I724684

(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 I724684 B**

(45)公告日： 中華民國 110 (2021) 年 04 月 11 日

(21)申請案號：108145434　(22)申請日： 中華民國 108 (2019) 年 12 月 12 日

(51)Int. Cl.：　*G06K19/077 (2006.01)*　*G06F21/62 (2013.01)*

(30)優先權：2019/03/29　世界智慧財產權組織　PCT/CN2019/080393

(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	201638798A	TW	201729136A
TW	201810111A	US	2008/0192937A1

審查人員：彭智煇

申請專利範圍項數：10 項　圖式數：6　共 35 頁

(54)名稱

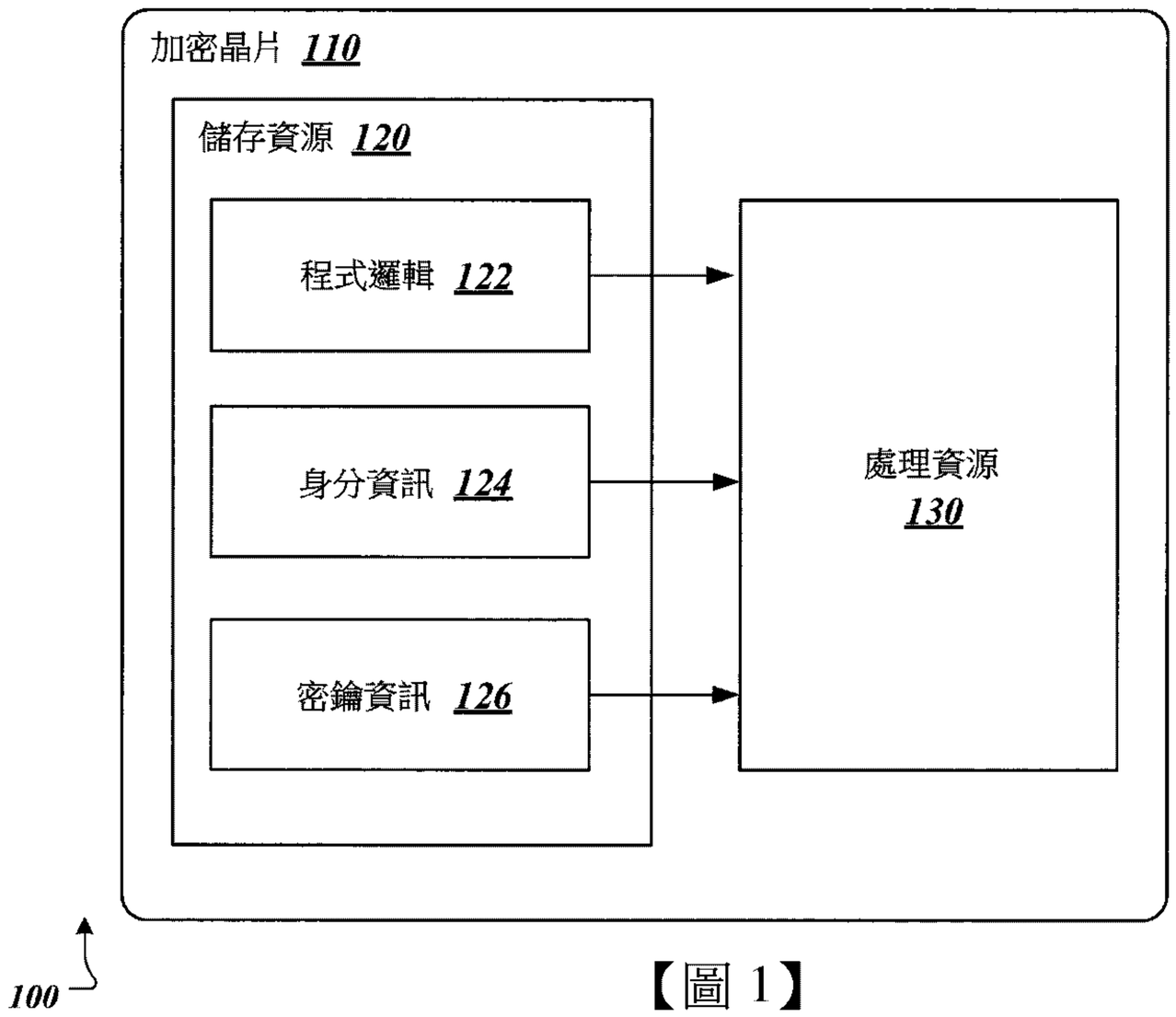
用於執行經過身分驗證的加密操作的方法、系統及裝置

(57)摘要

本文公開了用於執行經過身分驗證的加密操作的方法、系統和裝置，包括編碼在電腦儲存媒介上的電腦程式。其中一種方法包括：由加密晶片從客戶端接收包括客戶端執行所請求的加密操作的請求，其中，該請求包括客戶端身分資訊，並且加密晶片包括處理資源和儲存資源，其中，該處理資源執行加密操作，該儲存資源儲存加密操作中使用的密鑰資訊和與被允許請求加密操作的客戶端相關聯的身分資訊；由加密晶片確定客戶端身分資訊與所述被允許請求加密操作的客戶端之一相關聯；由加密晶片基於儲存在儲存資源中的密鑰資訊執行所請求的加密操作。

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for performing cryptographic operations subject to identity verification. One of the methods includes receiving, by a cryptography chip, a request to perform a requested cryptographic operation from a client including client identity information, wherein the cryptography chip includes a processing resource that performs cryptographic operations and a storage resource that stores key information used in the cryptographic operations, and identity information associated with clients that are permitted to request cryptographic operations; determining, by the cryptography chip, that the client identity information is associated with one of the clients that are permitted to request cryptographic operations; and performing, by the cryptography chip, the requested cryptographic operation based on the key information stored in the storage resource.

指定代表圖：



【圖 1】

符號簡單說明：

110:加密晶片

120:儲存資源

122:程式邏輯

124:身分資訊

126:密鑰資訊

130:處理資源

I724684 第 108145434 號

民國 109 年 11 月 24 日修正

公告本

【發明摘要】

【中文發明名稱】

用於執行經過身分驗證的加密操作的方法、系統及裝置

【英文發明名稱】

METHOD, SYSTEM AND DEVICE FOR PERFORMING CRYPTOGRAPHIC OPERATIONS SUBJECT TO IDENTITY VERIFICATION

【中文】

本文公開了用於執行經過身分驗證的加密操作的方法、系統和裝置，包括編碼在電腦儲存媒介上的電腦程式。其中一種方法包括：由加密晶片從客戶端接收包括客戶端執行所請求的加密操作的請求，其中，該請求包括客戶端身分資訊，並且加密晶片包括處理資源和儲存資源，其中，該處理資源執行加密操作，該儲存資源儲存加密操作中使用的密鑰資訊和與被允許請求加密操作的客戶端相關聯的身分資訊；由加密晶片確定客戶端身分資訊與所述被允許請求加密操作的客戶端之一相關聯；由加密晶片基於儲存在儲存資源中的密鑰資訊執行所請求的加密操作。

第 108145434 號 民國 109 年 11 月 24 日修正

【英文】

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for performing cryptographic operations subject to identity verification. One of the methods includes receiving, by a cryptography chip, a request to perform a requested cryptographic operation from a client including client identity information, wherein the cryptography chip includes a processing resource that performs cryptographic operations and a storage resource that stores key information used in the cryptographic operations, and identity information associated with clients that are permitted to request cryptographic operations; determining, by the cryptography chip, that the client identity information is associated with one of the clients that are permitted to request cryptographic operations; and performing, by the cryptography chip, the requested cryptographic operation based on the key information stored in the storage resource.

