I724681

(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 I724681 B**

(45)公告日： 中華民國 110 (2021) 年 04 月 11 日

(21)申請案號：108145255　(22)申請日： 中華民國 108 (2019) 年 12 月 11 日

(51)Int. Cl.：　*G06F21/62　(2013.01)*　*G06F21/31　(2013.01)*

H04L9/32　(2006.01)

(30)優先權：2019/03/29　世界智慧財產權組織　PCT/CN2019/080372

(71)申請人：開曼群島商創新先進技術有限公司 (開曼群島) ADVANCED NEW TECHNOLOGIES CO., LTD.　(KY)
開曼群島

(72)發明人：馮志遠 (CN) ；李艷鵬 (CN) ；程龍 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	201741922A	CN	101436247A
CN	109150535A	US	2011/0126024A1

審查人員：吳家豪

申請專利範圍項數：7 項　圖式數：7　共 41 頁

(54)名稱

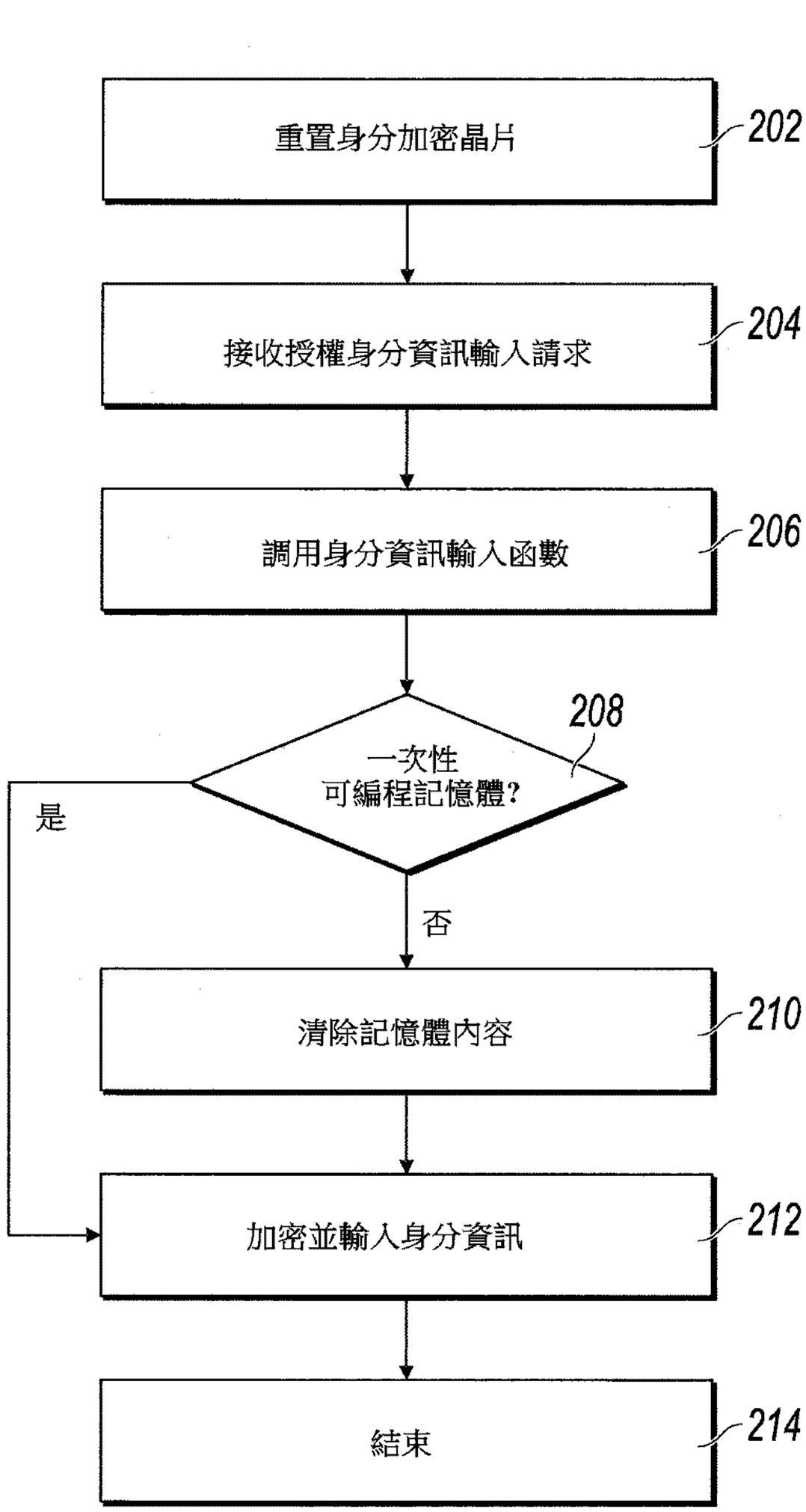
基於身分資訊管理密碼金鑰

(57)摘要

本文公開了用於基於用戶身分資訊管理密碼金鑰的方法、系統和裝置，包括編碼在電腦儲存媒體上的電腦程式。方法之一包括：接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至身分加密晶片(ICC)上的記憶體中的請求；將與所述用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較；回應於確定與所述用戶相關聯的生物特徵資訊和預先儲存的生物特徵資訊匹配，對用戶金鑰對進行加密以提供加密的用戶金鑰對；並將加密的用戶金鑰對儲存至所述記憶體中。

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for managing cryptographic keys based on user identity information. One of the methods includes receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC); comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information; in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and storing the encrypted user key pair to the memory.

指定代表圖：


200
重置身分加密晶片
202
接收授權身分資訊輸入請求
204
調用身分資訊輸入函數
206
一次性
可編程記憶體?
208
是
否
清除記憶體內容
210
加密並輸入身分資訊
212
結束
214

【圖 2】

專利案號：108145255

公告本

I724681

【發明摘要】

【中文發明名稱】

基於身分資訊管理密碼金鑰

【英文發明名稱】

MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

【中文】

本文公開了用於基於用戶身分資訊管理密碼金鑰的方法、系統和裝置，包括編碼在電腦儲存媒體上的電腦程式。方法之一包括：接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至身分加密晶片(ICC)上的記憶體中的請求；將與所述用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較；回應於確定與所述用戶相關聯的生物特徵資訊和預先儲存的生物特徵資訊匹配，對用戶金鑰對進行加密以提供加密的用戶金鑰對；並將加密的用戶金鑰對儲存至所述記憶體中。

【英文】

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for managing cryptographic keys based on user identity information. One of the methods includes receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC); comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information; in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and storing the encrypted user key pair to the memory.

【指定代表圖】第(２)圖。
【代表圖之符號簡單說明】無

【特徵化學式】無

【發明說明書】

【中文發明名稱】

基於身分資訊管理密碼金鑰

【英文發明名稱】

MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

【技術領域】

本文有關身分認證技術和資料安全性。

【先前技術】

身分認證技術通常用於電腦網路中以驗證用戶身分並確保資料安全性。如同在電腦網路中數位化儲存或傳送的其他資訊一樣，身分資訊可以由資料集表示。電腦可以基於用戶的數位身分來識別和認證用戶。對於資料安全性，重要的是確保數字身分屬於授權用戶，或者換句話說，數字身分與實際身分相匹配。

身分認證技術通常用於電腦網路中以驗證用戶身分並確保資料安全性。如同在電腦網路中數位化儲存或傳送的其他資訊一樣，身分資訊可以由資料集表示。電腦可以基於用戶的數位身分來識別和認證用戶。對於資料安全性，重要的是確保數字身分屬於授權用戶，或者換句話說，數字身分與實際身分相匹配。

隨著技術的發展，已經出現了諸如區塊鏈網路和物聯網(IoT)網路的去中心化系統。在去中心化系統下，個人可以安全地自行儲存他們自己的身分資訊。例如，用戶可以持有數位錢包，該數位錢包儲存用戶可以用來添加數位簽章以授權區塊鏈網路或IoT設備上的交易的私密金鑰。私密金鑰通常作為具有加密語義的資料串儲存在計算設備上，並且意圖僅供用戶存取。與其他資料串一樣，私密金鑰可潛在地被複製和共用。具有私密金鑰的任何用戶都可以控制與該私密金鑰相關聯的數位資產。此外，如果私密金鑰丟失，則無法檢索數字資產。因此，安全儲存和有效使用密碼金鑰會是重要的。

期望開發一種金鑰管理技術，其可以基於用戶的真實身分安全地管理用戶的密碼金鑰。

【發明內容】

本文描述了用於基於用戶身分資訊管理密碼金鑰的技術。這些技術通常涉及：身分加密晶片(ICC)接收生物特徵資訊和用以將用戶金鑰對儲存至ICC上的記憶體中的請求，確定生物特徵資訊與預先儲存在晶片上的生物特徵資訊匹配，以及對用戶金鑰對進行加密並將其儲存在ICC的記憶體中。

本文還提供了耦接到一個或多個處理器並且其上儲存有指令的一個或多個非暫態電腦可讀儲存媒體，當所述指令由所述一個或多個處理器執行時，所述指令將促使所述

一個或多個處理器按照本文提供的方法的實施例執行操作。

本文還提供了用於實施本文提供的所述方法的系統。該系統包括一個或多個處理器以及耦接到所述一個或多個處理器並且其上儲存有指令的電腦可讀儲存媒體，當所述指令由所述一個或多個處理器執行時，所述指令將導致所述一個或多個處理器按照本文提供的方法的實施例執行操作。

