I818515

(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 I818515 B**

(45)公告日： 中華民國 112 (2023) 年 10 月 11 日

(21)申請案號：111114452 (22)申請日： 中華民國 111 (2022) 年 04 月 15 日

(51)Int. Cl.： *G06F21/62 (2013.01)* *G06F21/70 (2013.01)*
H04L9/12 (2006.01) *G06F3/0487 (2013.01)*

(30)優先權：2021/04/19 中華民國 110113909

(71)申請人：鈃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：鄭嘉信 CHENG, CHIA-HSIN (TW) ；蕭志平 HSIAO, CHIH-PING (TW) ；吳明鋌 WU, MING-TING (TW)

(74)代理人：楊代強

(56)參考文獻：

TW	201121280A	CN	101872399A
CN	110502885A	CN	112131541A
US	2015/0143496A1		

審查人員：陳昱潭

申請專利範圍項數：10 項 圖式數：6 共 24 頁

(54)名稱

數位密鑰服務裝置以及數位密鑰服務啟動方法

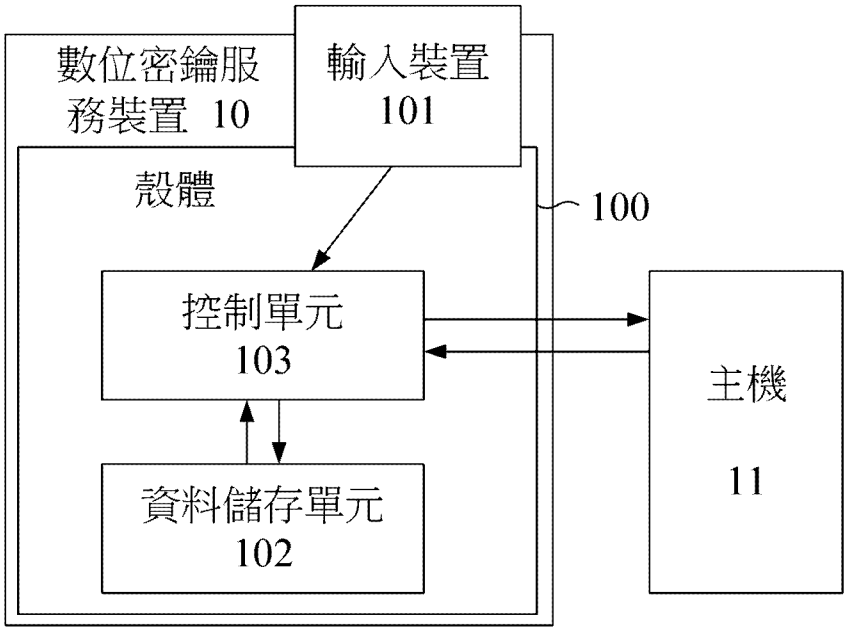
(57)摘要

本發明係有關於一種數位密鑰服務裝置以及數位密鑰服務啟動方法，該裝置可信號連接至一主機，該裝置包含：一殼體；一輸入裝置，其設置於該殼體之附近，提供一使用者進行指令輸入；一資料儲存單元，設置於該殼體中，用以儲存至少一筆數位資料與一數位密鑰；以及一控制單元，設置於該殼體中並信號連接至該主機、該輸入裝置以及該資料儲存單元，其係因應一確認程序之正確完成，而進行與該資料儲存單元所儲存之該數位密鑰相關之一密鑰服務，或輸出該資料儲存單元所儲存之該筆數位資料至該主機，而該確認程序中包含有一第一實體確認程序，該第一實體確認程序為：該使用者透過該輸入裝置所輸入指令被該控制單元確認為正確地對應一第一組預設時機點。

The present invention relates to a digital key service device and a method for activating a digital key service. The device is adapted to be in communication with a host. The device includes: a casing; an input device disposed near the casing and used for receiving a user instruction input; a data storage unit disposed in the casing and used for storing at least a record of digital data and a digital key; and a controlling unit disposed in the casing and in communication with the host, the input device and the data storage unit and used for performing a digital key service relating to the digital key stored in the data storage unit or outputting the record of digital data stored in the data storage unit after completing an authentication procedure successfully. The authentication procedure includes a first physical verification procedure. The authentication procedure is that the controlling unit determines that the user instruction inputted through the input device correctly corresponds to a first set of preset time points.