【指定代表圖】第(1)圖。
【代表圖之符號簡單說明】

110:加密晶片

120:儲存資源

122:程式邏輯

124:身分資訊

126:密鑰資訊

130:處理資源

【特徵化學式】無

第 108145434 號 民國 109 年 11 月 24 日修正

【發明說明書】

【中文發明名稱】

用於執行經過身分驗證的加密操作的方法、系統及裝置

【英文發明名稱】

METHOD, SYSTEM AND DEVICE FOR PERFORMING CRYPTOGRAPHIC OPERATIONS SUBJECT TO IDENTITY VERIFICATION

【技術領域】

本文涉及執行經過身分驗證的加密操作。

【先前技術】

在一些計算應用中，密碼術用於將資料轉換為在不擁有相關加密密鑰的情況下相當難以破譯以獲得資料原始值的形式。加密密鑰的丟失會致使用該密鑰加密的所有資料都不可恢復。此外，如果加密密鑰被未授權方知道，則因為用該密鑰加密的所有資料都可以被未授權方讀取，因此該資料將不再安全。期望加密密鑰免受丟失或損害，以降低密鑰所有者可能產生的相關經濟損失的風險。

【發明內容】

本文描述了用於執行經過身分驗證的加密操作的技術。這些技術總體上涉及例如與儲存的身分資訊比照來驗

證請求加密操作的客戶端的身分資訊，以及如果驗證成功則執行所請求的加密操作。如果驗證不成功，則不執行及/或拒絕所請求的加密操作。

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介，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介，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請求項，本文的其他特徵和優點將顯而易見。

【圖式簡單說明】

[圖 1] 是示出可用於執行本文的實施例的環境的示例的示圖。

[圖 2] 是示出可用於執行本文的實施例的系統的示例

的示圖。

[圖3]是示出圖2中所示系統的組件之間的交互的示圖。

[圖4]是示出可用於執行本文的實施例的環境的示例的示圖

[圖5]描繪了可以根據本文的實施例執行的處理的示例。

[圖6]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】

本文描述了用於使用加密晶片執行加密操作的技術。在一些計算應用中使用密碼術將資料轉換成在不擁有相關加密密鑰的情況下相當難以破譯以獲得資料的原始值的形式。例如，如果兩個計算設備想要透過允許網路上的所有各方存取資料的公共網路傳送敏感資料，則發送計算設備可以在發送之前將資料加密成密文，並且接收計算設備可以對該密文以恢復資料的原始值進行解密。加密的示例包括但不限於對稱加密和非對稱加密。

對稱加密是指使用單個密鑰既加密(從明文產生密文)又解密(從密文產生明文)的加密處理。在對稱加密中，同一個密鑰被分發給通訊的所有各方，因此每一方都可以對交易資料進行加密和解密。

非對稱加密使用密鑰對，每個密鑰對包括私鑰和公鑰，私鑰由特定方保密，並且公鑰能夠由特定方與其他方自由共享。一方可以使用特定方的公鑰來對資料進行加密，然後該加密的資料可以使用該特定方的私鑰被解密。使用該方的公鑰加密的資料只能使用該方的私鑰解密。此外，私鑰不能從公鑰導出，這允許公鑰被自由地共享。

非對稱加密用於提供數位簽名，這使得接收方能夠確認所接收的資料源自預期的發送方並且未被竄改。數位簽名還可用於確保資料未被竄改(即，其值未被改變)。例如，第一方可以透過首先使用雜湊函數(例如MD5、SHA-256或其他函數)計算資料的雜湊值來對資料集進行數位簽名。然後，第一方使用其私鑰來對雜湊值進行加密並產生數位簽名。然後，第二方可以使用第一方的公鑰來對數位簽名進行解密並恢復雜湊值。然後，第二方使用相同的雜湊函數計算與數位簽名相關聯的資料的雜湊值。如果該雜湊值與從數位簽名中恢復的雜湊值匹配，則第二方知道簽名的第一方使用其私鑰創建了數位簽名，這是因為如果數位簽名是使用不同的密鑰創建的，則當使用相應公鑰對資料進行解密時，它不會產生針對該資料的正確的雜湊值。此外，第二方知道資料自第一方簽名以來未被竄改，這是因為竄改方在不知道私鑰的情況下將無法修改加密的雜湊值以使其與資料的新值匹配。

本文描述了用於使用加密晶片執行加密操作的技術，該加密晶片被配置為保護用於執行操作的密鑰免受損害或

丟失。在一些實施例中，加密晶片包括儲存密鑰資訊(例如，一個或多個加密密鑰)和身分資訊的整合儲存資源。加密晶片接收用以執行加密操作的請求(例如，對資料進行加密、對資料進行解密、產生/驗證數位簽名)。請求包括請求操作的用戶的身分資訊。對於每個請求，加密晶片基於將來自請求的身分資訊與儲存的身分資訊進行比較來驗證請求的用戶的身分。如果請求的用戶的身分被驗證(例如，所接收的身分資訊與所儲存的身分資訊匹配)，則加密晶片執行所請求的加密操作。如果請求的用戶的身分未被驗證(例如，所接收的身分資訊與所儲存的身分資訊不匹配)，則加密晶片不執行所請求的加密操作。雖然本文提供了驗證用戶身分的示例，但是在本文描述的每個示例中，還可以驗證客戶端。客戶端可以是用戶、計算設備、組織或其他類型的實體。

圖1是示出可用於執行本文的實施例的環境100的示例的示圖。如圖所示，環境100包括加密晶片110。加密晶片110包括儲存了程式邏輯122、身分資訊124和密鑰資訊126的儲存資源120。加密晶片110還包括處理資源130。

加密晶片110是被配置為執行加密操作的計算組件(例如，積體電路)。在一些情況下，加密晶片110可以是包括所描繪的組件的積體電路。加密晶片110可以包括由半導體材料(例如矽)構成的基底，所描繪的部件附著在該基底上。在一些情況下，所描繪的組件可以透過導電材料區域(例如，導線或引線)連接，以在組件之間形成電連接。加

密晶片110還可以包括允許其安裝在其他計算系統中並與其他計算系統進行介面連接的連接件(例如，引腳)。

加密晶片110包括儲存資源120。在一些情況下，儲存資源120是允許永久儲存資料的電子儲存設備(即，當設備掉電時儲存的資料不會丟失)。在一些實施例中，儲存資源120可以包括快閃記憶體設備、可程式化唯讀記憶體(PROM)設備、電可抹除可程式化唯讀記憶體(EEPROM)設備或者永久儲存資料並允許資料被抹除和重新程式化的其他類型的儲存設備。

加密晶片110還包括處理資源130。在一些情況下，處理資源130是能夠執行軟體指令的處理器，例如，現場可程式化閘陣列(FPGA)、專用積體電路(ASIC)、單片機、微處理器或其他類型的處理器。

如圖所示，程式邏輯122儲存在儲存資源120中。在一些情況下，程式邏輯122包括將由處理資源130執行的軟體指令。程式邏輯122可包括在被執行以執行與接收到的用以執行加密操作的請求有關的操作時可操作的指令，該加密操作為例如用以解析檢索資料的請求、驗證請求中的身分資訊以及如果身分驗證成功則執行請求的加密操作。在一些情況下，程式邏輯122可以被未加密地儲存，這是因為指令本身可能不包括任何敏感資訊。

儲存資源120還包括表示被允許使用加密晶片110執行加密操作的用戶的身分的身分資訊124。在一些情況下，用以執行發送到加密晶片110的加密操作的請求包括用戶

身分資訊。加密晶片110基於身分資訊124驗證請求加密操作的用戶的身分。如果加密晶片110能夠驗證用戶的身分，則執行所請求的加密操作。如果不能，則不執行所請求的加密操作。針對圖2更詳細地描述該處理。

儲存資源120還包括密鑰資訊126，密鑰資訊126包括由加密晶片110使用以執行加密操作的一個或多個加密密鑰。在一些情況下，加密密鑰可以是對稱密鑰、非對稱密鑰對中的私鑰或者要保密的其他類型的密鑰。在一些實施例中，密鑰資訊126可以以加密的形式儲存，使得在不具有用於解密該資訊的適當密鑰的情況下，不能從儲存資源120讀取密鑰資訊126。針對圖2更詳細地描述該處理。