應瞭解，依據本文的方法可以包括本文描述的方面和特徵的任意組合。也就是說，根據本文的方法不限於本文具體描述的方面和特徵的組合，還包括所提供的方面和特徵的任意組合。

以下在圖式和描述中闡述了本文的一個或多個實施例的細節。根據說明書和圖式以及申請專利範圍，本文的其他特徵和優點將顯而易見。

【圖式簡單說明】

[圖1] 是顯示用於執行可用於執行本文的實施例的處理的身分加密晶片的示例的示圖。

[圖2] 是顯示根據本文的實施例的用於身分加密晶片初始化處理的示例的流程圖。

[圖3] 是顯示根據本文的實施例的用於向身分加密晶片輸入資訊的處理的示例的流程圖。

[圖4] 是顯示根據本文的實施例的使用身分加密晶片

執行加密操作的處理的示例的流程圖。

[圖5]是顯示根據本文的實施例的金鑰管理設備的示例的示圖。

[圖6]描繪了可以根據本文的實施例執行的方法的示例。

[圖7]描繪了根據本文的實施例的裝置的模組的示例。

各圖式中相同的圖式標記和名稱表示相同的元件。

【實施方式】

本文描述了用於基於用戶身分資訊管理密碼金鑰的技術。這些技術通常涉及：身分加密晶片(ICC)接收生物特徵資訊和用以將用戶金鑰對儲存至ICC上的記憶體中的請求，確定生物特徵資訊與預先儲存在晶片上的生物特徵資訊匹配，以及對用戶金鑰對進行加密並將其儲存在ICC的記憶體中。

圖1是顯示用於執行可用於執行本文的實施例的處理的ICC 100的示例的示圖。在較高層面上，ICC 100可以是包括記憶體102和邏輯計算元件104的電腦晶片。ICC 100可用於安全地執行加密操作。在一些實施例中，ICC 100可以是包括一個或多個晶片組件的晶片組。記憶體102和邏輯計算元件104可以整合到不同的晶片組件中。在一些實施例中，記憶體102可用於提供永久儲存。在一些示例中，記憶體102可以是可程式設計唯讀記憶體(PROM)，其

允許被寫入一次並且之後僅唯讀。在一些示例中，記憶體102可以是電可抹除可程式設計唯讀記憶體(EEPROM)或快閃記憶體，其可以被重新格式化並重新程式設計。在一些實施例中，邏輯計算元件可以是專用積體電路(ASIC)或單晶片微電腦(SCM)。

在一些電腦網路中，實施密碼術以維護資料或交易的隱私。例如，在區塊鏈網路中，如果兩個節點想要保持交易隱私，使得區塊鏈網路中的其他節點無法辨別該交易的細節，則節點可以加密交易資料。示例性加密操作包括但不限於對稱式金鑰密碼編譯和非對稱式金鑰密碼編譯。對稱加密是指使用單個金鑰既進行加密(從明文產生密文)又進行解密(從密文產生明文)的加密處理。

非對稱加密使用金鑰對，每個金鑰對包括私密金鑰和公開金鑰，私密金鑰僅對對應用戶是已知的，並且公開金鑰可以公開地傳播。用戶可以使用另一用戶的公開金鑰來加密資料，並且該加密的資料可以使用該另一用戶的私密金鑰來解密。

可以使用非對稱加密來提供數位簽章，這使得交易中的用戶能夠確認交易中的其他用戶以及交易的有效性。例如，用戶可以對訊息進行數位簽章，而另一用戶可以基於數位簽章確認訊息是由該用戶發送的。數位簽章還可用於確保訊息在傳輸過程中不被篡改。例如，用戶A將向用戶B發送訊息。用戶A產生訊息的雜湊值，然後使用其私密金鑰加密雜湊值以提供為加密雜湊值的數位簽章。用戶A

將數位簽章附加到訊息，並將帶有數位簽章的訊息發送給用戶B。用戶B使用用戶A的公開金鑰解密數位簽章，並提取雜湊值。用戶B對訊息進行雜湊處理並比較雜湊值。如果雜湊值相同，則用戶B可以確認該訊息確實來自用戶A，並且未被篡改。

ICC 100可以用於基於對用戶身分資訊進行驗證來安全地執行加密操作。記憶體102可用於儲存可信用戶身分資訊和密碼金鑰資訊。記憶體102還可以儲存身分認證演算法(例如，作為電腦可執行碼)和加密操作演算法(例如，作為電腦可執行碼)。在一些實施例中，儲存在記憶體102中的資訊和演算法被加密以即使在ICC 100被進行逆向工程的情況下也防止洩密。當從用戶接收到用以執行加密操作的請求時，邏輯計算元件104可以使用從用戶收集的身分資訊和儲存在記憶體102中的可信用戶身分資訊，以基於身分認證演算法驗證用戶的身分。例如，如果身分資訊是用戶指紋的指紋圖像，則身分認證演算法可以是本地認證演算法，其將從用戶收集的指紋圖像和儲存的指紋圖像進行比較。如果收集的指紋圖像與儲存的指紋圖像匹配，則成功驗證用戶的身分。然後，邏輯計算元件104可以使用所儲存的密碼金鑰資訊來執行所請求的加密操作。在執行加密操作之後，可以由ICC 100輸出操作結果。透過使用ICC 100，可以僅在驗證或認證用戶的身分可信之後執行加密操作。這樣，可以保證用戶執行操作的許可權。此外，由於密碼金鑰作為密文儲存在ICC 100中，因此加密

操作在ICC 100內部執行。只有操作結果從ICC 100輸出。以這種方式，可以確保密碼金鑰的安全性。

在110，授權身分資訊被輸入到ICC 100。授權身分資訊可以在ICC 100的初始化期間輸入到ICC 100。在一些實施例中，授權身分資訊可以是用戶的生物特徵資訊，例如指紋、聲紋、心跳資訊或虹膜資訊。在一些實施例中，授權身分資訊可以由ICC 100的所有者輸入。如將在本文的實施例中進一步討論的，輸入授權身分資訊的用戶可以使用該授權身分資訊來控制輸入到ICC 100的密碼金鑰。除非可以基於授權身分資訊驗證用戶身分，否則不能將密碼金鑰輸入到ICC 100。

授權身分資訊可以用於執行身分驗證以便為儲存密碼金鑰或執行加密操作提供授權。身分資訊可以由與ICC 100可通訊地耦接的計算設備收集。例如，計算設備可以是能夠檢測用戶的生物特徵資訊的智慧型手錶。

在112，清除記憶體內容並且將授權身分資訊寫入記憶體102。在一些實施例中，記憶體102是永久記憶體。在一些實施例中，為了防止篡改，身分資訊只能被寫入記憶體102的儲存單元一次。如果需要使用新的身分資訊來替換現有的授權金鑰，則可以在寫入新的身分資訊之前抹除記憶體102的內容。在一些實施例中，可以在將授權身分資訊寫入記憶體102之前對授權身分資訊進行加密以增強安全性。

在114，接收用戶的身分資訊和用以寫入用戶的非對

稱金鑰對的請求。如本文所述，可用於執行加密操作的非對稱金鑰對可被寫入記憶體102。應理解的是，還可以基於特定加密操作請求將其他密碼金鑰寫入ICC 100。身分資訊可以是生物特徵資訊，例如指紋、聲紋、心跳資訊或虹膜資訊。身分資訊可以由與ICC 100可通訊地耦接的計算設備收集。在116，從記憶體102讀取授權身分資訊以在118驗證用戶的身分。可以基於將在114接收的用戶的身分資訊與授權身分資訊進行匹配來執行驗證。如果身分資訊匹配，則驗證成功。結果，用戶被認證為ICC 100的授權用戶，以允許非對稱金鑰對被輸入到ICC 100。否則，拒絕在114的請求。在122，將非對稱金鑰對寫入ICC 100的記憶體102。在一些實施例中，可以在將非對稱金鑰對寫入記憶體102之前對非對稱金鑰對加密以增強安全性。在一些實施例中，可以將非對稱金鑰對寫入記憶體102的與儲存授權身分資訊的儲存單元分開的儲存單元。

在124，接收用戶的身分資訊和用以執行加密操作的請求。身分資訊可以由與ICC 100可通訊地耦接的計算設備收集。例如，計算設備可以是可以收集用戶的生物特徵資訊的智慧型手錶，生物特徵資訊被用作用以識別用戶的身分資訊。在收集身分資訊之後，可以將其發送到ICC 100。在一些實施例中，還可以將要被執行加密操作的資料發送到ICC 100。例如，如果加密操作是加密，則對應的資料可以是要被加密的資料檔案。在126，在122寫入記憶體102的授權身分資訊從記憶體102被讀取以在128執行

身分驗證。可以基於在124接收的身分資訊與授權身分資訊的比較來執行身分驗證。如果身分資訊匹配，則驗證成功，並且在130從記憶體102讀取對應的非對稱金鑰資訊以執行加密操作。在132，使用合適的密碼金鑰執行加密操作。如果身分資訊不匹配，則驗證不成功，並且可以拒絕用以執行加密操作的請求。在一些實施例中，可以基於所接收的特定類型的身分資訊，使用身分驗證演算法來在128執行身分驗證。在一些實施例中，可以基於加密操作演算法來執行加密操作。如上所述，加密操作可以是加密、解密和/或向資料添加數位簽章。在執行加密操作之後，可以在134輸出操作結果。

如上所述，ICC 100可以在硬體內創建可信環境，以便用戶安全地儲存密碼金鑰並使用金鑰來執行加密操作。例如，ICC 100的用戶可以將多個非對稱金鑰對儲存至ICC 100。在通過身分資訊驗證用戶的身分(例如，生物特徵認證)之後，將每個非對稱金鑰對寫入ICC 100的記憶體。可以基於將從用戶收集的身分資訊與在ICC 100的初始化期間預先儲存的身分資訊進行比較來執行身分認證。如果身分資訊匹配，則可以允許對應的身分資訊和非對稱金鑰對儲存在ICC 100中。

