將動作感測元件1101設於安全晶片1102中之實施

例，其需要特殊規格的安全晶片，但是可以確保該動作感測元件1101的正確運作且不會被駭客從遠端操控。

【0036】包含有上述安全晶片1102的資訊安全硬體模組110更可加強本案的資訊交換系統的資安功能，進而執行如圖5所示之另一較佳實施例方法流程圖，其相較於圖1所示之方法流程圖，其概念相通但同樣具有不易破解的加解密步驟。首先，第一使用者裝置11中的該資訊安全硬體模組110中之安全晶片1102生成一密鑰建立組合，該密鑰建立組合中至少包含該第一公鑰-私鑰對以及一第二公鑰-私鑰對。另外，安全晶片1102還可亂數生成一主密鑰來加密該第一私鑰(步驟41)。當然，而該主密鑰還可以其它方式生成，例如該主密鑰是選用在安全晶片1102中所儲存之一固定值，或是將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出之該主密鑰。而為能節省安全晶片1102的儲存空間，主密鑰加密該第一私鑰之該加密結果可被傳出安全晶片1102外，只留下主密鑰存在安全晶片1102內並將該加密結果刪除。當後續系統需要第一使用者之第一私鑰時，再將該加密結果傳回安全模組(安全晶片1102)，使用內部之主密鑰解密。而被解密回來的第一使用者之第一私鑰，可以接著進行密鑰建立（例如是遵從迪菲-赫爾曼密鑰交換的協定來建立），運用至少包含第二使用者之第一公鑰來共同建立共享秘密或共享密鑰。

【0037】另外，在前述雙方建立共享秘密或共享密鑰時，若直接使用自己的私鑰與接收到的公鑰，但卻無從確認該公鑰的真偽，便會產生中間人攻擊（man in the middle attack）的問題。於是本案在此處再導入數位簽章，以加強資訊安全。於是在第一使用者裝置11進行如圖2所示之步驟22中的身份註冊後便對應產生「第一數位簽章」，產生此第一數位簽章所使用的加密私鑰可以是第一使用者之該第一私鑰或是一第二私鑰，而此簽章所內含的訊息是雙方共同知道的公開資訊

（例如，第一使用者之第一公鑰，當然也可以選用另外一組第二公私鑰對中之一第二公鑰，又或是選用其他與第一使用者相關的公開資訊）。以Signal的實作為例，此處的數位簽章所使用之訊息亦是雙方知道的公開資訊，由於Signal的協議內每個使用者都產生了數個公鑰-私鑰對，然後使用其中一個特定的公鑰(例如是該第二公鑰)作為數位簽章所內含之訊息。

【0038】 而後將此第一數位簽章傳送至訊息交換中心。第二使用者裝置12自訊息交換中心10拿到第一數位簽章後，使用第一使用者裝置11的相關公開資訊(本例是第一使用者的第一公鑰)進行驗章，若是驗章通過，才接著使用至少包含第二使用者之第一私鑰、第一使用者之第一公鑰進行上述之一連串密鑰建立程序。

【0039】 因此，該第一公鑰、被該主密鑰來加密之該第一私鑰以及該數位簽章被送出該安全晶片1102之外，儲存至該第一使用者裝置11的一儲存空間(步驟42)，另外，可將該資訊安全硬體模組110之安全晶片1102內的被該主密鑰加密之該第一私鑰、該第一公鑰及該數位簽章刪除，用以節省該資訊安全硬體模組110的資料儲存空間，安全晶片1102內僅儲存主密鑰。直到需要該第一私鑰來進行解密時，再將該儲存空間中存放之該被該主密鑰加密之第一私鑰傳回該資訊安全硬體模組，並利用該主密鑰解密還原出該第一私鑰。

【0040】 而該第一使用者裝置11再將包含該第一公鑰之該加密組合以及該數位簽章傳至訊息交換中心10(步驟43)。接著，因應該第二使用者裝置12對該訊息交換中心10發起對象為該第一使用者裝置11的訊息傳輸動作(步驟44)，該訊息交換中心10便將該加密組合以及該數位簽章傳送至該第二使用者裝置12(步驟

45)，該第二使用者裝置12便根據該第一公鑰與該數位簽章來確認該數位簽章之內容是否正確，進而驗證該數位簽章之真偽(步驟46)。

【0041】驗證該數位簽章為真後之該第二使用者裝置12，至少運用該第一使用者之第一公鑰及第二使用者之第一私鑰來進行密鑰建立而產生共享密鑰，利用共享密鑰來將該第一訊息加密而得出一第一訊息密文再傳送至該訊息交換中心10(步驟47)，該訊息交換中心10將該第一訊息密文傳送至該第一使用者裝置11(步驟48)，收到該第一訊息密文之該第一使用者裝置11便自該訊息交換中心10取得該第二使用者之第一公鑰，並使該資訊安全硬體模組110之安全晶片1102運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰交換與建立，後而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文 (步驟49)。

【0042】另外，在上述例子中，僅描述該第一使用者裝置11中設有資訊安全硬體模組110的實施例，但實際上，該第二使用者裝置12也可設有另一資訊安全硬體模組(圖1未示出)或是提供類似功能的軟體，亦可發出對應於第二使用者裝置12之另一加密組合以及另一數位簽章傳至訊息交換中心10，該訊息交換中心10因應該第二使用者裝置12對該訊息交換中心10發起對象為該第一使用者裝置11的該訊息傳輸動作時，再將該另一加密組合以及該另一數位簽章傳送至該第一使用者裝置11，該第一使用者裝置11根據該另一加密組合與該另一數位簽章來驗證該另一數位簽章之真偽。當驗證該數位簽章為真時，便可認證該第二使用者裝置12之身份為真，如此一來，收到該第一訊息密文之該第一使用者裝置11，便可再使該資訊安全硬體模組110之安全晶片1102運用至少包含該第二使用者之第一

公鑰及第一使用者之第一私鑰進行密鑰交換與建立，後而得出該共享密鑰後來將該第一訊息密文進行解密，進而得回該第一訊息。

【0043】 而這部份認證該第二使用者裝置12之身份是否為真的方法可以放在圖5中步驟49之前來進行即可，若驗證該數位簽章位程序失敗，無法認證該第二使用者裝置12之身份為真時，收到該第二使用者裝置12所發送之該第一訊息密文之該第一使用者裝置11，將不會執行解密動作。