圖2是示出可用於執行本文的實施例的系統200的示例的示圖。系統200描繪了加密晶片110的一部分，如以上關於圖1所述，該加密晶片110包括儲存在儲存資源120中的身分資訊124和密鑰資訊126。系統200還包括認證模組250和加密模組260。

如圖所示，系統200包括認證模組250，其可操作以驗證包括在所接收的用以執行加密操作的請求中的身分資訊加密。在一些情況下，認證模組250可以是由處理資源130執行的程式邏輯122中定義的軟體模組。在一些實施例中，認證模組250可以是包括在加密晶片110中的獨立硬體組件，例如處理資源130的附加處理器或處理內核。認證模組250還可以是負責執行認證處理的處理資源130的邏輯或實體的劃分。

如圖所示，系統200包括可操作以執行所請求的加密操作的加密模組260。在一些情況下，加密模組260可以是由處理資源130執行的程式邏輯122中定義的軟體模組。在一些實施例中，加密模組260可以是包括在加密晶片110中的獨立硬體組件，例如處理資源130的附加處理器或處理內核。加密模組260還可以是負責執行認證處理的處理資源130的邏輯或實體的劃分。

系統200還包括介面210。介面210為外部組件或用戶提供用於向加密晶片110內的例如認證模組250和加密模組260加密的組件發送和接收資料的機制。在一些實施方式中，介面210是加密晶片110與其已經安裝在其中的系統之間的實體介面，諸如加密晶片110與諸如主板的較大積體電路之間的實體引腳連接。在一些情況下，介面210是軟體層，其向由加密晶片110的處理資源130執行的、或者由安裝了加密晶片的較大系統中的另一處理器執行的程式提供應用程式介面(API)。

在220處的操作中，認證模組250經由介面210從外部組件或程式接收用以執行加密操作的請求。每個請求包括與和請求相關聯的用戶相關聯的身分資訊。在一些情況下，所接收的身分資訊包括請求加密操作的用戶的數位簽名。

在一些情況下，所接收的身分資訊可包括與用戶相關聯的生物識別資訊或其他識別資訊。例如，加密晶片110可以包括指紋掃描儀或其他生物識別設備以從用戶收集生

物識別資訊。為了請求加密操作，用戶觸摸指紋掃描儀，其產生用戶指紋的數位表示。在一些情況下，用戶可以選擇所需的加密操作，例如透過鍵盤或加密晶片110的其他介面。可以由處理資源130產生對所需加密操作的請求，並經由介面210將其傳遞給認證模組250。

認證模組250基於儲存的身分資訊124驗證所接收的身分資訊。在身分資訊包括用戶的數位簽名的情況下，認證模組250可以透過用與用戶關聯的公鑰對簽名進行解密並將解密資料與期望值進行比較來驗證簽名(例如，上述雜湊值驗證)。如果值匹配，則用戶的身分被驗證。如果值不匹配，則用戶的身分未被驗證。在身分資訊是生物識別資訊的情況下，認證模組250將包括在請求中的生物識別資料的數位表示與包括在身分資訊124中的儲存的生物識別資料進行比較。如果接收的生物識別資料與儲存的生物識別資料匹配，則用戶的身分被驗證。如果接收的生物識別資料與儲存的生物識別資料不匹配，則用戶的身分未被驗證。

在一些情況下，如果認證模組250驗證了用戶，則認證模組向加密模組260指示身分資訊已被驗證(在230處)。響應於接收到該指示，加密模組260執行所請求的加密操作並經由介面210將加密結果返回給請求者(240)。在一些情況下，如果認證模組250不能驗證用戶，則加密模組260不執行所請求的加密操作。在一些示例中，由認證模組250、加密模組260或另一組件將拒絕發送給請求者。

由加密模組260執行的加密操作可以包括但不限於對資料進行加密、對資料進行解密、產生數位簽名、驗證數位簽名或其他加密操作。例如，用以執行加密操作的請求可以指示請求解密操作，並且可以包括將使用與請求的用戶相關聯的加密密鑰(例如，私鑰)來解密的密文。在這種情況下，加密模組260可以使用儲存的密鑰資訊126對密文進行解密，並在240處返回密文的解密版本作為加密結果。

圖3是示出圖2中所示系統的組件之間的交互300的示圖。在305處，介面210將包括用戶身分資訊的請求發送到認證模組140，如先前關於圖2所討論的。在310處，認證模組140從儲存資源120檢索加密的身分資訊(例如，用於驗證數位簽名、生物識別資料等的加密密鑰)。在315處，認證模組140對從儲存資源120檢索到的加密的身分資訊進行解密。在一些情況下，還從儲存資源120中檢索用於對所檢索的身分資訊進行解密的密鑰。密鑰還可以包括在認證模組140本身中，例如透過“硬編碼”到儲存在認證模組140或處理資源130的韌體中的軟體指令中。

在320處，認證模組140基於解密的身分資訊來驗證用戶身分資訊，如先前關於圖2所描述的。在325處，認證模組140的執行基於驗證的結果而分支。如果用戶身分未被驗證，則認證模組140經由介面210向請求者返回對請求的拒絕(在330處)。如果用戶身分被驗證，則認證模組140向加密模組150發送用戶身分被驗證的指示(在335處)。

在340處，響應於接收到指示，加密模組150從儲存資源120檢索與用戶相關聯的加密的加密密鑰。在345處，加密模組150對加密密鑰進行解密。在一些情況下，還從儲存資源120檢索用於對所檢索的身分資訊進行解密的密鑰。密鑰還可以被包括在加密模組150本身中，例如透過“硬編碼”到儲存在加密模組150或處理資源130的韌體中的軟體指令中。

還在345處，加密模組150執行所請求的加密操作。在350處，加密模組經由介面210將加密操作的結果返回給請求者。

圖4是示出可用於執行本文的實施例的環境400的示例的示圖。如圖所示，環境400包括包含加密晶片110的身分資訊卡410。身分資訊卡410可通訊地耦接到電腦420、智慧手機430、平板設備440和物聯網(IOT)設備450。

在操作中，身分資訊卡410與各種設備420、430、440和450通訊。該通訊可以透過例如近場通訊(NFC)協定、藍牙(BLUETOOTH)、WIFI、蜂巢式協定、紅外通訊協定或其他類型的協定的有線或無線通訊協定進行。在一些情況下，通訊涉及資料的加密及/或解密，例如，使用諸如傳輸層安全性(TLS)的安全通訊協定，對發送到設備420、430、440、450的資料提供數位簽名，驗證由設備420、430、440、450之一提供的數位簽名或使用其他機制。如上所述，如果加密晶片110可以驗證請求的用戶的身分，則這些加密操作將由包括在身分資訊卡410中的加密晶片

110執行。

在一些情況下，身分資訊卡410可以是由用戶攜帶的便攜式設備，例如智慧卡。在一些情況下，如上所述，身分資訊卡可以包括生物識別傳感器，並且用戶可以透過與生物識別傳感器交互來提供身分資訊。在一些情況下，身分資訊卡410可以插入兼容設備中並從該設備被提供電力以執行其操作。在這種情況下，可以透過該設備與身分資訊卡410之間的導電接觸在身分資訊卡410和該設備之間傳輸資料。

圖5是用於執行經過身分驗證的加密操作的處理500的示例的流程圖。為方便起見，處理500將被描述為由位於一個或多個位置並根據本文被適當地程式化的一個或多個電腦的系統執行。例如，如圖1的環境100的加密晶片110的被適當地程式化的加密晶片，可以執行處理500。

在510處，加密晶片從客戶端接收用以執行所請求的加密操作的請求，其中該請求包括與客戶端相關聯的客戶端身分資訊，並且其中加密晶片是包括處理資源和儲存資源的硬體組件，該處理資源執行加密操作，該儲存資源儲存在加密操作中使用的密鑰資訊以及與被允許請求加密操作的客戶端相關聯的身分資訊。在一些情況下，所請求的加密操作是加密操作、解密操作、數位簽名驗證操作或數位簽名產生操作。在一些情況下，加密晶片是現場可程式化閘陣列(FPGA)、專用積體電路(ASIC)或微處理器。