當用戶請求加密操作時，ICC 100可以從記憶體檢索生物特徵資訊和對應的非對稱金鑰對。生物特徵資訊可以用於驗證用戶的身分，並且非對稱金鑰對可以用於在驗證用戶的身分之後執行所請求的加密操作。可以針對各種實

際場景執行加密操作。例如，加密操作可以是將數位簽章添加到區塊鏈交易的操作。在該示例中，節點A可以是區塊鏈網路內的計算設備，其發起用以對與節點B的區塊鏈交易資料進行數位簽章的請求。區塊鏈交易資料可以是節點A與節點B之間的交易資料的經雜湊處理的值。節點A可以使用ICC 100來產生對經雜湊處理的交易資料的數位簽章。為了使用ICC 100，收集從節點A提供的身分資訊，並將其與儲存在ICC 100中的身分資訊進行比較。如果收集的身分資訊與儲存的身分資訊匹配，則可以確定節點A被授權存取和使用ICC 100。可以檢索分配給節點A並且先前儲存在ICC 100的記憶體中的私密金鑰，以產生對經雜湊處理的交易資料的數位簽章。然後，節點A可以將具有數位簽章的經雜湊處理的交易資料發送到節點B。節點B使用分配給節點A的公開金鑰對數位簽章進行解密並提取雜湊值。節點B對訊息進行雜湊處理並比較雜湊值。如果雜湊值相同，則節點B可以確認該訊息確實來自節點A並且未被篡改。

圖2是顯示根據本文的實施例的用於ICC初始化的處理200的示例的流程圖。在一些實施例中，ICC由ICC的用戶初始化。在一些實施例中，用戶可以控制要在ICC中儲存和使用的密碼金鑰以安全地執行加密操作。

在202，重置ICC。在一些實施例中，回應於接收到用以輸入授權身分資訊的請求，重置ICC。在一些實施例中，重置ICC可以包括抹除儲存在ICC的記憶體中的內

容，或將其重新格式化。在一些實施例中，重置ICC還可以包括將ICC的邏輯計算元件的設置重配或重置為預設值。透過重置ICC，可以保證使用一個授權身分資訊來控制輸入到ICC的資訊。此外，先前儲存在ICC中的密碼金鑰被抹除以確保資料安全性。在一些實施例中，ICC是新的ICC並且是第一次使用，ICC可以被初始化以接受授權身分資訊的輸入。如果ICC是新的，則可以初始化ICC以接受授權身分資訊。在一些實施例中，授權身分資訊可以是生物特徵資訊，例如，指紋、聲紋、虹膜資訊和心跳資訊。

在204，ICC接收用以輸入授權身分資訊的請求。在206，調用身分資訊輸入函數以將授權身分資訊輸入到記憶體202。在208，確定ICC的記憶體是否是一次性可程式設計(OTP)記憶體。 OTP記憶體只允許將資料寫入記憶體一次。當用戶向ICC輸入新的授權身分資訊時，可以抹除任何先前儲存的身分資訊和密碼金鑰，以確保新的授權身分不控制先前輸入的密碼金鑰。因此，如果記憶體是OTP，則在212可以對授權身分資訊進行加密並將其輸入到記憶體。否則，在授權身分資訊被加密並輸入到記憶體之前，在210清除記憶體的內容。在212之後，過程200在214結束。

圖3是顯示根據本文的實施例的用於輸入資訊到ICC的處理300的示例的流程圖。在初始化ICC之後，用戶可以基於對其身分資訊進行驗證將密碼金鑰安全地儲存至ICC。

在302，ICC接收用以儲存非對稱金鑰對的請求。在304，接收做出請求的用戶的身分資訊。在一些實施例中，身分資訊可以由與ICC可通訊地耦接的計算設備收集。示例性計算設備可以包括：IoT設備、智慧型手環、智慧型手錶、膝上型電腦(或桌上型電腦)和智慧型手機。在一些實施例中，身分資訊可以是用戶的生物特徵資訊，例如，指紋、聲紋、心跳資訊和虹膜資訊。計算設備可以包括指紋感測器、麥克風、心跳感測器或虹膜掃描器以收集對應的生物特徵資訊。例如，計算設備可以是可以收集可以用作身分資訊的用戶的心跳資訊的智慧型手錶。在收集身分資訊之後，可以將其與用戶的非對稱金鑰對一起發送到ICC。在一些實施例中，ICC可以基於例如藍牙、NFC、Wi-Fi或蜂窩資料的無線通訊協定與計算設備無線地通訊。在一些實施例中，ICC可以插入或整合到計算設備以執行與計算設備的有線通訊。

在306，基於預先儲存在ICC中的授權身分資訊來驗證身分資訊。如果接收到的身分資訊與授權身分資訊匹配，則在308對非對稱金鑰對進行加密並將其儲存至ICC的記憶體。之後，處理300在310結束。如果接收到的身分資訊與授權身分資訊不匹配，則拒絕用以儲存非對稱金鑰對的請求，並且處理300在310結束。在一些實施例中，可以重複處理300，使得授權用戶可以將對應於不同的用戶帳戶或應用的多個密碼金鑰儲存至ICC。在將用戶的密碼金鑰輸入到ICC之後，用戶可以使用ICC來安全地執行加密操

作。

圖4是顯示根據本文的實施例的用於使用ICC執行加密操作的處理400的示例的流程圖。在402，接收用以執行加密操作的請求。加密操作的示例可以包括資料加密、資料解密和添加數位簽章。

在404，接收用戶的身分資訊。如在圖3的描述中所討論的那樣，身分資訊可以由計算設備收集並發送到ICC。在406，可以驗證身分資訊。在一些實施例中，可以將身分資訊與儲存在ICC的記憶體中的身分資訊進行比較。如果身分資訊與儲存的身分資訊匹配，則驗證成功，隨後可以使用儲存在ICC的記憶體中的用戶的密碼金鑰在408執行所請求的加密操作。例如，如果密碼金鑰是非對稱金鑰對，則加密操作可以是基於非對稱金鑰對中的公開金鑰的加密操作、基於非對稱金鑰對中的私密金鑰的解密操作或數位簽章產生操作。如果身分資訊與儲存的身分資訊不匹配，則處理400在412結束。在408之後，處理400進行到410，其中返回操作結果。操作結果可以取決於在408執行的加密操作。例如，如果加密操作是檔案加密，則可以返回使用用戶的公開金鑰加密的檔案。類似地，如果加密操作是檔案解密，則可以返回使用用戶的私密金鑰解密的檔案。如果加密操作是添加數位簽章，則可以返回具有由用戶的私密金鑰產生的數位簽章的檔案。在410之後，處理在412結束。

圖5是顯示根據本文的實施例的金鑰管理設備500的示

例的示圖。在一些實施例中，可以由金鑰管理設備500管理由ICC使用以為用戶執行加密操作的密碼金鑰。金鑰管理設備500可以執行金鑰管理504和演算法管理514。金鑰管理504可以包括密碼金鑰的儲存506、寫入508、隨機產生510和刪除512。密碼金鑰可以包括與ICC的主用戶相關聯的用戶金鑰對和與ICC的授權用戶相關聯的密碼金鑰對以執行加密操作。

由演算法管理514管理的演算法可以包括儲存和管理身分驗證演算法516、數位簽章驗證演算法518、加密和解密演算法520以及權杖演算法522。身分驗證演算法516可以用於執行如圖4的步驟406的描述中所討論的身分驗證。數位簽章驗證演算法518可用於執行數位簽章驗證。如圖4的步驟408所討論的，加密和解密演算法520可用於執行所請求的加密操作。例如，如果所請求的加密操作是對用戶檔案的加密操作，則可以執行加密和解密演算法520以從ICC的記憶體檢索用戶的公開金鑰並對用戶檔案進行加密。權杖演算法522可用於管理權杖，該權杖指示對無需驗證用戶身分而執行所請求的加密操作的時間限制或數量限制。在一些實施例中，可以產生權杖並將其臨時儲存在ICC的記憶體中。權杖可以提供以下的授權：執行多次加密操作或在預定時間段內執行加密操作，而無需驗證用戶身分。例如，可以產生權杖以向ICC的用戶提供以下的授權：將數位簽章添加到接下來接收到的五個檔案中或者在接下來的三個小時內接收到的檔案中，無論首先滿足哪個

條件。在一些實施例中，可以在權杖到期或用完時清除權杖並將其從ICC中移除。

在一些實施例中，金鑰管理設備500可以用作ICC的備份。即使ICC丟失或被破壞，也可以從金鑰管理設備500檢索用於執行加密操作的密碼金鑰和演算法。

在一些實施例中，金鑰管理設備500還可以執行輸入管理524。金鑰管理設備500可以可通訊地耦接到ICC以管理演算法輸入526、身分資訊輸入528、密碼金鑰輸入530、數位簽章產生532和身分驗證534。

圖6描繪了可以根據本文的實施例執行的方法600的示例。為了清楚呈現，下面的描述在本文中的其他圖式的上下文中總體上描述了方法600。然而，應當理解，方法600可以例如由適當的任何系統、環境、軟體和硬體，或者系統、環境、軟體和硬體的組合來執行。在一些實施例中，方法600的各個步驟可以並行、組合、迴圈或以任何順序運行。在一些實施例中，方法600可以由根據本文的實施例描述的ICC執行。

在602，接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至ICC上的記憶體中的請求。在一些實施例中，在ICC的初始化期間將預先儲存的生物特徵資訊儲存至記憶體中。公有授權金鑰和私有授權金鑰是分配給ICC的主用戶的非對稱金鑰對。在一些實施例中，ICC的初始化包括：儲存身分認證碼，所述身分認證碼可執行以基於預先儲存的生物特徵資訊來認證用戶。在一些實施例