【0044】 當然，在本實施例中，資訊安全硬體模組110中之該安全晶片1102也提供身份認證功能，該第一使用者裝置11通過該身份認證程序後，才能驅動該安全晶片1102提供解密功能，進而還原出該第一訊息與該數位簽章。而且該身份認證功能為手動輸入密碼或生物特徵(例如指紋)或兩者的組合，該安全晶片1102驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置11的使用者通過該身份認證程序。另外，在上述的各種實施例中，該第一使用者裝置11於成功收到該第一訊息密文後，便可發出一確認信號給該訊息交換中心10，該訊息交換中心10於收到該確認信號後，便將該第一訊息密文刪除，降低訊息被不當利用的可能性。

【0045】 再請參見圖6，其係本案所發展出來之又一較佳實施例方法流程圖，其與上述圖2所述實施例方法的主體大致相同，也就是步驟61、步驟62、步驟63以及步驟65與圖2中之步驟21、步驟22、步驟23以及步驟25的內容一致。但是，原步驟24中的共享密鑰生成方式，在步驟64中則改成以亂數生成該共享密鑰、選用在該第二使用者裝置中所儲存之一固定值為該共享密鑰或是將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出該共享密鑰等方式來完成。

【0046】至於原本步驟26中的共享密鑰獲取手段，在步驟66中則是改以下列步驟來完成：該第二使用者裝置12自該訊息交換中心10取得該第一使用者之第一公鑰，運用該第一使用者之第一公鑰對該共享密鑰進行加密而形成一加密後之共享密鑰，然後將該加密後之共享密鑰傳送給該第一使用者裝置11，該第一使用者裝置11利用該資訊安全硬體模組110中所儲存之該第一使用者之第一私鑰來對該加密後之共享密鑰進行解密，進而得回該共享密鑰。而本實施例中的共享密鑰生成方式與共享密鑰獲取手段，也可以延用至圖3至圖5中所示的本案系統與方法實施例中，用以取代其中的密鑰生成與交換機制。由於概念類似，故在此不再贅述。

【0047】綜上所述，透過額外安裝本案所發展出的資訊安全硬體模組110，例如以安全數位記憶卡(Secure Digital Memory Card) 形式完成之資訊安全硬體模組110插置於使用者裝置(例如智慧型手機)中，便可以讓使用者裝置(例如智慧型手機)上即時通訊軟體的通訊安全性大幅提昇，因為重要的密鑰將被妥善保管在資訊安全硬體模組110中而不被輕易取得，成功消除習用手段中資訊安全的漏洞，進而改善傳統技術的問題，完成更佳的資訊安全方案，進而達成發展本案之主要目的。

【0048】另外，本案所提出的資訊安全硬體模組解決方案，若要能安裝在使用者裝置(例如智慧型手機)上並且順利執行，是需要與運作在使用者裝置(例如智慧型手機)上之通訊軟體應用程式間完成的良好配合。因此，通訊軟體應用程式必須被修改成可以與資訊安全硬體模組110(例如安全數位記憶卡(Secure Digital Memory Card))協同運作。由於有些應用程式（例如Signal通訊軟體）是屬於開放原始碼的型態，所以便可以對程式開發廠商所提供的通訊軟體應用程式原

始碼直接進行修改，然後將修改後的原始碼進行編譯而生成可以配合本案的資訊安全硬體模組解決方案的通訊軟體應用程式，然後再將完成之待安裝應用程式提供給購買資訊安全硬體模組110的客戶來進行安裝。當然，也可以額外提供修改後的完整原始碼給購買資訊安全硬體模組110的下游客戶，讓客戶能有再次修改的空間。

【0049】 而上述待安裝之應用程式可以在出廠時便預先安裝於使用者的裝置（例如上述的第一使用者裝置11及第二使用者裝置12）中，或是提供遠端連結(例如公開網站、私有雲或是應用程式商店)來供使用者來下載安裝，當然也可以將應用程式直接儲存於資訊安全硬體模組110中, 讓使用者可以在將資訊安全硬體模組110插置於使用者裝置後再點選安裝。或者，資訊安全硬體模組110的製造上也可提供安全數位記憶卡(Secure Digital Memory Card) 的應用程式介面函式庫（API library）來讓下游客戶自行整合。

【0050】 在上述實施例中的元件/裝置，還可以有不同的設置與排列，主要可視應用時之實際需求與條件而可作適當的調整或變化。因此，說明書與圖式中所示之功能方塊圖僅作說明之用，並非用以限制本揭露欲保護之範圍。另外，相關技藝者當知，實施例中的方法步驟的細節亦並不限於圖式所繪之單一態樣，亦是根據實際應用時之需求在不脫離本案揭露之技術精神的情況下而可作相應調整。因此，本案提出的訊息傳輸系統以及裝載有資訊安全硬體模組的使用者裝置，其相關技術概念當然可以運用到電子郵件系統或是線上會議系統等類似的訊息傳輸系統上，同樣可以達到通訊安全性大幅提昇，重要的密鑰不被輕易取得的優點。

【0051】綜上所述，雖然本發明以實施例揭露如上，但並非用以限定本發明。本發明所屬技術領域中具有通常知識者，在不脫離本發明之技術精神和範圍內，當可作各種之更動與潤飾。因此，本發明之保護範圍當視後附之申請專利範圍請求項所界定者為準。

【符號說明】

【0052】

1：網際網路

10：訊息交換中心

100：身分註冊中心

11：第一使用者裝置

12：第二使用者裝置

111、121：通訊軟體應用程式

112、122：通訊模組

110：資訊安全硬體模組

1101：動作感測元件

1102：安全晶片

1100：殼體

【發明申請專利範圍】

【請求項1】一種訊息傳輸系統，其包含：

一訊息交換中心；

一第一使用者裝置，信號連接至該訊息交換中心，該第一使用者裝置中插置安裝有一第一資訊安全硬體模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第一資訊安全硬體模組中，而該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心；以及

一第二使用者裝置，信號連接至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，該共享密鑰獲取手段中有運用僅儲存於該第一資訊安全硬體模組中之該第一私鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文，該第一使用者之該第一公鑰被該第二使用者裝置從該訊息交換中心取得後，被該第二使用者裝置用來產生該共享密鑰，或被該第二使用者裝置用來將該共享密鑰傳送給該第一使用者裝置的過程中。

【請求項2】如請求項1所述之訊息傳輸系統，其中該第二使用者裝置依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對之一第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二使用

者裝置中，而該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，該第二使用者裝置至少運用該第一使用者之第一公鑰及第二使用者之第一私鑰來進行密鑰建立而產生該共享密鑰，而該共享密鑰獲取手段則是該第一使用者自該訊息交換中心取得該第二使用者之第一公鑰，並使該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立而得出該共享密鑰。