在520處，基於將客戶端身分資訊與儲存在儲存資源

中的身分資訊進行比較，確定客戶端身分資訊與被允許請求加密操作的客戶端之一相關聯。

在530處，響應於確定客戶端身分資訊與被允許請求加密操作的客戶端之一相關聯，基於儲存在儲存資源中的密鑰資訊來執行所請求的加密操作。在一些情況下，請求包括資料，並且加密晶片對資料執行所請求的加密操作。在一些示例中，加密晶片包括由處理資源執行以操作包括加密晶片的電腦系統的操作系統。

在一些情況下，該請求是第一請求，所請求的加密操作是第一請求加密操作，客戶端身分資訊是第一客戶端身分資訊，並且處理500包括從第二客戶端接收執行第二請求加密操作的第二請求，其中，該第二請求包括與第二客戶端相關聯的第二客戶端身分資訊；基於將第二客戶端身分資訊與儲存在儲存資源中的身分資訊比較，確定第二客戶端身分資訊與被允許請求加密操作的客戶端之一無關，其中，響應於確定第二客戶端身分資訊與被允許請求加密操作的客戶端之一無關，加密晶片不執行第二請求的加密操作。

在一些示例中，處理500包括：基於用以執行加密操作的一個或多個請求不包括與被允許請求加密操作的客戶端之一相關聯的客戶端身分資訊來確定該請求是惡意的；並且響應於確定用以執行加密操作的一個或多個請求是惡意的，從儲存資源中清除身分資訊和密鑰資訊。在一些情況下，加密晶片可以基於多個因素確定請求是惡意的，包

括但不限於接收到不能被驗證的請求的頻率、與請求中包括的客戶端身分相關聯的模式(例如，指示攻擊者按順序嘗試不同的身分值以嘗試查找到有效身分)、特定時間量內來自特定客戶端的未被驗證的請求的數量或其他因素。從儲存資源中抹除密鑰資訊和身分資訊以確保攻擊者無法透過任何方式存取此資訊。

在一些實施例中，加密晶片是現場可程式化閘陣列(FPGA)，並且處理500包括接收包括重新程式化資訊以對加密晶片重新程式化的請求；並且響應於接收到請求，用重新程式化資訊替換儲存在儲存資源中的資訊。

圖6是根據本文的實施例的裝置600的模組的示例的示圖。

裝置600可以是用於執行經過身分驗證的加密操作的加密晶片的實施例的示例。裝置600可以對應於上述實施例，並且裝置600包括以下：接收模組602，用於由加密晶片從客戶端接收用以執行所請求的加密操作的請求，其中該請求包括與客戶端相關聯的客戶端身分資訊，並且加密晶片是包括處理資源和儲存資源的硬體組件，其中，該處理資源執行加密操作，該儲存資源儲存加密操作中使用的密鑰資訊和與被允許請求加密操作的客戶端相關聯的身分資訊；確定模組604，用於由加密晶片基於將客戶端身分資訊與儲存在儲存資源中的身分資訊進行比較，確定客戶端身分資訊與被允許請求加密操作的客戶端之一相關聯；以及執行模組606，用於響應於確定客戶端身分資訊與被

允許請求加密操作的客戶端之一相關聯，由加密晶片基於儲存在儲存資源中的密鑰資訊執行所請求的加密操作。

在先前實施例中示出的系統、裝置、模組或模組可以透過使用電腦晶片或實體來實現，或者可以透過使用具有特定功能的產品來實現。典型的實施例設備是電腦，電腦可以是個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧電話、個人數位助理、媒體播放器、導航設備、電子郵件收發設備、遊戲控制台、平板電腦、可穿戴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例處理，可以參考前一方法中相應步驟的實施例處理。為簡單起見，這裡省略了細節。

由於裝置實施例基本上對應於方法實施例，對於相關部分，可以參考方法實施例中的相關描述。先前描述的裝置實施例僅是示例。被描述為單獨部分的模組可以是或不是實體上分離的，並且顯示為模組的部分可以是或不是實體模組，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，以實現本文方案的目標。本領域普通技術人員無需付出創造性勞動就能理解和實現本申請的實施例。

再次參照圖6，它可以被解釋為示出用於執行經過身分驗證的加密操作的加密晶片的內部功能模組和結構。本質上，執行主體可以是電子設備，並且該電子設備包括以下：一個或多個處理器；以及記憶體，其被配置為儲存一

個或多個處理器的可執行指令。

本文中描述的技術產生一個或多個技術效果。在一些實施例中，該技術透過在使用儲存加密密鑰執行所請求的加密操作之前驗證客戶端的身分(例如，透過驗證數位簽名)來為客戶端提供增強的安全性。這提高了安全性，因為它可以防止攻擊者(其身分將不會被驗證)使用客戶端的加密密鑰來解密私有資料、透過偽造客戶端的數位簽名來冒充客戶端、或執行其他有害操作。在一些實施例中，該技術透過響應於檢測到惡意活動而抹除儲存的加密密鑰來提供額外的安全性。這可以防止攻擊者透過向設備發送大量身分以嘗試與儲存的身分匹配以便存取設備的加密功能來對設備執行“強力”攻擊。

所描述的主題的實施例可以單獨或組合地包括一個或多個特徵。例如，在第一實施例中，由加密晶片從客戶端接收用以執行所請求的加密操作的請求，其中請求包括與客戶端相關聯的客戶端身分資訊，並且加密晶片是包括處理資源和儲存資源的硬體組件，其中，該處理資源執行加密操作，該儲存資源儲存在加密操作中使用的密鑰資訊以及與被允許請求加密操作的客戶端相關聯的身分資訊；加密晶片基於將客戶端身分資訊與儲存在儲存資源中的身分資訊比較，確定客戶端身分資訊與被允許請求加密操作的客戶端之一相關聯；並且響應於確定客戶端身分資訊與被允許請求加密操作的客戶端之一相關聯，由加密晶片基於儲存在儲存資源中的密鑰資訊來執行所請求的加密操作。

前述和其他描述的實施例均可以可選地包括以下特徵中的一個或多個：

第一特徵，可與以下特徵中的任一個組合，指定所請求的加密操作是加密操作、解密操作、數位簽名驗證操作或數位簽名產生操作。

第二特徵，可與先前或以下特徵中的任一個組合，指定加密晶片是現場可程式化閘陣列(FPGA)、專用積體電路(ASIC)或微處理器。

第三特徵，可與先前或以下特徵中的任一個組合，指定該請求包括資料，並且加密晶片對資料執行所請求的加密操作。

第四特徵，可與先前或以下特徵中的任一個組合，指定加密晶片包括由處理資源執行以操作包括加密晶片的電腦系統的操作系統。

第五特徵，可與先前或以下特徵中的任一個組合，指定該請求是第一請求，所請求的加密操作是第一請求加密操作，客戶端身分資訊是第一客戶端身分資訊，並且方法包括：由加密晶片從第二客戶端接收用以執行第二請求加密操作的第二請求，其中，該第二請求包括與第二客戶端相關聯的第二客戶端身分資訊；由加密晶片基於將第二客戶端身分資訊與儲存資源中儲存的身分資訊比較，確定第二客戶端身分資訊與被允許請求加密操作的客戶端之一無關，其中，響應於確定第二客戶端身分資訊與被允許請求加密操作的客戶端之一無關，加密晶片不執行第二請求的

加密操作。

第六特徵，可與先前或以下特徵中的任一個組合，指定該方法包括：由加密晶片基於用以執行加密操作的一個或多個請求不包括與被允許請求加密操作的客戶端之一相關聯的客戶端身分資訊，確定該請求是惡意的；響應於確定執行加密操作的一個或多個請求是惡意的，由加密晶片從儲存資源清除身分資訊和密鑰資訊。

第七特徵，可與先前或以下特徵中的任一個組合，指定加密晶片是現場可程式化閘陣列(FPGA)，並且該方法包括：由加密晶片接收包括重新程式化資訊以對加密晶片重新程式化的請求；並且響應於接收到該請求，由加密晶片用重新程式化資訊替換儲存在儲存資源中的資訊。