中，ICC的初始化還包括：儲存可執行以基於用戶金鑰對添加數位簽章的第一加密操作碼；以及儲存可執行以基於用戶金鑰對執行檔案加密或檔案解密的第二加密操作碼。

在一些實施例中，用以儲存用戶金鑰對的請求是第一請求，生物特徵資訊是第一生物特徵資訊，並且，方法600還包括：接收第二生物特徵資訊和用以向檔案添加數位簽章的第二請求；基於第二生物特徵資訊與預先儲存的生物特徵資訊匹配來認證第二請求可信；並且基於第一加密操作碼和用戶金鑰對中的私密金鑰將數位簽章添加到檔案。在一些實施例中，身分資訊是與用戶相關聯的生物特徵資訊。在一些實施例中，方法600還包括：接收第三生物特徵資訊和用以對檔案進行加密或解密的第三請求；基於第三生物特徵資訊與預先儲存的生物特徵資訊匹配來認證用戶可信；以及基於第三請求、第二加密操作碼以及用戶金鑰對中的公開金鑰或私密金鑰來執行加密或解密。

在一些實施例中，基於生物特徵識別，將與用戶相關聯的生物特徵資訊和預先儲存的生物特徵資訊進行比較；並且生物特徵識別包括指紋識別、聲紋識別、虹膜掃描、面部識別和心跳識別中的一個或多個。

在604，將與用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較。在一些實施例中，記憶體是可程式設計唯讀記憶體(PROM)、電可抹除PROM或快閃記憶體，並且身分資訊和用戶金鑰對儲存在記憶體的單獨儲存單元中。

在606，回應於確定與用戶相關聯的生物特徵資訊與預先儲存的生物特徵資訊匹配，對用戶金鑰對進行加密以提供加密的用戶金鑰對。

在608，將加密的用戶金鑰對儲存至記憶體。

圖7描繪了根據本文的實施例的裝置700的模組的示例。裝置700可以是ICC的實施例的示例。裝置700可以對應於上述實施例，並且裝置700包括以下：

請求接收模組702，用於接收與用戶相關聯的生物特徵資訊以及用以將用戶金鑰對儲存至ICC上的記憶體的請求。身分資訊比較模組704，用於將與用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較。加密模組706，用於回應於確定和用戶相關聯的生物特徵資訊與預先儲存的生物特徵資訊匹配，對用戶金鑰對進行加密以提供加密的用戶金鑰對。儲存模組708，用於將身分資訊和用戶金鑰對儲存至記憶體。

在可選實施例中，在ICC的初始化期間將預先儲存的生物特徵資訊儲存在記憶體中。在可選實施例中，ICC的初始化包括：儲存身分認證碼，所述身分認證碼可執行以基於預先儲存的生物特徵資訊來認證用戶。在可選實施例中，ICC的初始化包括：儲存可執行以基於用戶金鑰對添加數位簽章的第一加密操作碼；以及儲存可執行以基於用戶金鑰對執行檔案加密或檔案解密的第二加密操作碼。

在可選實施例中，記憶體是可程式設計唯讀記憶體

(PROM)、電可抹除PROM或快閃記憶體，並且生物特徵資訊和用戶金鑰對儲存在記憶體的單獨儲存單元中。

前述實施例中顯示的系統、裝置、模組或單元可以透過使用電腦晶片或實體來實施，或者可以透過使用具有特定功能的產品來實施。典型的實施設備是電腦，並且電腦可以是個人電腦、膝上型電腦、蜂巢式電話、照相手機、智慧型手機、個人數位助理、媒體播放機、導航設備、電子郵件收發、遊戲控制台、平板電腦、穿戴式設備或這些設備的任意組合。

對於裝置中每個模組的功能和角色的實施過程，可以參考前一方法中對應步驟的實施過程。為簡單起見，這裡省略了細節。

由於裝置實施基本上對應於方法實施，對於相關部件，可以參考方法實施中的相關描述。先前描述的裝置實施僅是示例。被描述為單獨部分的模組可以或不是物理上分離的，並且顯示為模組的部分可以是或不是物理模組，可以位於一個位置，或者可以分佈在多個網路模組上。可以基於實際需求來選擇一些或所有模組，以實現本文額解決的目標。本領域普通技術人員無需創造性的努力即可理解和實現本申請的實施例。

本文中描述的技術產生若干技術效果。例如，主題的實施例允許ICC的用戶儲存多個密碼金鑰來安全地執行加密操作。可以基於對用戶的身分資訊進行驗證將密碼金鑰儲存至ICC。如果身分資訊驗證失敗，則ICC將拒絕密碼

金鑰資訊輸入。

為了請求ICC執行加密操作，需要收集用戶的身分資訊，並且該收集的身分資訊需要被先前認證並儲存在ICC中的身分資訊驗證為可信。這樣，可以確保請求加密操作的用戶是密碼金鑰的用戶。

此外，可以在將身分資訊和密碼金鑰儲存至ICC的記憶體之前對身分資訊和密碼金鑰進行加密。該資訊僅在ICC中解密以執行對應的身分驗證和加密操作。加密操作在ICC內部執行，並且僅操作結果從ICC輸出。因此，ICC的用戶的身分資訊和密碼金鑰是安全的，即使ICC被駭客攻擊或進行逆向工程也不會被洩露。在一些實施例中，金鑰管理設備可用於以密文儲存身分資訊和密碼金鑰以向ICC提供備份並進一步增強資料安全性。

計算設備可用於收集用戶身分資訊並發起對加密操作的請求。ICC可以透過各種通訊協定與計算設備無線地通訊，或者它可以整合或插入到計算設備中以便容易地用於安全的加密操作。

本文中描述的主題、動作以及操作的實施例可以在數位電子電路、有形體現的電腦軟體或韌體、電腦硬體中實現，包括本文中公開的結構及其結構等同物，或者它們中的一個或多個的組合。本文中描述的主題的實施例可以實現為一個或多個電腦程式，例如，一個或多個電腦程式指令模組，編碼在電腦程式載體上，用於由資料處理裝置執行或控制資料處理裝置的操作。載體可以是有形的非暫態

電腦儲存媒體。例如，電腦程式載體可以包括一個或多個電腦可讀儲存媒體，其具有編碼或儲存在其上的指令。載體可以是有形的非暫態電腦可讀媒體，例如磁片、磁光碟或光碟、固態驅動器、隨機存取記憶體(RAM)、唯讀記憶體(ROM)或其他媒體類型。可選地或附加地，載體可以是人工產生的傳播信號，例如，機器產生的電、光或電磁信號，其被產生來編碼資訊用於傳輸到合適的接收器裝置以供資料處理裝置執行。電腦儲存媒體可以是或部分是機器可讀存放裝置、機器可讀儲存基板、隨機或串列存取記憶體設備或它們中的一個或多個的組合。電腦儲存媒體不是傳播信號。

電腦程式也可以被稱為或描述為程式、軟體、軟體應用程式、app、模組、軟體模組、引擎、腳本或碼，可以以任何形式的程式設計語言編寫，包括編譯或演繹性語言、說明或程式性語言；它可以配置為任何形式，包括作為獨立程式，或者作為模組、元件、引擎、副程式或適合在計算環境中執行的其他單元，該環境可包括由通訊資料網路互聯的在一個或多個位置的一台或多台電腦。

電腦程式可以但非必須對應於檔案系統中的檔案。電腦程式可以儲存在：保存其他程式或資料的檔案的一部分中，例如，儲存在標記語言文檔案中的一個或多個腳本；專用於所討論的程式的單個檔案；或者多個協調檔案，例如，儲存一個或多個模組、副程式或碼部分的多個檔案。

舉例來說，用於執行電腦程式的處理器包括通用微處

理器和專用微處理器，以及任何類型的數位電腦的任何一個或多個處理器。通常，處理器將從耦接到處理器的非暫態電腦可讀媒體接收用於執行的電腦程式的指令以及資料。

術語“資料處理裝置”包括用於處理資料的所有類型的裝置、設備和機器，包括例如可程式設計處理器、電腦或者多處理器或電腦。資料處理裝置可以包括專用邏輯電路，例如FPGA(現場可程式設計閘陣列)、ASIC(專用積體電路)或GPU(圖形處理單元)。除了硬體，該裝置還可以包括為電腦程式創建執行環境的碼，例如，構成處理器韌體、協定棧、資料庫管理系統、作業系統或者它們中的一個或多個的組合的碼。

本文中描述的處理和邏輯流程可由一個或多個電腦或處理器執行一個或多個電腦程式進行，以進行透過對輸入資料進行運算並產生輸出的操作。處理和邏輯流程也可以由例如FPGA、ASIC、GPU等的專用邏輯電路或專用邏輯電路與一個或多個程式設計電腦的組合來執行。

適合於執行電腦程式的電腦可以基於通用和/或專用微處理器，或任何其他種類的中央處理單元。通常，中央處理單元將從唯讀記憶體和/或隨機存取記憶體接收指令和資料。電腦的元件可包括用於執行指令的中央處理單元以及用於儲存指令和資料的一個或多個記憶體設備。中央處理單元和記憶體可以補充有專用邏輯電路或整合在專用邏輯電路中。