【請求項3】如請求項2所述之訊息傳輸系統，其中該訊息交換中心中包含一身分註冊中心而且該第二使用者裝置中安裝有一第二資訊安全硬體模組，該第二資訊安全硬體模組依據該密鑰建立演算法生成該第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二資訊安全硬體模組中，該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第一使用者裝置屬於該第一使用者，同樣地，該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第二使用者裝置屬於該第二使用者，該第一資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第一使用者裝置中或該第二資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第二使用者裝置中，其中該第二使用者裝置自該身分註冊中心取得第一使用者之第一公鑰，運用至少包含該第一使用者之第一公鑰及第二使用者之第一私鑰，進行密鑰建立而獲得一共享秘密，然後再基於該共享秘密衍生出該共享密鑰，該第一使用者裝置，自身分註冊中心取得第二使用者之第一公鑰，並利用該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立並獲得該共享秘密並儲存於該第一資訊安全硬體模組中，該第一資訊安全硬體模組基於該共享秘密衍生出該共享密鑰，並利用該共享密鑰解密該第

一訊息密文，用以得回該第一訊息明文，其中該第一使用者裝置進行完身份註冊後便對應產生一第一數位簽章，該第一數位簽章使用該第一使用者之該第一私鑰或一第二私鑰進行簽章，簽章的訊息是與該第一使用者裝置的相關公開資訊，然後該第一使用者裝置將該第一數位簽章傳送至該訊息交換中心，該第二使用者裝置自訊息交換中心拿到該第一數位簽章後，使用該第一使用者裝置的相關公開資訊進行驗章，若通過才接著使用至少包含第二使用者之第一私鑰、第一使用者之第一公鑰進行密鑰建立。

【請求項4】 如請求項2所述之訊息傳輸系統，其中該第一資訊安全硬體模組更提供一身份認證功能，該第一使用者裝置通過該身份認證程序後，才能驅動該第一資訊安全硬體模組提供該第一私鑰來將該第一訊息密文解密而還原出該第一訊息，其中該身份認證功能為手動輸入一密碼、一生物特徵或兩者的組合，該第一資訊安全硬體模組驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置通過該身份認證程序，其中該第一資訊安全硬體模組中包含一動作感測元件，用以偵測手動輸入該密碼或該生物特徵時對該第一使用者裝置所產生之震動，進而判斷出為使用者是否以手動方式輸入，當該動作感測元件未能偵測到震動時則判斷為不合法輸入。

【請求項5】 一種訊息傳輸系統，其包含：

一第一使用者裝置，信號連接至網際網路，該第一使用者裝置中插置安裝有一第一資訊安全硬體模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第一資訊安全硬體模組中；以及

一第二使用者裝置，信號連接至網際網路，當該第二使用者裝置對該第一使用者裝置發起一訊息傳輸動作時，該第二使用者裝置直接將其網路位址發給第

一使用者裝置而建立一點對點的連線，該第二使用者裝置產生一共享密鑰，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文，該第二使用者裝置利用已建立之點對點的連線，將該第一訊息密文傳送至該第一使用者裝置，而收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，該共享密鑰獲取手段中有運用僅儲存於該第一資訊安全硬體模組中之該第一私鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文，該第一使用者之該第一公鑰被該第二使用者裝置取得後，被該第二使用者裝置用來產生該共享密鑰，或被該第二使用者裝置用來將該共享密鑰傳送給該第一使用者裝置的過程中。

【請求項6】 如請求項5所述之訊息傳輸系統，其中該第二使用者裝置依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對之一第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二使用者裝置中，而該第一使用者之第一公鑰-私鑰對中之該第一公鑰透過該點對點的連線被傳送至該第二使用者裝置，該第二使用者裝置至少運用該第一使用者之第一公鑰及該第二使用者之第一私鑰來進行密鑰建立而產生該共享密鑰，而該共享密鑰獲取手段則是該第一使用者透過該點對點的連線自該第二使用者取得該第二使用者之第一公鑰，並使該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立而得出該共享密鑰，該第一資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第一使用者裝置中。

【請求項7】 如請求項5所述之訊息傳輸系統，其中該第二使用者裝置生成該共享密鑰之方式包含下列中之一：亂數生成該共享密鑰、選用在該第二使用者裝置中所儲存之一固定值為該共享密鑰以及將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出該共享密鑰，而該共享密鑰獲取手段則包含下列步驟：該第

二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，並運用該第一使用者之第一公鑰對該共享密鑰進行加密而形成一加密後之共享密鑰，然後將該加密後之共享密鑰傳送給該第一使用者，該第一使用者利用該第一資訊安全硬體模組中所儲存之該第一使用者之第一私鑰來對該加密後之共享密鑰進行解密，進而得回該共享密鑰。

【請求項8】一種第一使用者裝置，其應用於一訊息交換中心與一第二使用者裝置之間，該第一使用者裝置包含：

一通訊模組，信號連接至該訊息交換中心；以及

一第一資訊安全硬體模組，插置安裝至該第一使用者裝置的一殼體中並信號連接至該通訊模組，該第一資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對之一第一密鑰建立組合，該第一使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第一資訊安全硬體模組中，而該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，該共享密鑰獲取手段中有運用僅儲存於該第一資訊安全硬體模組中之該第一私鑰，並利用該共享密鑰解密該第一訊息密文，以得回該第一訊息明文，該第一使用者之該第一公鑰被該第二使用者裝置從該訊息交換中心取得後，被該第二使用者裝置用來產生該共享密鑰，或被該第二使用者裝置用來將該共享密鑰傳送給該第一使用者裝置的過程中。

【請求項9】 如請求項8所述之第一使用者裝置，其應用之該第二使用者裝置依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對之一第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二使用者裝置中，而該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，該第二使用者裝置至少運用該第一使用者之第一公鑰及第二使用者之第一私鑰來進行密鑰建立而產生該共享密鑰，而該共享密鑰獲取手段則是該第一使用者自該訊息交換中心取得該第二使用者之第一公鑰，並使該第一資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立而得出該共享密鑰。

【請求項10】 如請求項9所述之第一使用者裝置，其應用之訊息交換中心中包含一身分註冊中心而且該第二使用者裝置中安裝有一第二資訊安全硬體模組，該第二資訊安全硬體模組依據該密鑰建立演算法生成該第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二資訊安全硬體模組中，該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第一使用者裝置屬於該第一使用者，同樣地，該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第二使用者裝置屬於該第二使用者，該第一資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第一使用者裝置中或該第二資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第二使用者裝置中，該第二使用者裝置自該身分註冊中心取得第一使用者之第一公鑰，運用至少包含該第一使用者之第一公鑰及第二使用者之第一私鑰，進行密鑰建立而獲得一共享秘密，然後再基於該共享秘密衍生出該共享密鑰，該第一使用者裝置，自身分註冊中心取得第二使用者之第一公鑰，並利用該第一資訊安全

硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立並獲得該共享秘密並儲存於該第一資訊安全硬體模組中，該第一資訊安全硬體模組基於該共享秘密衍生出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文。

【請求項11】 如請求項10所述之第一使用者裝置，其中該第一使用者裝置進行完身份註冊後便對應產生一第一數位簽章，該第一數位簽章使用該第一使用者之該第一私鑰或一第二私鑰進行簽章，簽章的訊息是與該第一使用者裝置的相關公開資訊，然後該第一使用者裝置將該第一數位簽章傳送至該訊息交換中心，該第二使用者裝置自訊息交換中心拿到該第一數位簽章後，使用該第一使用者裝置的相關公開資訊進行驗章，若通過才接著使用至少包含第二使用者之第一私鑰、第一使用者之第一公鑰進行密鑰建立。

【請求項12】 如請求項9所述之第一使用者裝置，其中該第一資訊安全硬體模組更提供一身份認證功能，該第一使用者裝置通過該身份認證程序後，才能驅動該第一資訊安全硬體模組提供該第一私鑰來將該第一訊息密文解密而還原出該第一訊息，其中該身份認證功能為手動輸入一密碼、一生物特徵或兩者的組合，該第一資訊安全硬體模組驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置通過該身份認證程序，其中該第一資訊安全硬體模組中包含一動作感測元件，用以偵測手動輸入該密碼或該生物特徵時對該第一使用者裝置所產生之震動，進而判斷出為使用者是否以手動方式輸入，當該動作感測元件未能偵測到震動時則判斷為不合法輸入。

【請求項13】 一種資訊安全硬體模組，插置安裝至一第一使用者裝置的殼體中，該第一使用者裝置、一第二使用者裝置皆信號連接至一訊息交換中心構成一訊息傳輸系統，該資訊安全硬體模組電性連接至該第一使用者裝置，該資訊安全硬體模組依據一密鑰建立演算法生成至少包含一第一公鑰-私鑰對之一第一密鑰

建立組合，該第一公鑰-私鑰對中之該第一私鑰僅儲存於該資訊安全硬體模組中，而該第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置產生一共享密鑰，當該第二使用者裝置對該訊息交換中心發起對象為該第一使用者裝置的一訊息傳輸動作時，該第二使用者裝置運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心，該訊息交換中心將該一第一訊息密文傳送至該第一使用者裝置，收到該第一訊息密文之該第一使用者裝置透過一共享密鑰獲取手段而取得該共享密鑰，該共享密鑰獲取手段中有運用僅儲存於該資訊安全硬體模組中之該第一私鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文，該第一使用者之該第一公鑰被該第二使用者裝置從該訊息交換中心取得後，被該第二使用者裝置用來產生該共享密鑰，或被該第二使用者裝置用來將該共享密鑰傳送給該第一使用者裝置的過程中。

【請求項14】 如請求項13所述之資訊安全硬體模組，其應用之該第二使用者裝置依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對之一第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該第二使用者裝置中，而該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該訊息交換中心，該第二使用者裝置自該訊息交換中心取得該第一使用者之第一公鑰，該第二使用者裝置至少運用該第一使用者之第一公鑰及第二使用者之第一私鑰來進行密鑰建立而產生該共享密鑰，而該共享密鑰獲取手段則是該第一使用者自該訊息交換中心取得該第二使用者之第一公鑰，該資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立而得出該共享密鑰。

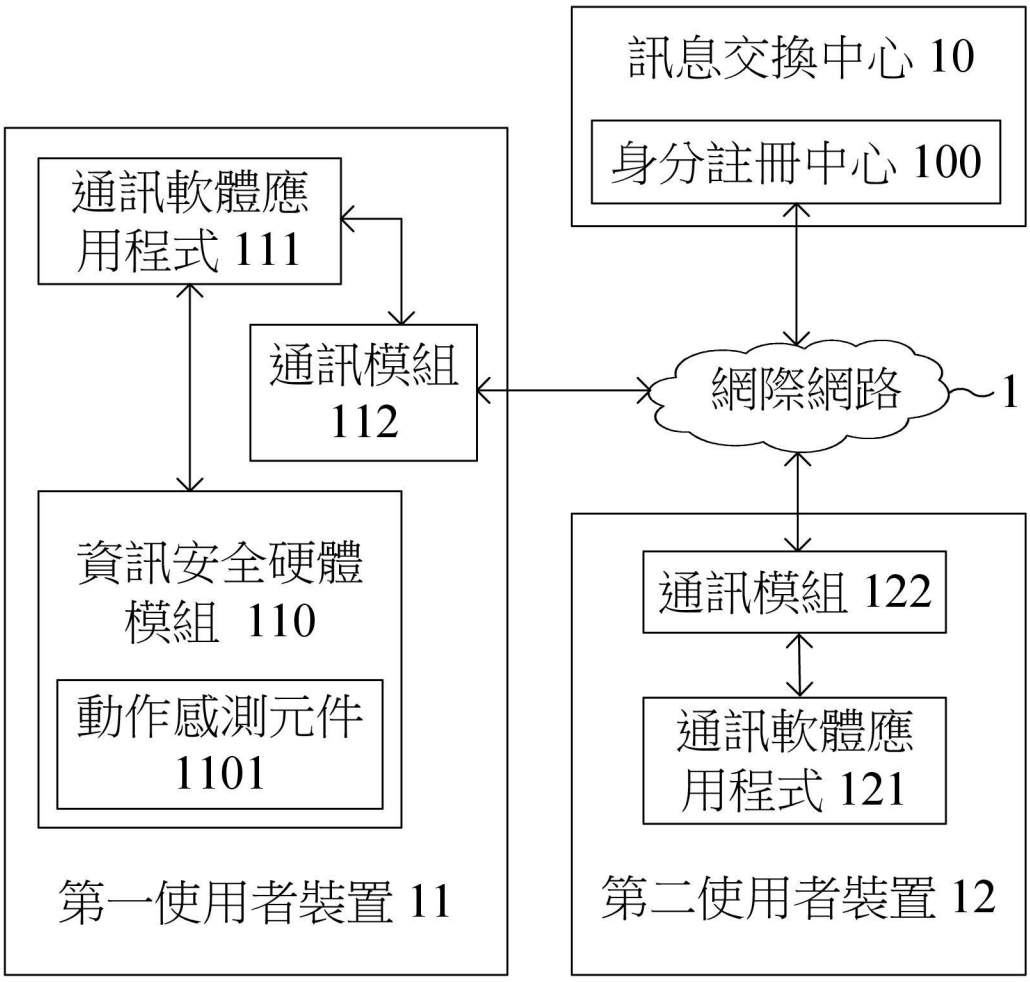
【請求項15】 如請求項14所述之資訊安全硬體模組，其應用之該訊息交換中心中包含一身分註冊中心而且該第二使用者裝置中安裝有一另一資訊安全硬體