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介。例如，電腦程式載體可以包括一個或多個電腦可讀儲存媒介，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介，例如磁碟、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)或其他媒介類型。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。電腦儲存媒介可以是或部分是機器可讀儲存設備、機器可讀儲存基板、隨機或序列存取記憶體設備或它們中的一個或多個的組合。電腦儲存媒介不是傳播信號。

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、腳本或代碼，可以以任何形式的程式化語言編寫，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、組件、引擎、子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文件系統中的文件。電腦程式可以儲存在：保存其他程式或資料的文件的一部分中，例如，儲存在標記語言文檔中的一個或多個腳本；專用於所討論的程式的單個文件；或者多個協調文件，例如，儲存一個或多個模組、子程式或代碼部分的多個文件。

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介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，包括例如可程式化處理器、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(現場可程式化閘陣列)、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代碼，例如，構成處理器韌體、協定棧、資料庫管理系統、操作系統或者它們中的一個或多個的組合的代碼。

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化電腦的組合來執行。

適合於執行電腦程式的電腦可以基於通用及/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及/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容量儲存設備，以從一個或多個大容量儲存設備接收資料或將資料傳輸到一個或多個大容量儲存設備。大容量儲存設備可以是例如磁碟、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介。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及/或遠端的例如一個或多個記憶體的一個或多個大容量儲存設備。例如，電腦可以包括作為電腦的組件的一個或多個本地記憶體，或者電腦可以耦接到雲網路中的一個或多個遠端記憶體。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)、行動音訊或視訊播放器、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便攜式儲存設備，僅舉幾例。

組件可以透過直接地或經由一個或多個中間件例如可交換地電或光地彼此連接而彼此“耦接”。如果其中一個組件整合到另一個組件中，組件還可以彼此“耦接”。例如，整合到處理器中的儲存組件(例如，L2高速緩存組件)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，該電腦具有：顯示設備，例如，LCD(液晶顯示器)監視器，用於向用戶顯示資訊；以及輸入設備，用戶可以透過該輸入設備向該電腦提供輸入，例如鍵盤和例如滑鼠、軌跡球或觸摸板等的指針設備。其他類型的設備也可用於提供與用戶的交互；例如，提供給用戶的反饋可以是任何形式的感官反饋，例如視覺反饋、聽覺反饋或觸覺反饋；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和從用戶使用的設備接收文檔來與用戶交互；例如，透過向用戶設備上的web瀏覽器發送web頁面以響應從web瀏覽器收到的請求，或者透過與例如智慧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響應訊息來與用戶交互。

本文使用與系統、裝置和電腦程式組件有關的術語“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請求項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個實施例中的組合實現。相反，在單個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請求項中敘述了操作，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，或者要求執行所有示出的操作。在一些情況下，多任務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組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，所描述的程式組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。其他實施例在以下請求項的範圍內。例如，請求項中記載的動作可以以不同的順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，多任務和並行處理可能是有利的。

【符號說明】

100:環境

110:加密晶片

120:儲存資源

122:程式邏輯

124:身分資訊

126:密鑰資訊

130:處理資源

140:認證模組

150:加密模組

200:系統

210:介面

220:包括身分資訊的請求

230:指示

240:加密結果

250:認證模組

260:加密模組

300:交互

410:身分資訊卡

420:電腦

430:智慧手機

440:平板設備

450:物聯網設備

500:處理

600:裝置

602:接收模組

604:確定模組

606:執行模組

第 108145434 號 民國 109 年 11 月 24 日修正

【發明申請專利範圍】

【請求項1】一種電腦實施的用於執行經過身分驗證的加密操作的方法，所述方法包括：

由加密晶片從客戶端接收用以執行請求的加密操作的請求，其中，所述請求包括與所述客戶端相關聯的客戶端身分資訊，並且所述加密晶片是包括處理資源和儲存資源的硬體組件，所述處理資源執行加密操作，所述儲存資源儲存所述加密操作中使用的密鑰資訊和與被允許請求加密操作的客戶端相關聯的身分資訊；

由所述加密晶片基於將所述客戶端身分資訊與儲存在所述儲存資源中的所述身分資訊進行比較，確定所述客戶端身分資訊與所述被允許請求加密操作的客戶端之一相關聯；以及

響應於確定所述客戶端身分資訊與所述被允許請求加密操作的客戶端之一相關聯，由所述加密晶片基於儲存在所述儲存資源中的所述密鑰資訊執行所述請求的加密操作；

由所述加密晶片基於用以執行加密操作的一個或多個請求不包括與任何一個所述被允許請求加密操作的客戶端相關聯的客戶端身分資訊，確定所述請求是惡意的；以及

響應於確定所述用以執行加密操作的一個或多個請求是惡意的，由所述加密晶片從所述儲存資源清除所述身分資訊和所述密鑰資訊。

【請求項2】根據請求項1所述的電腦實施的方法，其

中，所述請求的加密操作是加密操作、解密操作、數位簽名驗證操作或數位簽名產生操作。

【請求項3】根據請求項1或2所述的電腦實施的方法，其中，所述加密晶片是現場可程式化閘陣列(FPGA)、專用積體電路(ASIC)或微處理器。

【請求項4】根據請求項1或2所述的電腦實施的方法，其中，

所述請求包括資料，並且

所述加密晶片對所述資料執行所述請求的加密操作。

【請求項5】根據請求項1或2所述的電腦實施的方法，其中，所述加密晶片包括由所述處理資源執行以操作包括所述加密晶片的電腦系統的操作系統。

【請求項6】根據請求項1或2所述的電腦實施的方法，其中，所述請求是第一請求，所述請求的加密操作是第一請求加密操作，所述客戶端身分資訊是第一客戶端身分資訊，所述方法還包括：