通常，電腦還將包括或可操作地耦接至一個或多個大型存放區設備，以從一個或多個大型存放區設備接收資料或將資料傳輸到一個或多個大型存放區設備。大型存放區設備可以是例如磁片、磁光碟或光碟、固態驅動器或任何其他類型的非暫態電腦可讀媒體。但是，電腦不需要具有這樣的設備。因此，電腦可以耦接到本地和/或遠端的例如一個或多個記憶體的一個或多個大型存放區設備。例如，電腦可以包括作為電腦的元件的一個或多個本機存放區器，或者電腦可以耦接到雲端網路中的一個或多個遠端存放器。此外，電腦可以嵌入在另一個設備中，例如行動電話、個人數位助理(PDA)、移動音訊或視頻播放機、遊戲控制台、全球定位系統(GPS)接收器或例如通用序列匯流排(USB)快閃記憶體驅動器的可攜式存放裝置，僅舉幾例。

元件可以透過直接地或經由一個或多個中介軟體例如可交換地電或光地彼此連接而彼此“耦接”。如果其中一個元件整合到另一個元件中，元件還可以彼此“耦接”。例如，整合到處理器中的儲存元件(例如，L2快取記憶體元件)被“耦接到”處理器。

為了提供與用戶的交互，本文中描述的主題的實施例可以在電腦上實現或配置為與該電腦通訊，該計算機具有：顯示裝置，例如，LCD(液晶顯示器)監視器，用於向用戶顯示資訊；以及輸入裝置，用戶可以透過該輸入裝置向該電腦提供輸入，例如鍵盤和例如滑鼠、軌跡球或觸控

板等的指標裝置。其他類型的設備也可用於提供與用戶的交互；例如，提供給用戶的回饋可以是任何形式的感官回饋，例如視覺回饋、聽覺回饋或觸覺回饋；並且可以接收來自用戶的任何形式的輸入，包括聲音、語音或觸覺輸入。此外，電腦可以透過向用戶使用的設備發送文檔案和從用戶使用的設備接收文檔案來與用戶交互；例如，透過向用戶設備上的web瀏覽器發送web頁面以回應從web瀏覽器收到的請求，或者透過與例如智慧型電話或電子平板電腦等的用戶設備上運行的應用程式(app)進行交互。此外，電腦可以透過向個人設備(例如，運行訊息應用的智慧型手機)輪流發送文本訊息或其他形式的訊息並接收來自用戶的回應訊息來與用戶交互。

本文使用與系統、裝置和電腦程式元件有關的術語“配置為”。對於被配置為執行特定操作或動作的一個或多個電腦的系統，意味著系統已經在其上安裝了在運行中促使該系統執行所述操作或動作的軟體、韌體、硬體或它們的組合。對於被配置為執行特定操作或動作的一個或多個電腦程式，意味著一個或多個程式包括當被資料處理裝置執行時促使該裝置執行所述操作或動作的指令。對於被配置為執行特定操作或動作的專用邏輯電路，意味著該電路具有執行所述操作或動作的電子邏輯。

雖然本文包含許多具體實施細節，但是這些不應被解釋為由申請專利範圍本身限定的對要求保護的範圍的限制，而是作為對特定實施例的具體特徵的描述。在本文多

個單獨實施例的上下文中描述的多個特定特徵也可以在單一實施例中的組合實現。相反，在單一實施例的上下文中描述的各種特徵也可以單獨地或以任何合適的子組合在多個實施例中實現。此外，儘管上面的特徵可以描述為以某些組合起作用並且甚至最初如此要求保護，但是在一些情況下，可以從要求保護的組合中刪除來自該組合的一個或多個特徵，並且可以要求保護指向子組合或子組合的變體。

類似地，雖然以特定順序在圖式中描繪了操作並且在申請專利範圍中敘述了操作，但是這不應該被理解為：為了達到期望的結果，要求以所示的特定順序或依次執行這些操作，或者要求執行所有顯示的操作。在一些情況下，多工和並行處理可能是有利的。此外，上述實施例中的各種系統模組和元件的劃分不應被理解為所有實施例中都要求如此劃分，而應當理解，所描述的程式元件和系統通常可以一起整合在單個軟體產品或者打包成多個軟體產品。

已經描述了主題的特定實施例。其他實施例在以下申請專利範圍的範圍內。例如，申請專利範圍中記載的動作可以以不同的循序執行並且仍然實現期望的結果。作為一個示例，圖式中描繪的處理無需要求所示的特定順序或次序來實現期望的結果。在一些情況下，多工和並行處理可能是有利的。

【符號說明】

100:身分加密晶片(ICC)

102:記憶體

104:邏輯計算元件

110:步驟

112:步驟

114:步驟

116:步驟

118:步驟

122:步驟

124:步驟

126:步驟

128:步驟

130:步驟

132:步驟

134:步驟

202:步驟

204:步驟

206:步驟

208:步驟

210:步驟

212:步驟

214:步驟

300:處理

302:步驟

304:步 驟

306:步 驟

308:步 驟

310:步 驟

400:處 理

402:步 驟

404:步 驟

406:步 驟

408:步 驟

410:步 驟

412:步 驟

500:金 鑰 管 理 設 備

504:步 驟

506:步 驟

504:金 鑰 管 理

506:儲 存

508:寫 入

510:隨 機 產 生

512:刪 除

514;演 算 法 管 理

516:身 分 驗 證 演 算 法

518:數 位 簽 章 驗 證 演 算 法

520:加 密/解 密 演 算 法

522:權 杖 演 算 法

524:輸入管理

526:演算法輸入

528:身分資訊輸入

530:密碼金鑰輸入

532:數位簽章

534:身分驗證

600:步驟

602:步驟

604:步驟

606:步驟

608:步驟

700:裝置/身分加密晶片

702:接收模組

704:數位簽章認證模組

706:加密模組

708:儲存模組

【發明申請專利範圍】

【請求項1】一種電腦實施的用於管理用戶金鑰對的方法，該方法包括：

接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至身分加密晶片(ICC)上的記憶體中的請求；

將與該用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較，其中，在該ICC的初始化期間，將該預先儲存的生物特徵資訊儲存至該記憶體中，其中，該ICC的初始化包括：

儲存第一加密操作碼，該第一加密操作碼能夠執行以基於該用戶金鑰對來添加數位簽章；以及

儲存第二加密操作碼，該第二加密操作碼能夠執行以基於該用戶金鑰對來執行檔案加密或檔案解密；

回應於確定與該用戶相關聯的生物特徵資訊和該預先儲存的生物特徵資訊匹配，對該用戶金鑰對進行加密以提供加密的用戶金鑰對；以及

將該加密的用戶金鑰對儲存至該記憶體中，

其中，用以儲存該用戶金鑰對的請求是第一請求，該生物特徵資訊是第一生物特徵資訊，且其中，該電腦實施的方法還包括：

接收第二生物特徵資訊和用以將數位簽章添加到檔案的第二請求；

基於該第二生物特徵資訊與該預先儲存的生物特

徵資訊匹配來認證該第二請求可信；以及

基於該第一加密操作碼和該用戶金鑰對中的私密金鑰將該數位簽章添加到該檔案。

【請求項2】如請求項1之電腦實施的方法，其中，該ICC的初始化包括：

儲存身分認證碼，該身分認證碼能夠執行以基於該預先儲存的生物特徵資訊來認證該用戶。

【請求項3】如請求項1之電腦實施的方法，還包括：

接收第三生物特徵資訊和用以對檔案進行加密或解密的第三請求；

基於該第三生物特徵資訊與該預先儲存的生物特徵資訊匹配來認證該第三請求可信；以及

基於該第三請求、該第二加密操作碼以及該用戶金鑰對中的公開金鑰或該私密金鑰來執行加密或解密。

【請求項4】如請求項1之電腦實施的方法，其中：

基於生物特徵識別，將與該用戶相關聯的生物特徵資訊和該預先儲存的生物特徵資訊進行比較；以及

該生物特徵識別包括指紋識別、聲紋識別、虹膜掃描、面部識別和心跳識別中的一個或多個。

【請求項5】如請求項1之電腦實施的方法，其中，該記憶體是可程式設計唯讀記憶體(PROM)、電可抹除PROM或快閃記憶體，並且該生物特徵資訊和該用戶金鑰對儲存在該記憶體的單獨儲存單元中。

【請求項6】一種用於管理用戶金鑰對的系統，包

括：

一個或多個電腦；以及

一個或多個電腦記憶體裝置，該電腦記憶體與該一個或多個電腦可互相操作地耦接並且具有有形非暫態機器可讀媒體，其儲存一個或多個指令，當該一個或多個指令由該一個或多個電腦執行時，以執行一個或多個操作，該一個或多個操作包括：

接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至身分加密晶片(ICC)上的記憶體中的請求；

將與該用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊進行比較，其中，在該ICC的初始化期間，將該預先儲存的生物特徵資訊儲存至該記憶體中，其中，該ICC的初始化包括：