模組，該另一資訊安全硬體模組依據該密鑰建立演算法生成該第二密鑰建立組合，該第二使用者之第一公鑰-私鑰對中之該第一私鑰僅儲存於該另一資訊安全硬體模組中，該第一使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第一使用者裝置屬於該第一使用者，同樣地，該第二使用者之第一公鑰-私鑰對中之該第一公鑰被傳送至該身分註冊中心進行身份註冊，該身分註冊中心確認該第二使用者裝置屬於該第二使用者，該資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第一使用者裝置中或該另一資訊安全硬體模組係以安全數位記憶卡形式完成並插置於該第二使用者裝置中，其應用之該第二使用者裝置自該身分註冊中心取得第一使用者之第一公鑰，運用至少包含該第一使用者之第一公鑰及第二使用者之第一私鑰，進行密鑰建立而獲得一共享秘密，然後再基於該共享秘密衍生出該共享密鑰，該第一使用者裝置，自身分註冊中心取得第二使用者之第一公鑰，並利用該資訊安全硬體模組運用至少包含該第二使用者之第一公鑰及第一使用者之第一私鑰進行密鑰建立並獲得該共享秘密並儲存於該資訊安全硬體模組中，該資訊安全硬體模組基於該共享秘密衍生出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文，其所安裝之該第一使用者裝置進行完身份註冊後便對應產生一第一數位簽章，該第一數位簽章使用該第一使用者之該第一私鑰或一第二私鑰進行簽章，簽章的訊息是與該第一使用者裝置的相關公開資訊，然後該第一使用者裝置將該第一數位簽章傳送至該訊息交換中心，該第二使用者裝置自訊息交換中心拿到該第一數位簽章後，使用該第一使用者裝置的相關公開資訊進行驗章，若通過才接著使用至少包含第二使用者之第一私鑰、第一使用者之第一公鑰進行密鑰建立。

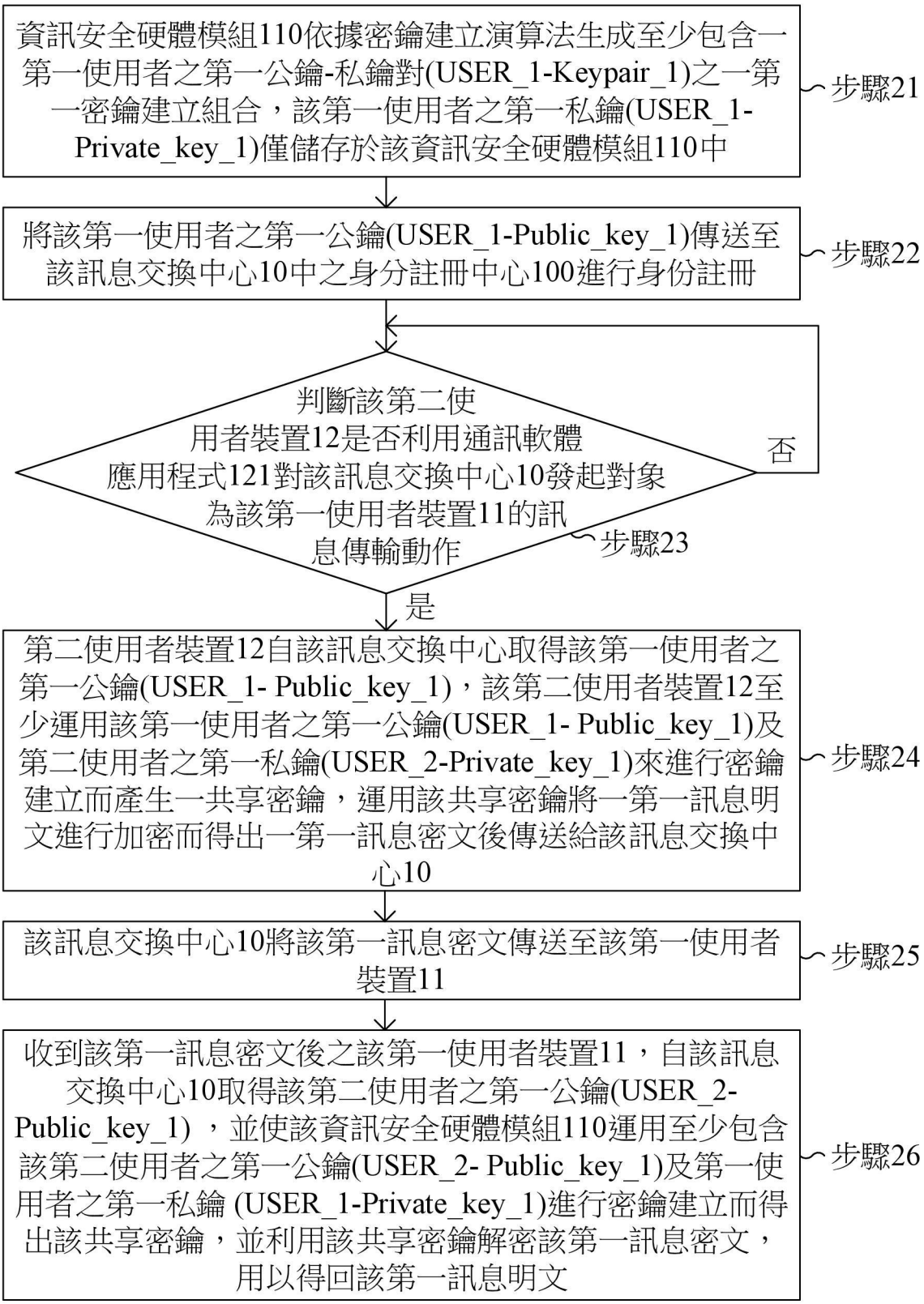
【請求項16】 如請求項14所述之資訊安全硬體模組，其中該資訊安全硬體模組更提供一身份認證功能，該第一使用者裝置通過該身份認證程序後，才能驅動

該資訊安全硬體模組提供該第一私鑰來將該第一訊息密文解密而還原出該第一訊息，其中該身份認證功能為手動輸入一密碼、一生物特徵或兩者的組合，該資訊安全硬體模組驗證該密碼或該生物特徵或兩者的組合無誤後，便判斷該第一使用者裝置通過該身份認證程序，其中該資訊安全硬體模組中包含一動作感測元件，用以偵測手動輸入該密碼或該生物特徵時對該第一使用者裝置所產生之震動，進而判斷出為使用者是否以手動方式輸入，當該動作感測元件未能偵測到震動時則判斷為不合法輸入。