由所述加密晶片從第二客戶端接收用以執行第二請求加密操作的第二請求，其中，所述第二請求包括與所述第二客戶端相關聯的第二客戶端身分資訊；和

由所述加密晶片基於將所述第二客戶端身分資訊與儲存在所述儲存資源中的所述身分資訊進行比較，確定所述第二客戶端身分資訊與所述被允許請求加密操作的客戶端之一無關，

其中，響應於確定所述第二客戶端身分資訊與所述被

允許請求加密操作的客戶端之一無關，所述加密晶片不執行所述第二請求的加密操作。

【請求項7】根據請求項1或2所述的電腦實施的方法，其中，所述加密晶片是現場可程式化閘陣列(FPGA)，並且所述方法還包括：

由所述加密晶片接收包括重新程式化資訊以對所述加密晶片重新程式化的請求；以及

響應於接收到所述請求，由所述加密晶片用所述重新程式化資訊替換儲存在所述儲存資源中的資訊。

【請求項8】根據請求項7所述的電腦實施的方法，其中，

所述儲存資源儲存由所述處理資源執行以執行所述加密操作的一個或多個算法，

所述重新程式化資訊包括一個或多個新算法，並且

用所述重新程式化資訊替換儲存在所述儲存資源中的資訊包括用所述新算法替換所述算法。

【請求項9】一種用於執行經過身分驗證的加密操作的系統，包括：

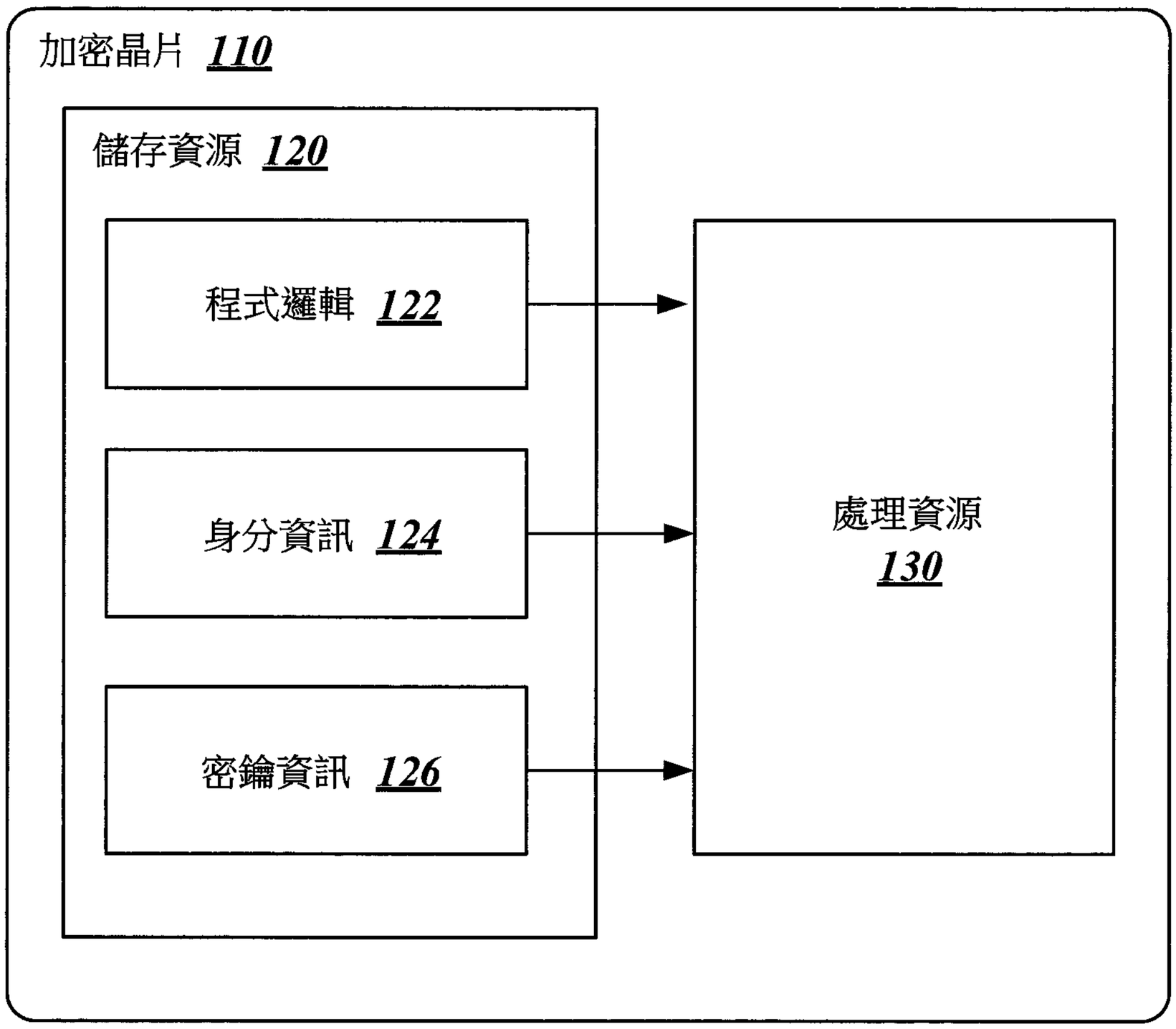
一個或多個處理器；和

一個或多個電腦可讀記憶體，所述電腦可讀記憶體耦接到所述一個或多個處理器並且其上儲存有指令，所述指令能夠由所述一個或多個處理器執行以執行請求項1至8中任一項所述的方法。