儲存第一加密操作碼，該第一加密操作碼能夠執行以基於該用戶金鑰對來添加數位簽章；以及

儲存第二加密操作碼，該第二加密操作碼能夠執行以基於該用戶金鑰對來執行檔案加密或檔案解密；

回應於確定與該用戶相關聯的生物特徵資訊和該預先儲存的生物特徵資訊匹配，對該用戶金鑰對進行加密以提供加密的用戶金鑰對；以及

將該加密的用戶金鑰對儲存至該記憶體中，

其中，用以儲存該用戶金鑰對的請求是第一請求，該生物特徵資訊是第一生物特徵資訊，且其中，該電腦實施

的方法還包括：

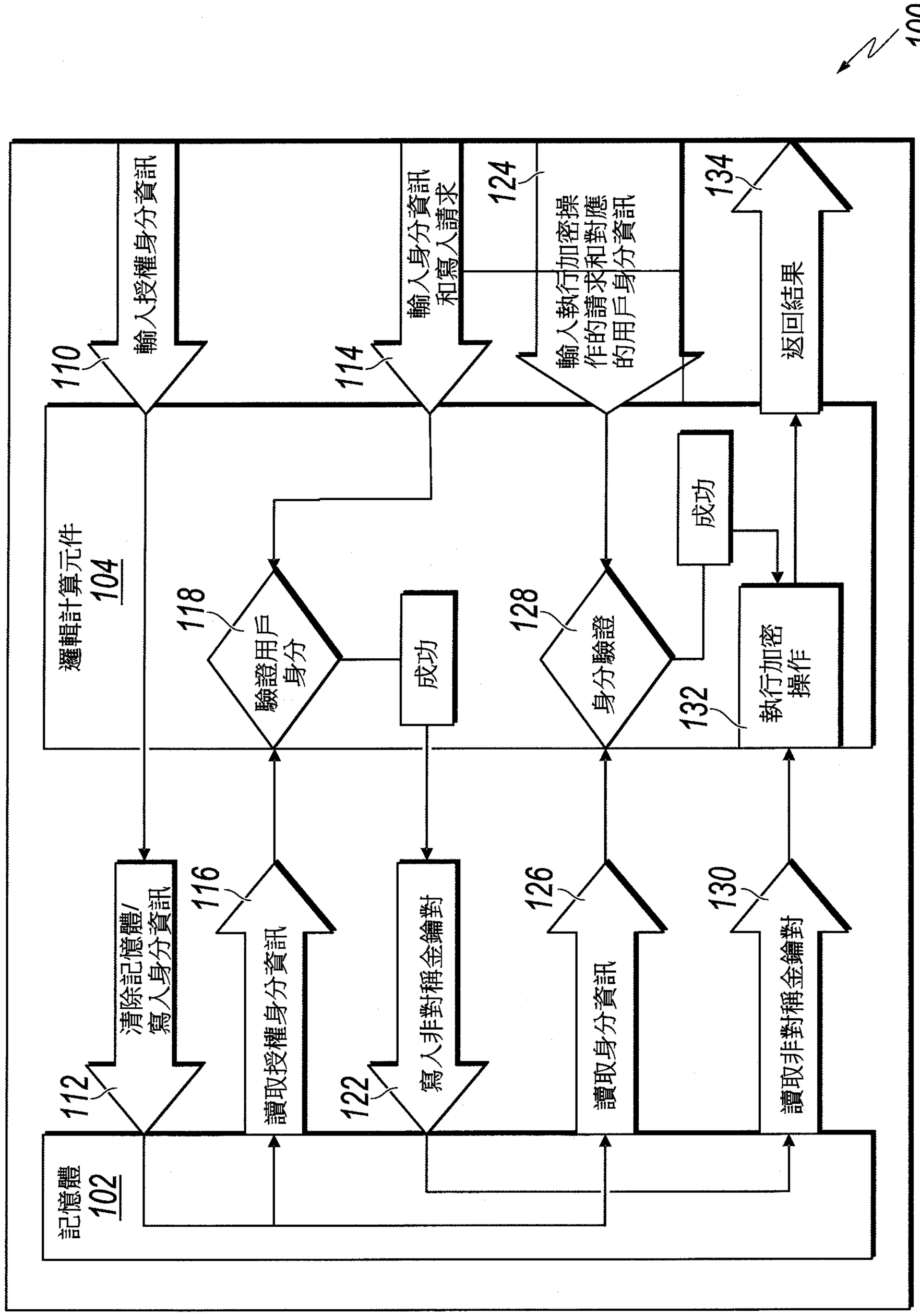
接收第二生物特徵資訊和用以將數位簽章添加到檔案的第二請求；

基於該第二生物特徵資訊與該預先儲存的生物特徵資訊匹配來認證該第二請求可信；以及

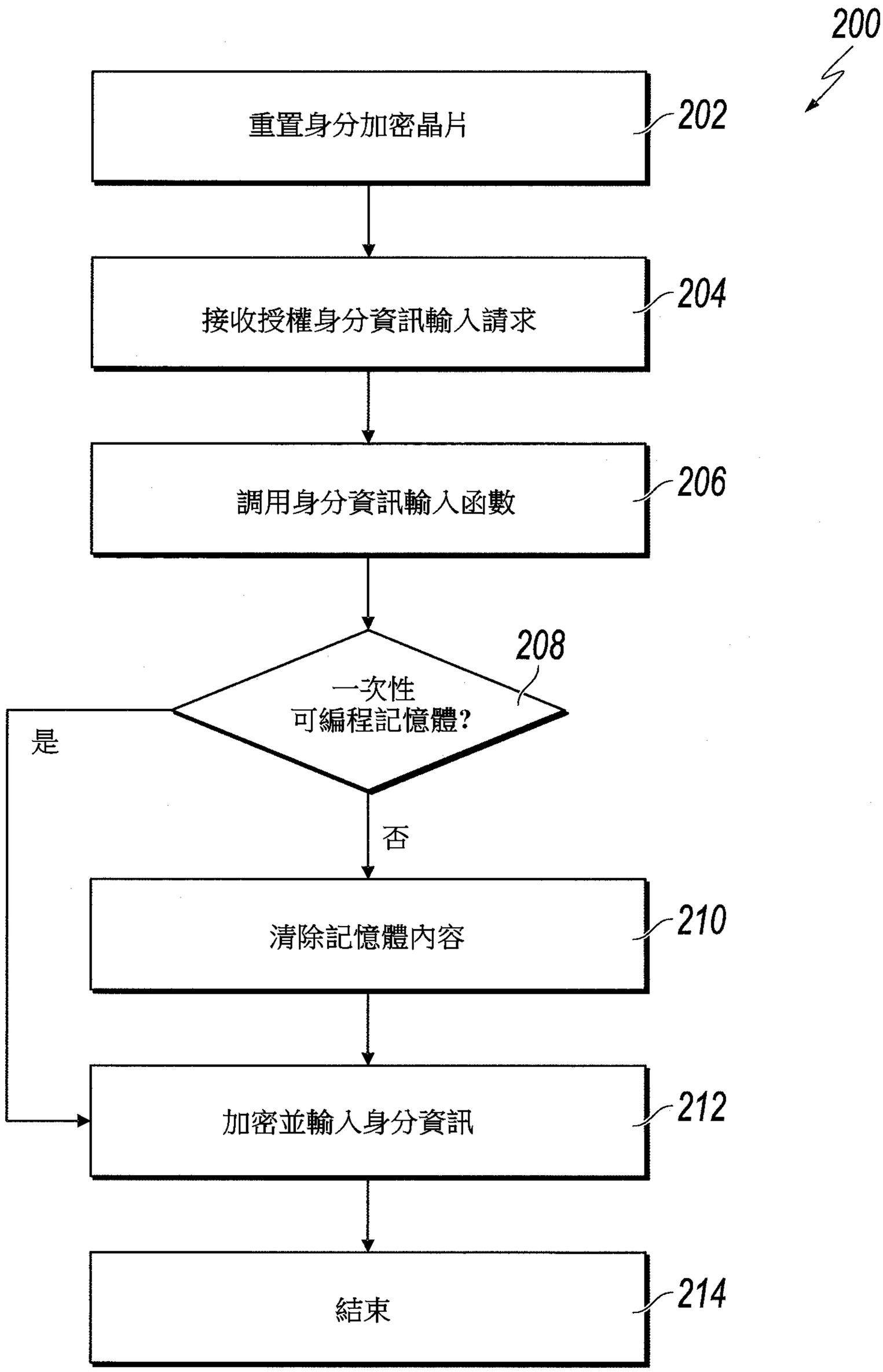
基於該第一加密操作碼和該用戶金鑰對中的私密金鑰將該數位簽章添加到該檔案。