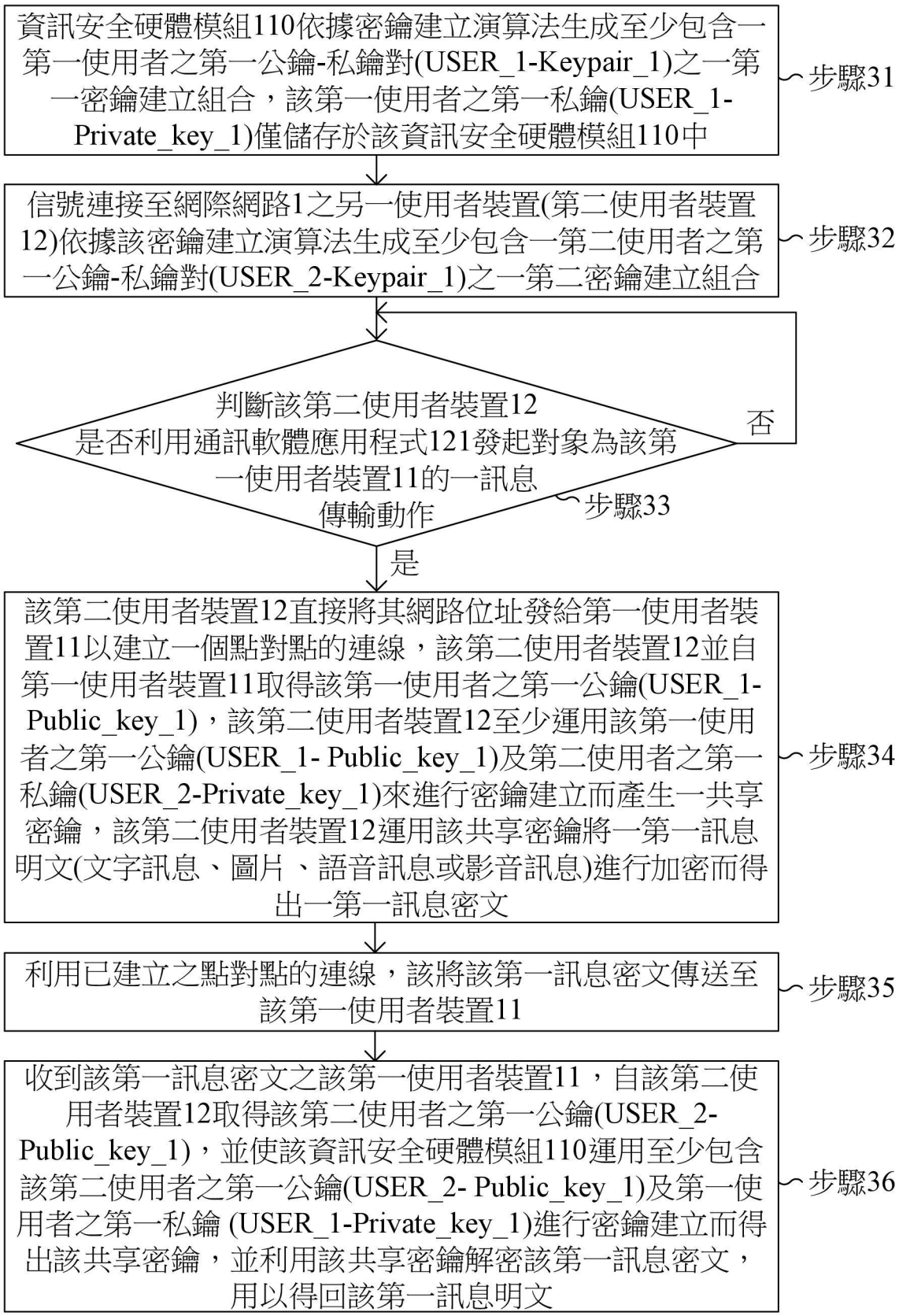
【發明圖式】


訊息交換中心 10
身分註冊中心 100
通訊軟體應用程式 111
通訊模組 112
網際網路
1
資訊安全硬體模組 110
動作感測元件 1101
第一使用者裝置 11
通訊模組 122
通訊軟體應用程式 121
第二使用者裝置 12

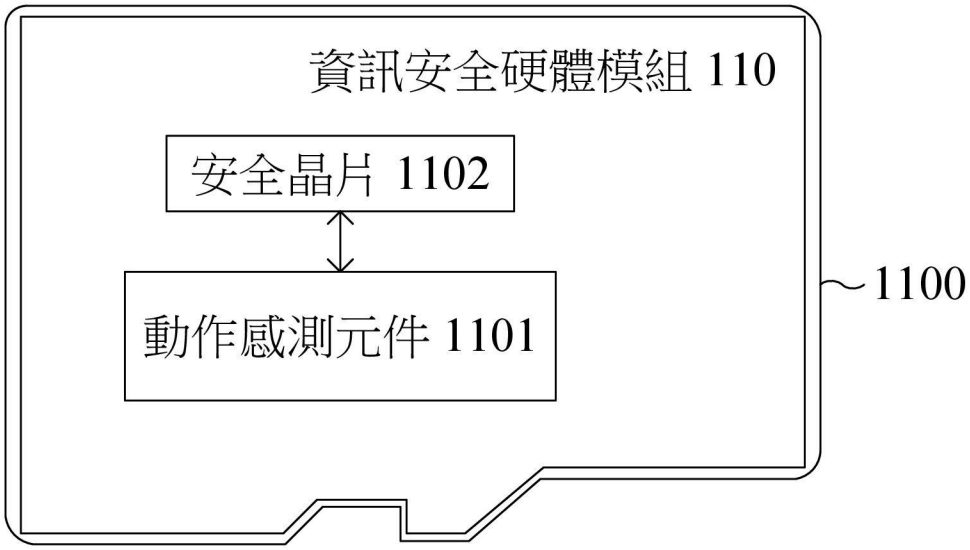
【圖 1】


資訊安全硬體模組110依據密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對(USER_1-Keypair_1)之一第一密鑰建立組合，該第一使用者之第一私鑰(USER_1-Private_key_1)僅儲存於該資訊安全硬體模組110中
步驟21
將該第一使用者之第一公鑰(USER_1-Public_key_1)傳送至該訊息交換中心10中之身分註冊中心100進行身份註冊
步驟22
判斷該第二使用者裝置12是否利用通訊軟體應用程式121對該訊息交換中心10發起對象為該第一使用者裝置11的訊息傳輸動作
步驟23
否
是
第二使用者裝置12自該訊息交換中心取得該第一使用者之第一公鑰(USER_1- Public_key_1)，該第二使用者裝置12至少運用該第一使用者之第一公鑰(USER_1- Public_key_1)及第二使用者之第一私鑰(USER_2-Private_key_1)來進行密鑰建立而產生一共享密鑰，運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心10
步驟24
該訊息交換中心10將該第一訊息密文傳送至該第一使用者裝置11
步驟25
收到該第一訊息密文後之該第一使用者裝置11，自該訊息交換中心10取得該第二使用者之第一公鑰(USER_2-Public_key_1) ，並使該資訊安全硬體模組110運用至少包含該第二使用者之第一公鑰(USER_2- Public_key_1)及第一使用者之第一私鑰 (USER_1-Private_key_1)進行密鑰建立而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文
步驟26