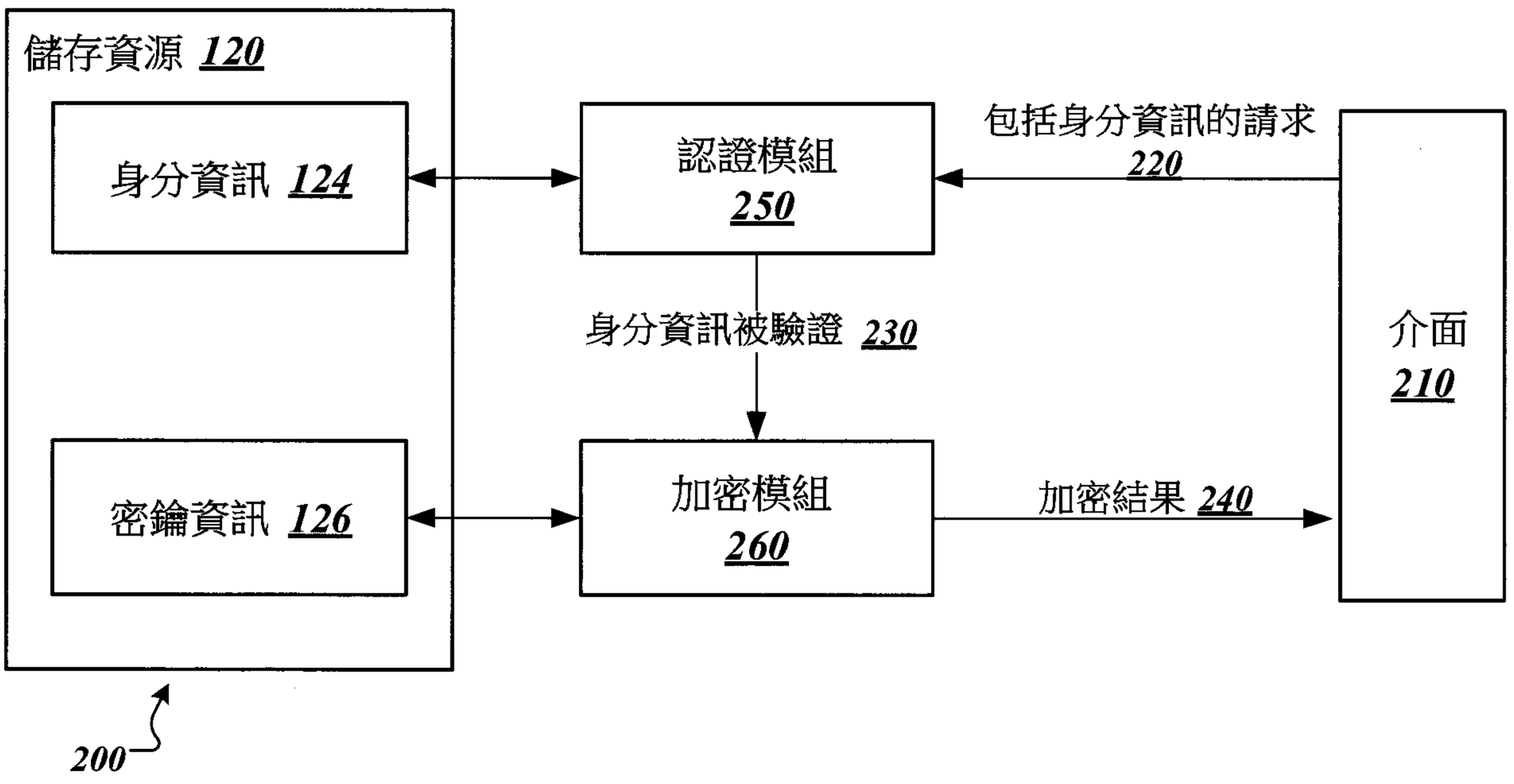
【請求項10】一種用於執行經過身分驗證的加密操作

的裝置，所述裝置包括用於執行請求項1至8中任一項所述的方法的多個模組。

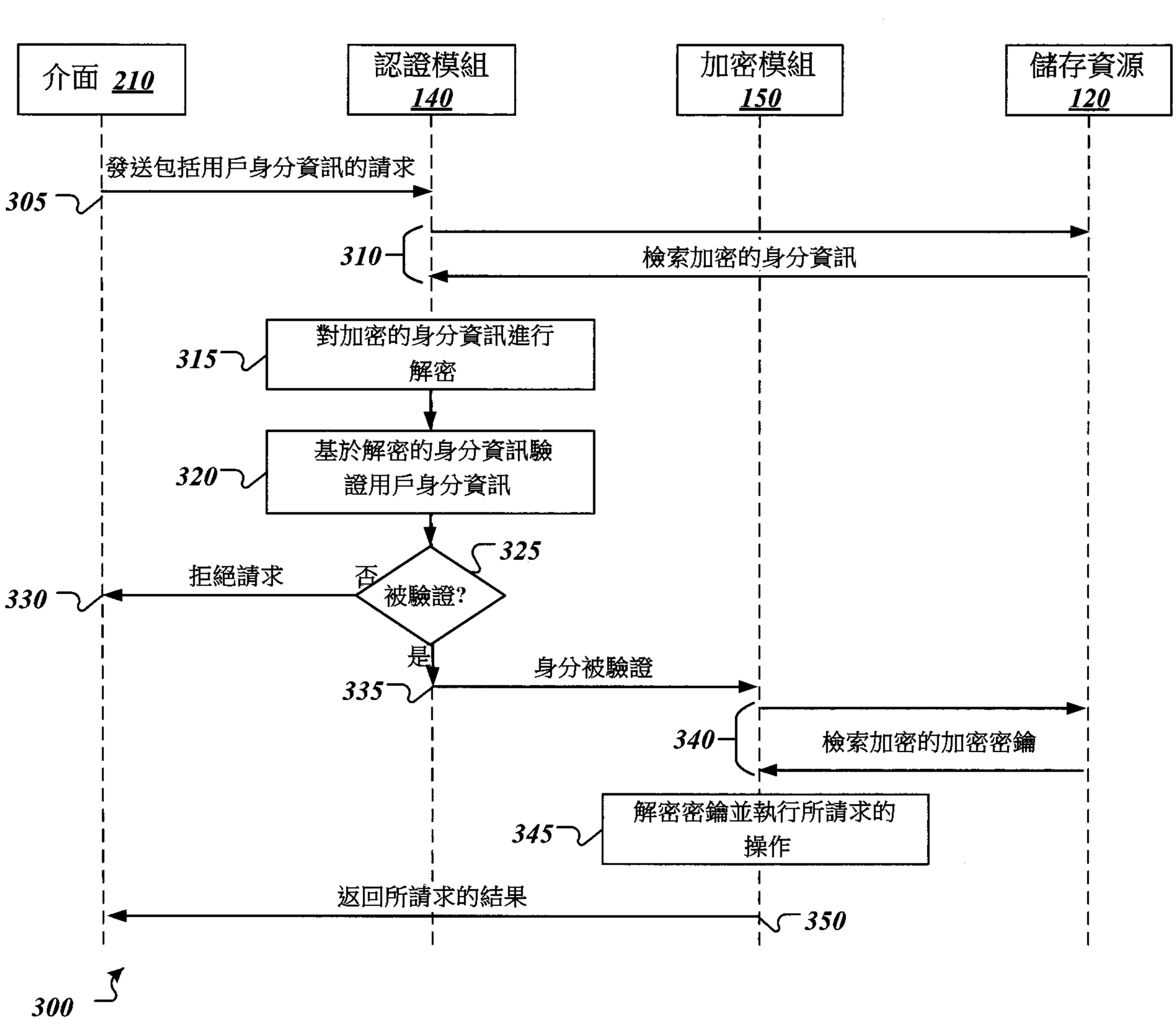
【發明圖式】


加密晶片 110
儲存資源 120
程式邏輯 122
身分資訊 124
密鑰資訊 126
處理資源 130
100

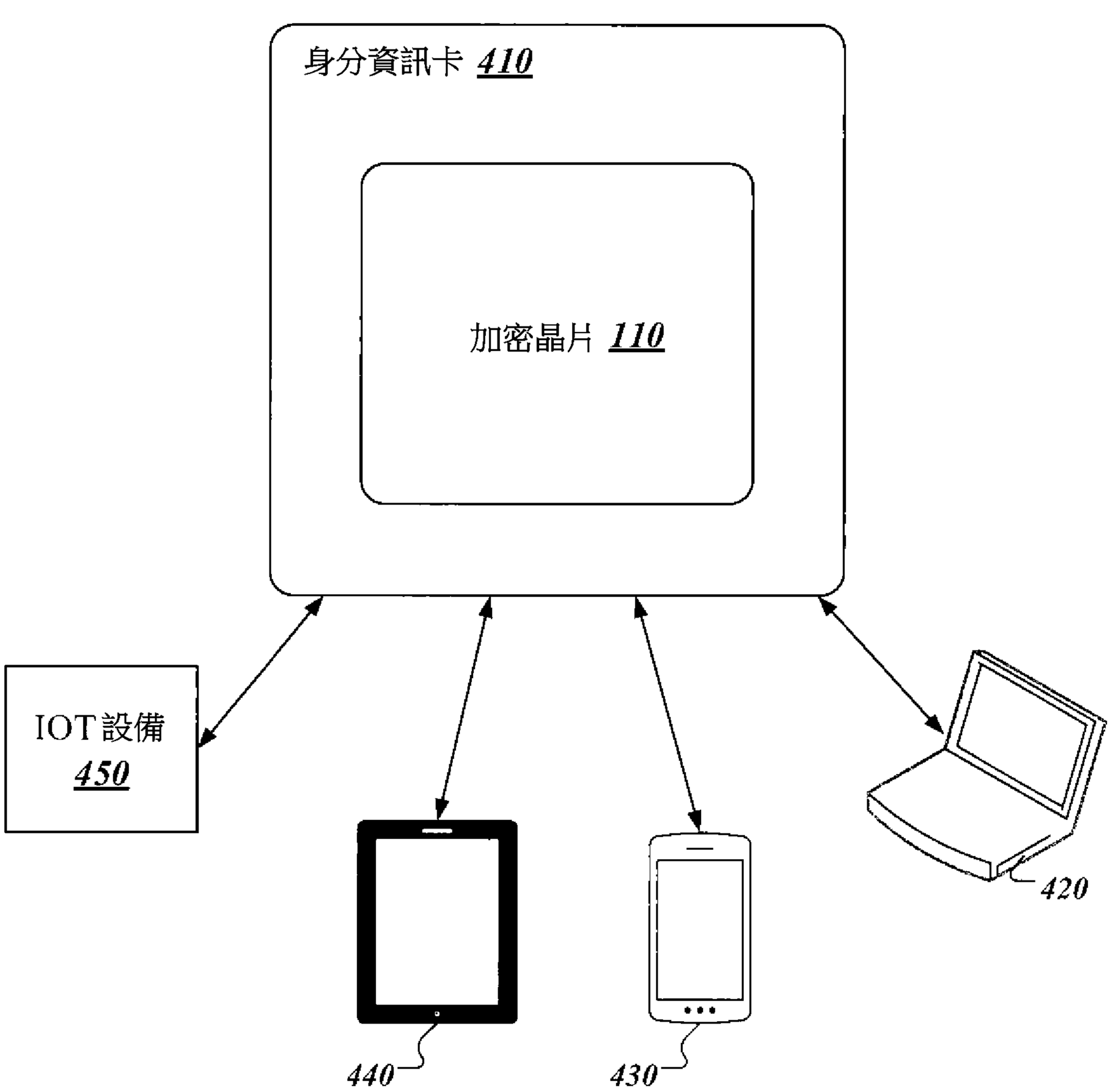
【圖 1】


儲存資源 120
身分資訊 124
密鑰資訊 126
認證模組 250
包括身分資訊的請求 220
身分資訊被驗證 230
加密模組 260
加密結果 240
介面 210
200