【請求項7】一種用於管理用戶金鑰對的裝置，該裝置包括用於執行如請求項1至5中任一項之方法的多個模組。

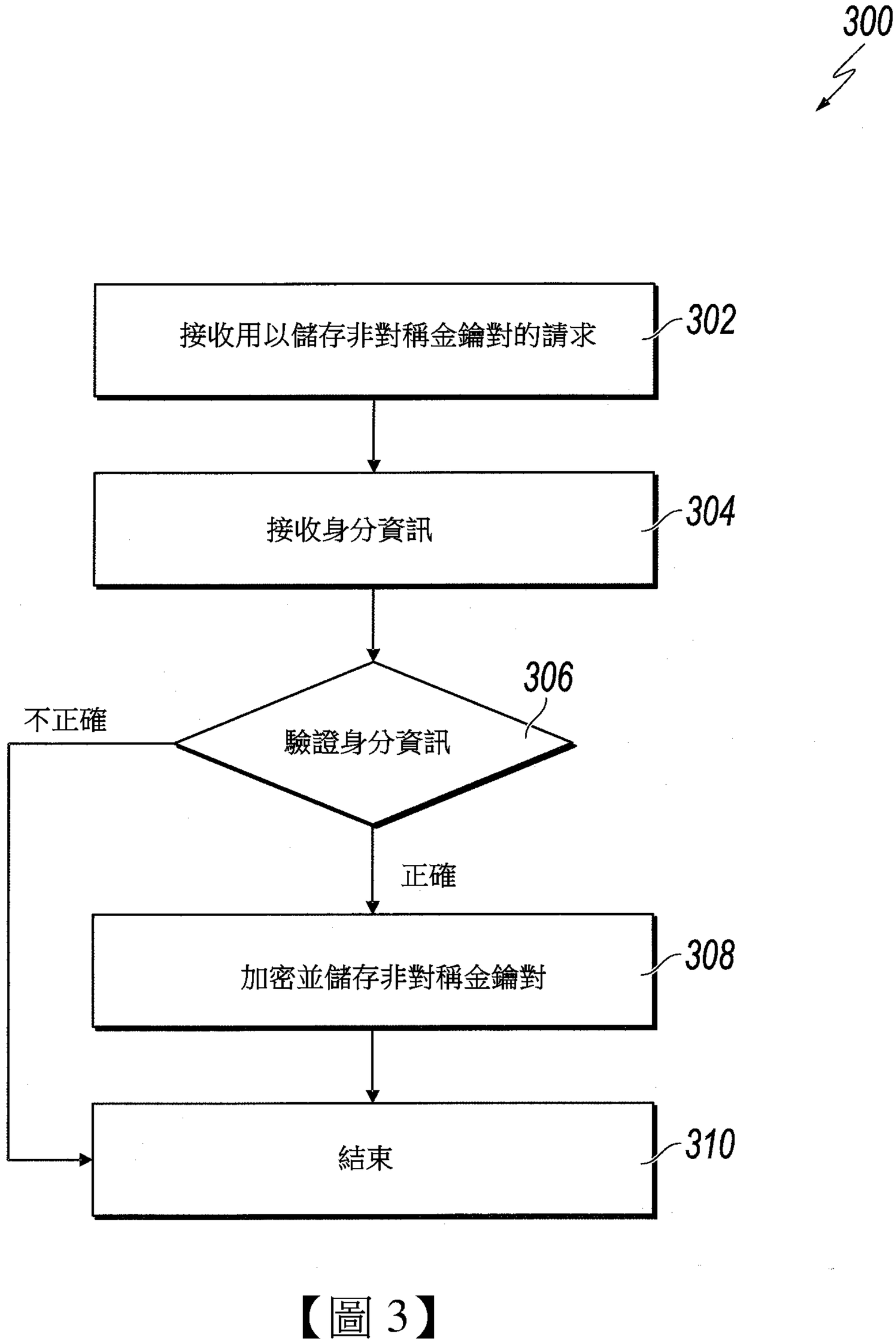
【發明圖式】


100
記憶體 102
邏輯計算元件 104
輸入授權身分資訊 110
清除記憶體/寫入身分資訊 112
讀取授權身分資訊 116
驗證用戶身分 118
成功
輸入身分資訊和寫入請求 114
寫入非對稱金鑰對 122
輸入執行加密操作和對應的用戶身分資訊 124
讀取身分資訊 126
身分驗證 128
成功
讀取非對稱金鑰對 130
執行加密操作 132
返回結果 134

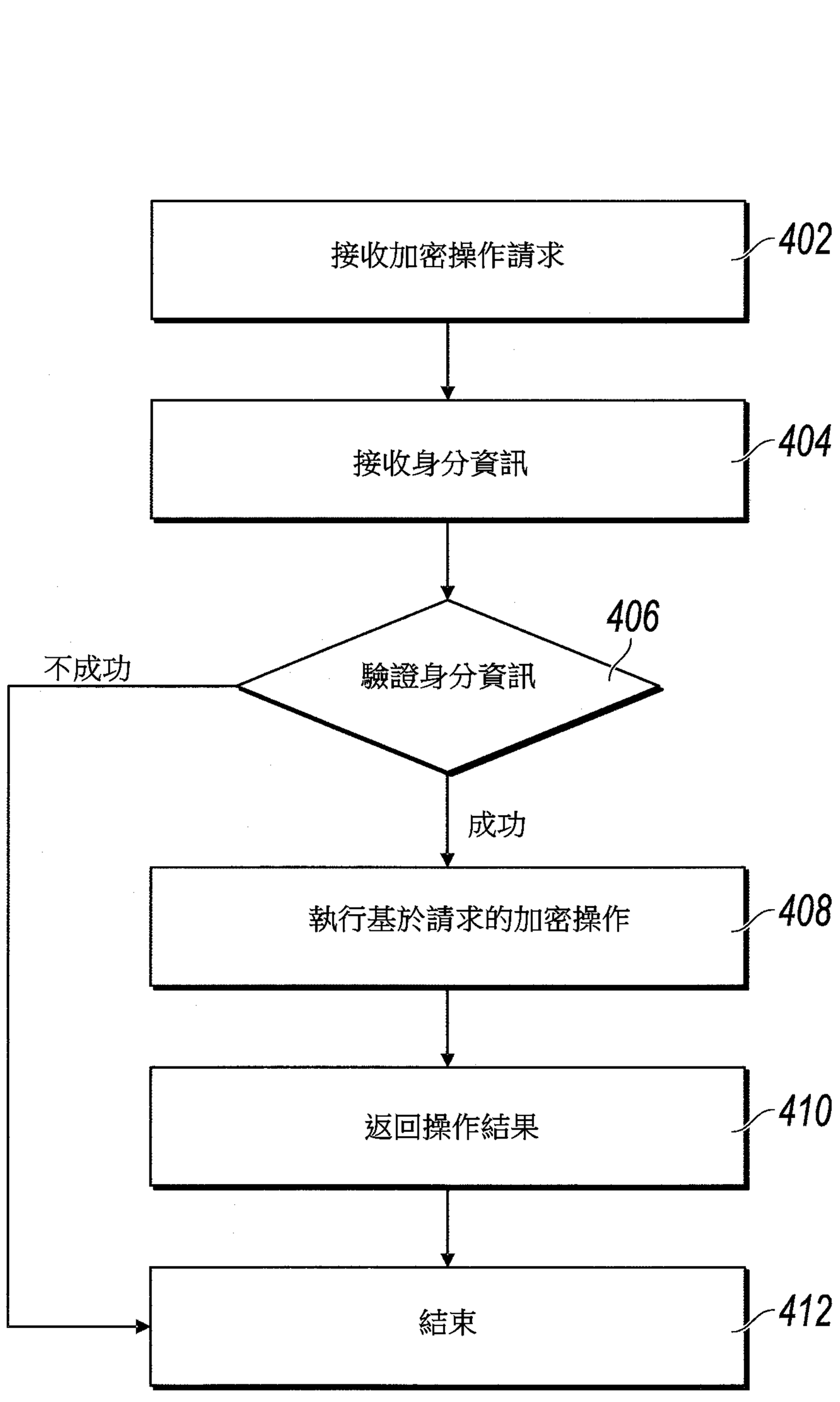
【圖 1】


200
重置身分加密晶片
202
接收授權身分資訊輸入請求
204
調用身分資訊輸入函數
206
一次性
可編程記憶體?
208
是
否
清除記憶體內容
210
加密並輸入身分資訊
212
結束
214