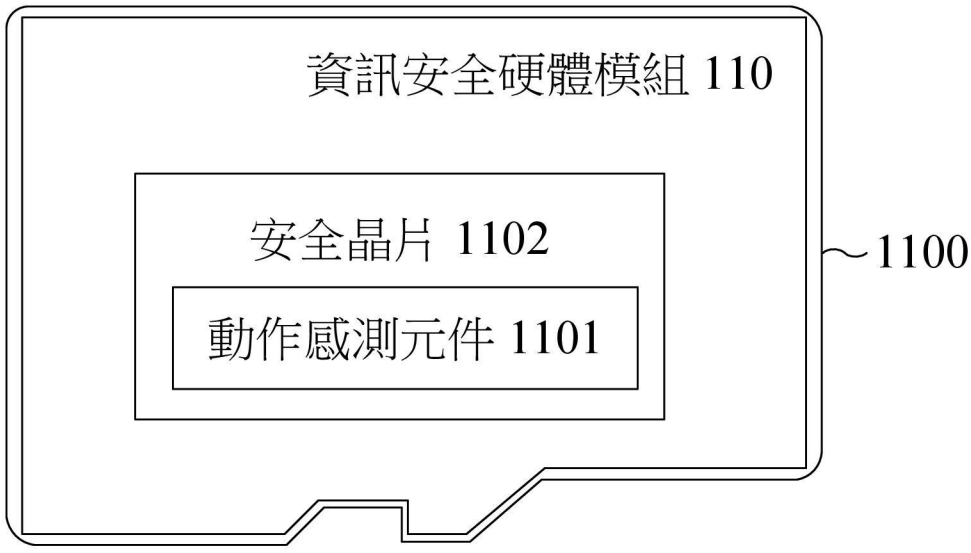
【圖 2】


資訊安全硬體模組110依據密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對(USER_1-Keypair_1)之一第一密鑰建立組合，該第一使用者之第一私鑰(USER_1-Private_key_1)僅儲存於該資訊安全硬體模組110中
步驟31
信號連接至網際網路1之另一使用者裝置(第二使用者裝置12)依據該密鑰建立演算法生成至少包含一第二使用者之第一公鑰-私鑰對(USER_2-Keypair_1)之一第二密鑰建立組合
步驟32
判斷該第二使用者裝置12是否利用通訊軟體應用程式121發起對象為該第一使用者裝置11的一訊息傳輸動作
步驟33
否
是
該第二使用者裝置12直接將其網路位址發給第一使用者裝置11以建立一個點對點的連線，該第二使用者裝置12並自第一使用者裝置11取得該第一使用者之第一公鑰(USER_1-Public_key_1)，該第二使用者裝置12至少運用該第一使用者之第一公鑰(USER_1- Public_key_1)及第二使用者之第一私鑰(USER_2-Private_key_1)來進行密鑰建立而產生一共享密鑰，該第二使用者裝置12運用該共享密鑰將一第一訊息明文(文字訊息、圖片、語音訊息或影音訊息)進行加密而得出一第一訊息密文
步驟34
利用已建立之點對點的連線，該將該第一訊息密文傳送至該第一使用者裝置11
步驟35
收到該第一訊息密文之該第一使用者裝置11，自該第二使用者裝置12取得該第二使用者之第一公鑰(USER_2-Public_key_1)，並使該資訊安全硬體模組110運用至少包含該第二使用者之第一公鑰(USER_2- Public_key_1)及第一使用者之第一私鑰 (USER_1-Private_key_1)進行密鑰建立而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文
步驟36