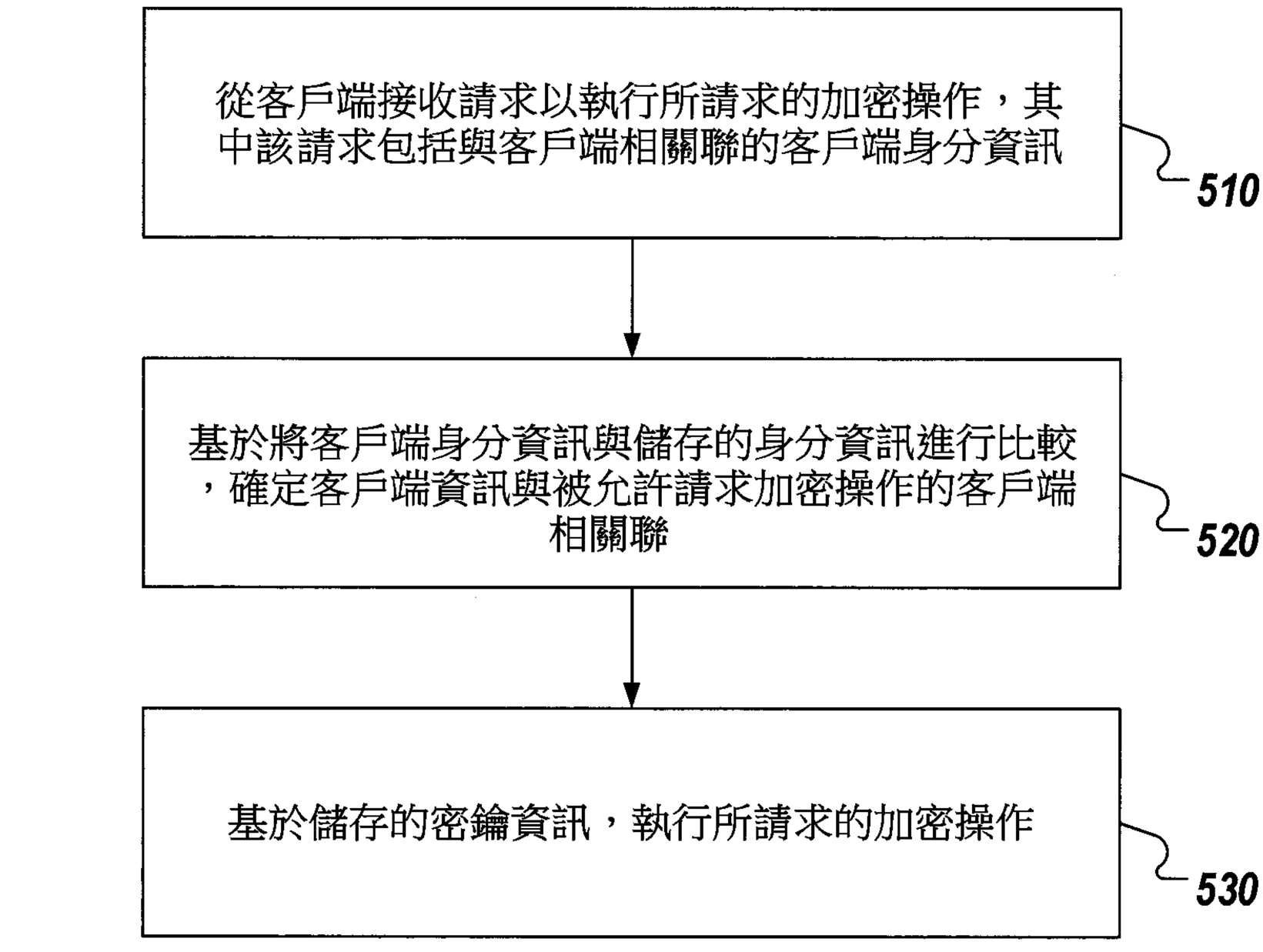
【圖 2】


介面 210
認證模組 140
加密模組 150
儲存資源 120
發送包括用戶身分資訊的請求
305
310
檢索加密的身分資訊
315
對加密的身分資訊進行解密
320
基於解密的身分資訊驗證用戶身分資訊
325
否
被驗證?
拒絕請求
330
是
335
身分被驗證
340
檢索加密的加密密鑰
345
解密密鑰並執行所請求的操作
返回所請求的結果
350
300

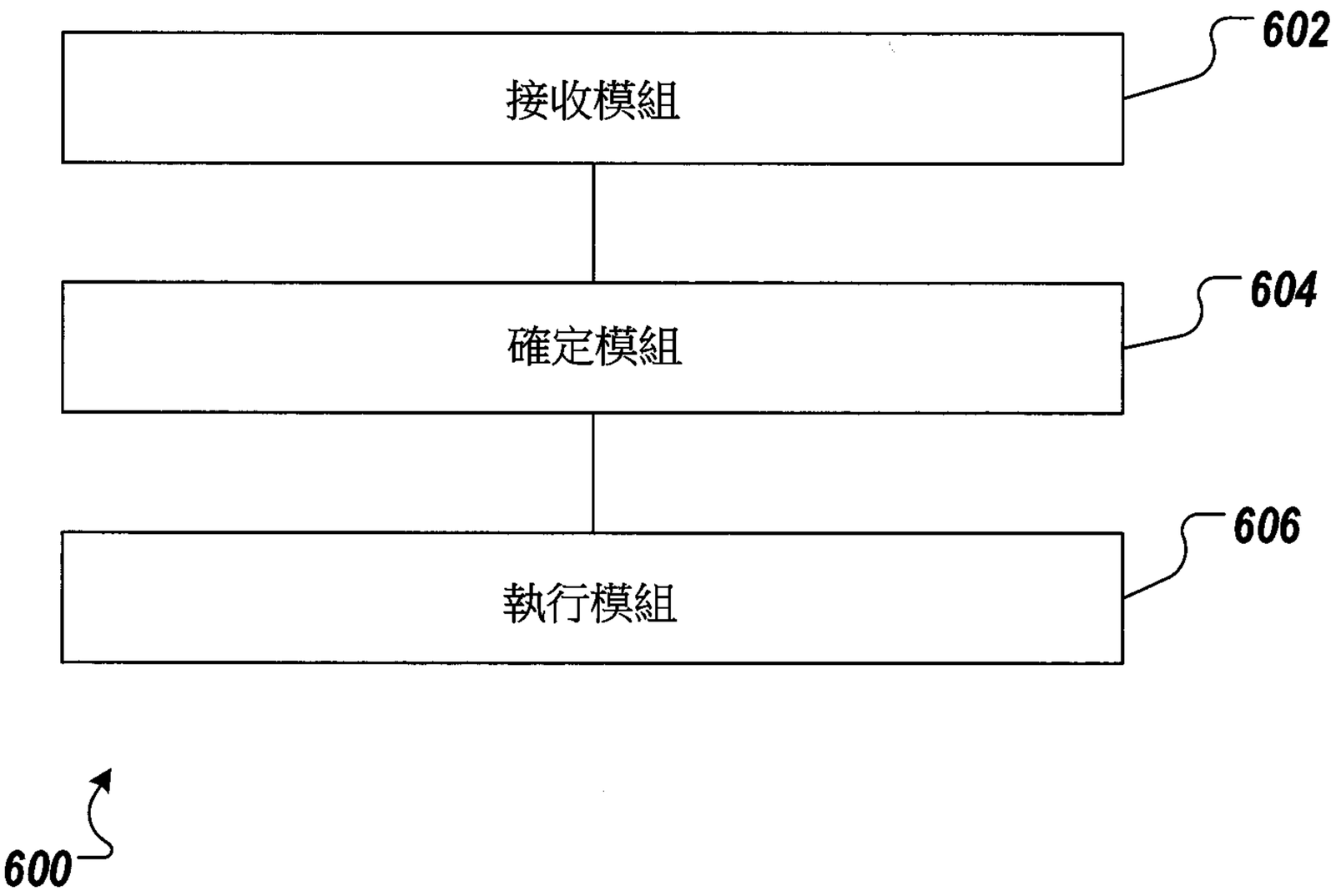
【圖 3】



【圖 4】


從客戶端接收請求以執行所請求的加密操作，其中該請求包括與客戶端相關聯的客戶端身分資訊
510
基於將客戶端身分資訊與儲存的身分資訊進行比較，確定客戶端資訊與被允許請求加密操作的客戶端相關聯
520
基於儲存的密鑰資訊，執行所請求的加密操作
530
500

【圖 5】


接收模組
602
確定模組
604
執行模組
606
600

【圖 6】