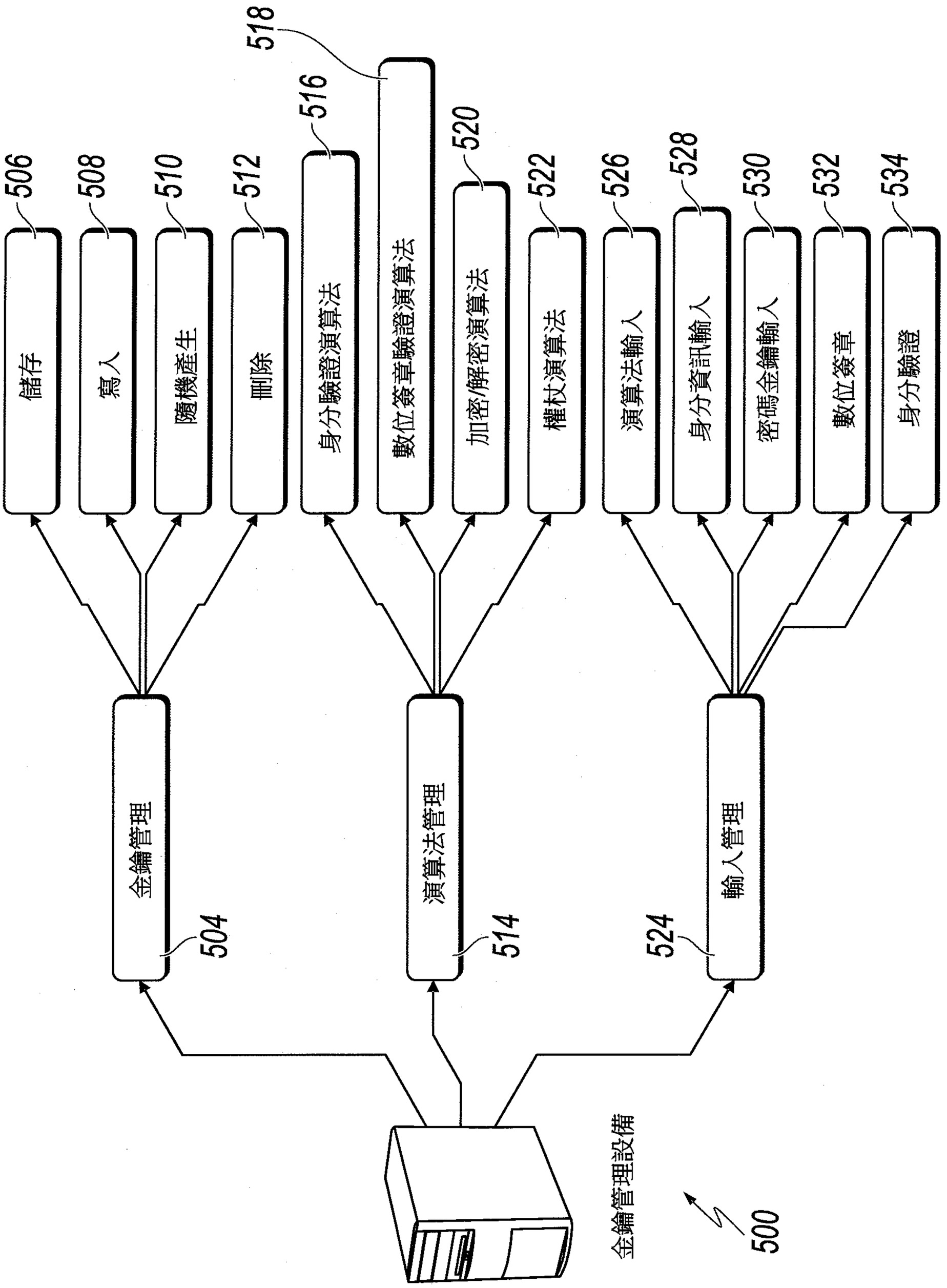
【圖 2】


300
接收用以儲存非對稱金鑰對的請求
302
接收身分資訊
304
306
驗證身分資訊
不正確
正確
加密並儲存非對稱金鑰對
308
結束
310

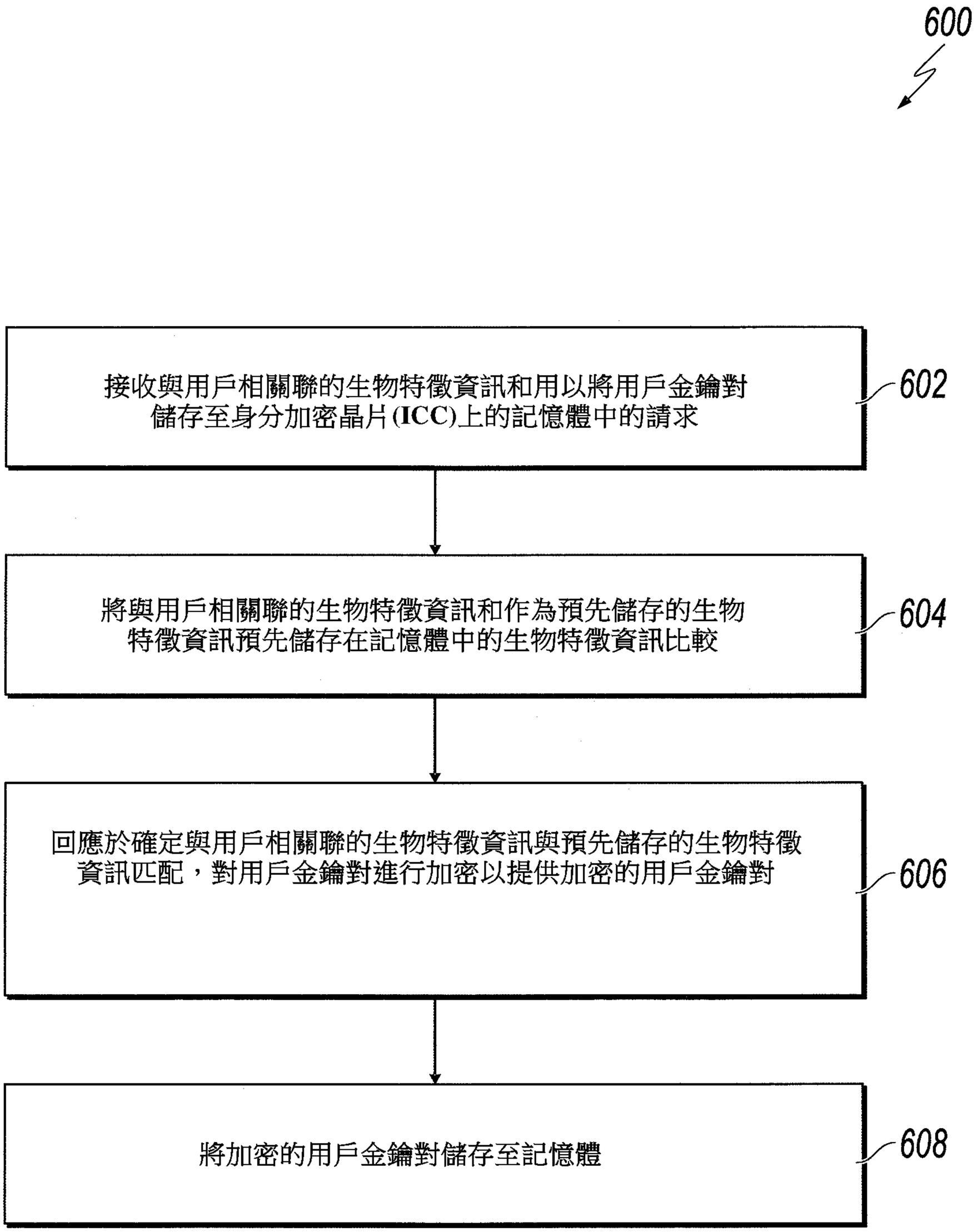
【圖 3】


400
接收加密操作請求
402
接收身分資訊
404
驗證身分資訊
406
不成功
成功
執行基於請求的加密操作
408
返回操作結果
410
結束
412

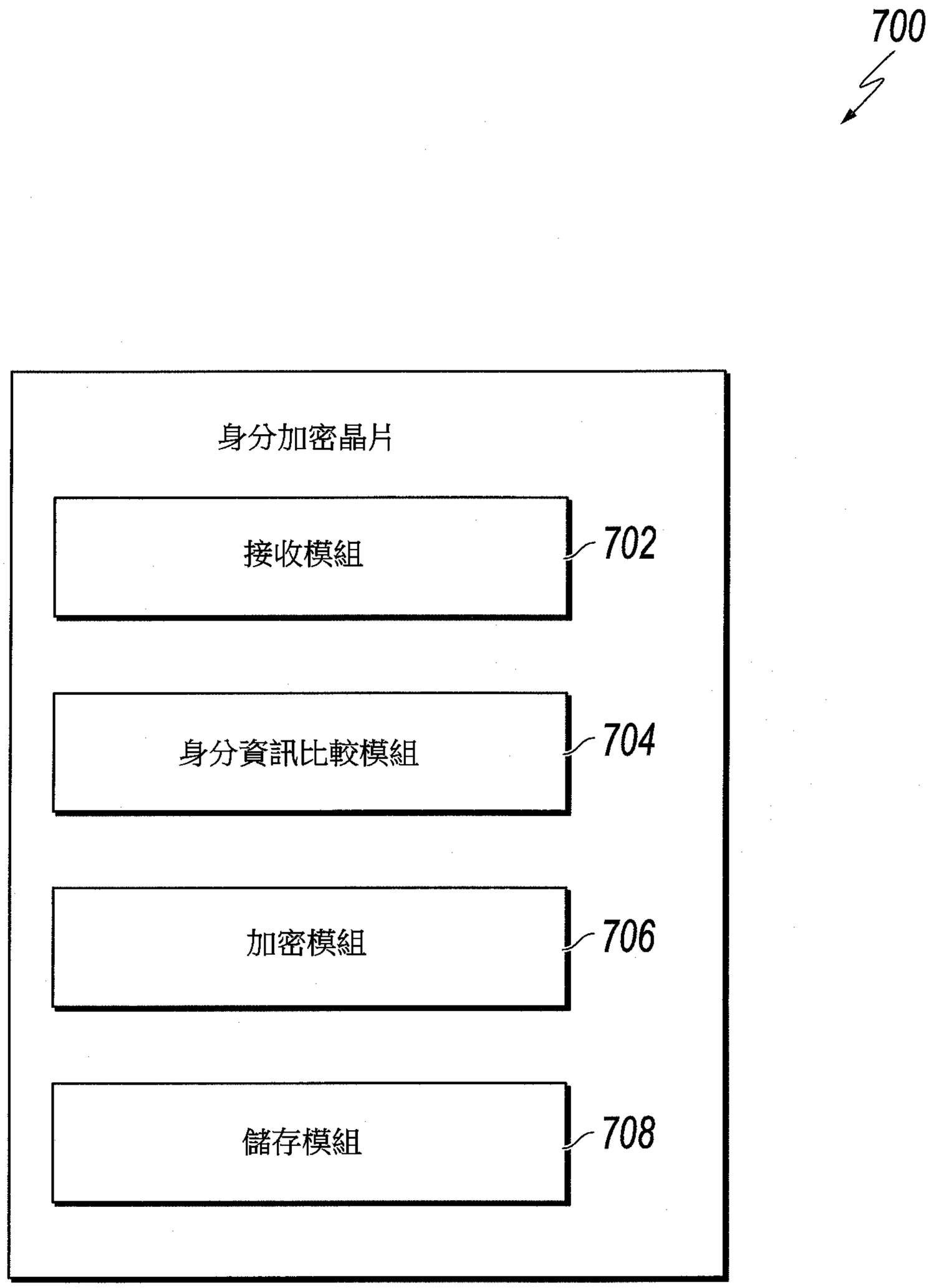
【圖 4】


金鑰管理設備
500
金鑰管理
504
演算法管理
514
輸入管理
524
儲存
506
寫入
508
隨機產生
510
刪除
512
身分驗證演算法
518
數位簽章驗證演算法
516
加密/解密演算法
520
權杖演算法
522
演算法輸入
526
身分資訊輸入
528
密碼金鑰輸入
530
數位簽章
532
身分驗證
534

【圖 5】


600
接收與用戶相關聯的生物特徵資訊和用以將用戶金鑰對儲存至身分加密晶片(ICC)上的記憶體中的請求
602
將與用戶相關聯的生物特徵資訊和作為預先儲存的生物特徵資訊預先儲存在記憶體中的生物特徵資訊比較
604
回應於確定與用戶相關聯的生物特徵資訊與預先儲存的生物特徵資訊匹配，對用戶金鑰對進行加密以提供加密的用戶金鑰對
606
將加密的用戶金鑰對儲存至記憶體
608

【圖 6】



【圖 7】