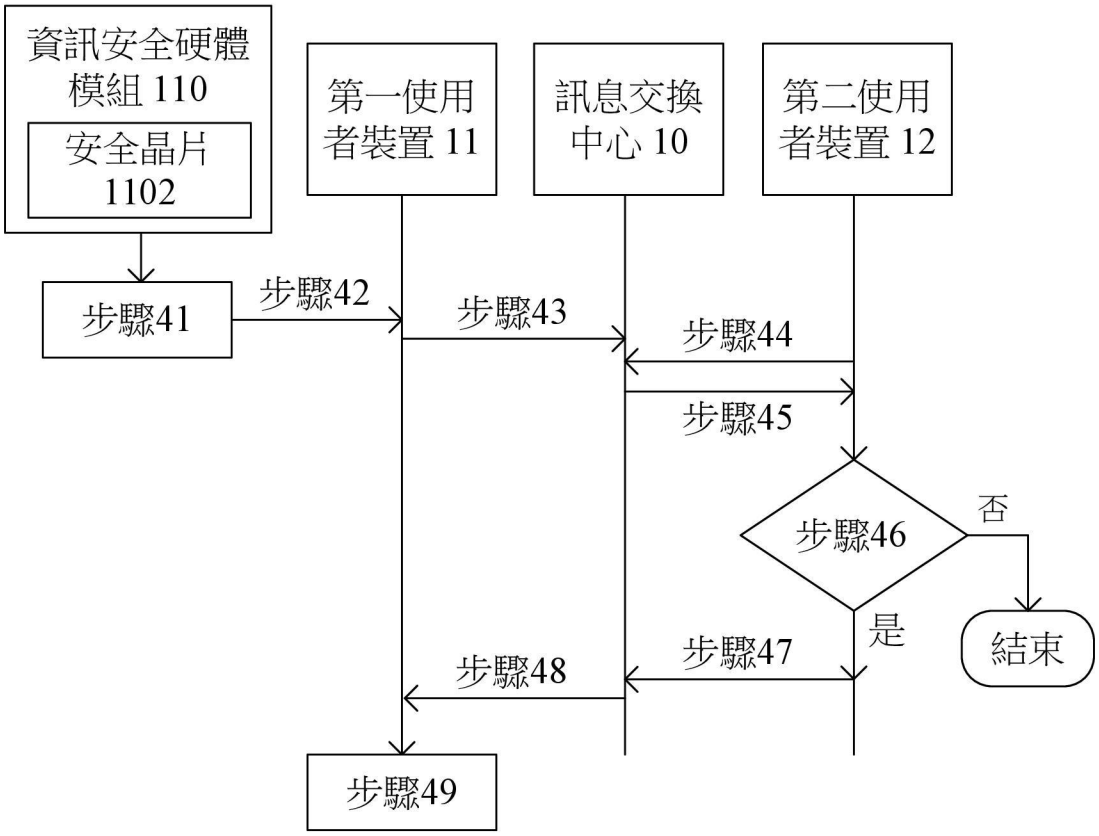
【圖 3】


資訊安全硬體模組 110
安全晶片 1102
動作感測元件 1101
1100

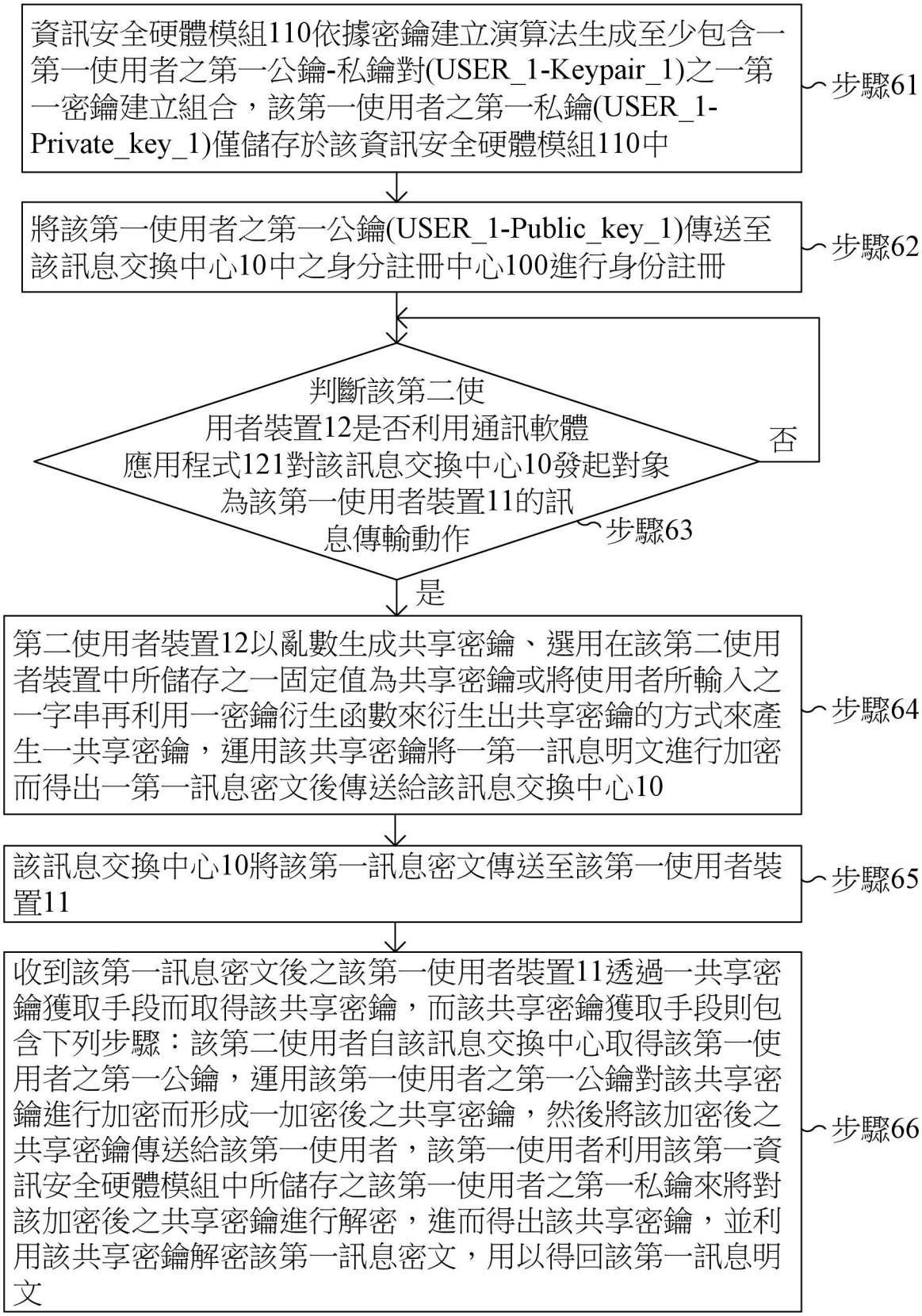
【圖 4a】


資訊安全硬體模組 110
安全晶片 1102
動作感測元件 1101
1100

【圖 4b】


資訊安全硬體模組 110
安全晶片 1102
第一使用者裝置 11
訊息交換中心 10
第二使用者裝置 12
步驟41
步驟42
步驟43
步驟44
步驟45
步驟46
否
是
結束
步驟47
步驟48
步驟49

【圖 5】


資訊安全硬體模組110依據密鑰建立演算法生成至少包含一第一使用者之第一公鑰-私鑰對(USER_1-Keypair_1)之一第一密鑰建立組合，該第一使用者之第一私鑰(USER_1-Private_key_1)僅儲存於該資訊安全硬體模組110中
步驟61
將該第一使用者之第一公鑰(USER_1-Public_key_1)傳送至該訊息交換中心10中之身分註冊中心100進行身份註冊
步驟62
判斷該第二使用者裝置12是否利用通訊軟體應用程式121對該訊息交換中心10發起對象為該第一使用者裝置11的訊息傳輸動作
步驟63
否
是
第二使用者裝置12以亂數生成共享密鑰、選用在該第二使用者裝置中所儲存之一固定值為共享密鑰或將使用者所輸入之一字串再利用一密鑰衍生函數來衍生出共享密鑰的方式來產生一共享密鑰，運用該共享密鑰將一第一訊息明文進行加密而得出一第一訊息密文後傳送給該訊息交換中心10
步驟64
該訊息交換中心10將該第一訊息密文傳送至該第一使用者裝置11
步驟65
收到該第一訊息密文後之該第一使用者裝置11透過一共享密鑰獲取手段而取得該共享密鑰，而該共享密鑰獲取手段則包含下列步驟：該第二使用者自該訊息交換中心取得該第一使用者之第一公鑰，運用該第一使用者之第一公鑰對該共享密鑰進行加密而形成一加密後之共享密鑰，然後將該加密後之共享密鑰傳送給該第一使用者，該第一使用者利用該第一資訊安全硬體模組中所儲存之該第一使用者之第一私鑰來將對該加密後之共享密鑰進行解密，進而得出該共享密鑰，並利用該共享密鑰解密該第一訊息密文，用以得回該第一訊息明文
步驟66

【圖 6】