TW I818515 B

指定代表圖：



【圖 1】

符號簡單說明：

10:數位密鑰服務裝置

11:主機

100:殼體

101:輸入裝置

102:資料儲存單元

103:控制單元

公告本

I818515

【發明摘要】

【中文發明名稱】　數位密鑰服務裝置以及數位密鑰服務啟動方法

【英文發明名稱】　DIGITAL KEY SERVICE DEVICE AND METHOD FOR ACTIVATING DIGITAL KEY SERVICE

【中文】本發明係有關於一種數位密鑰服務裝置以及數位密鑰服務啟動方法，該裝置可信號連接至一主機，該裝置包含：一殼體；一輸入裝置，其設置於該殼體之附近，提供一使用者進行指令輸入；一資料儲存單元，設置於該殼體中，用以儲存至少一筆數位資料與一數位密鑰；以及一控制單元，設置於該殼體中並信號連接至該主機、該輸入裝置以及該資料儲存單元，其係因應一確認程序之正確完成，而進行與該資料儲存單元所儲存之該數位密鑰相關之一密鑰服務，或輸出該資料儲存單元所儲存之該筆數位資料至該主機，而該確認程序中包含有一第一實體確認程序，該第一實體確認程序為：該使用者透過該輸入裝置所輸入指令被該控制單元確認為正確地對應一第一組預設時機點。

【英文】

The present invention relates to a digital key service device and a method for activating a digital key service. The device is adapted to be in communication with a host. The device includes: a casing; an input device disposed near the casing and used for receiving a user instruction input; a data storage unit disposed in the casing and used for storing at least a record of digital data and a digital key; and a controlling unit disposed in the casing and in communication with the host, the input device and the

data storage unit and used for performing a digital key service relating to the digital key stored in the data storage unit or outputting the record of digital data stored in the data storage unit after completing an authentication procedure successfully. The authentication procedure includes a first physical verification procedure. The authentication procedure is that the controlling unit determines that the user instruction inputted through the input device correctly corresponds to a first set of preset time points.

【指定代表圖】　圖1

【代表圖之符號簡單說明】

10：數位密鑰服務裝置

11：主機

100：殼體

101：輸入裝置

102：資料儲存單元

103：控制單元

【發明說明書】

【中文發明名稱】　數位密鑰服務裝置以及數位密鑰服務啟動方法

【英文發明名稱】　DIGITAL KEY SERVICE DEVICE AND METHOD FOR ACTIVATING DIGITAL KEY SERVICE

【技術領域】

【0001】 本案係為一種數位密鑰服務裝置以及數位密鑰服務啟動方法，尤指應用於使用者資訊裝置之數位密鑰服務裝置以及數位密鑰服務啟動方法。

【先前技術】

【0002】 隨著資訊科技的普及，許多實際上需要保密的重要資料(各式帳號與密碼)只能連同一般資料共同存放在使用者端的資訊裝置中，例如常見的個人電腦、筆記型電腦或是現今更普及的智慧手機中。而且在現今的使用場景中，智慧手機以及類似的可攜式資訊裝置，會頻繁地透過各式資料傳輸管道(例如 USB 介面、藍牙或是無線網路等)來與其它資訊裝置或雲端上的伺服器進行資料交換或是金融交易。因此，若不妥善儲存需要保密的重要資料，該等資料便有極大可能被竊取而造成重要損失。例如，當駭客竊取到登入密碼後，便可以從遠端駭入使用者端的資訊裝置來對其發出正確的登入密碼，進而成功完成帳號登入。如此一來，使用者端資訊裝置中的重要資料將可能被任意取走。

【發明內容】

【0003】 而如何能有效改善此一習用手段的缺失，讓現存的資訊裝置可以方便地增強資料安全的防護能力，係為發展本案之主要目的。以下呈現本案技術

手段的簡要概述，以提供對這些技術手段的基本理解。本發明內容不是對本案的所有預期特徵的廣泛概述，亦不想限制本案技術手段的關鍵或重要要素。其唯一目的是以簡化形式呈現本案的技術手段的各種概念，作為稍後呈現的詳細描述的前言。

【0004】 本發明係有關於一種數位密鑰服務裝置，可信號連接至一主機，該數位密鑰服務裝置包含：一殼體；一輸入裝置，其設置於該殼體之附近，提供一使用者進行指令輸入；一資料儲存單元，設置於該殼體中，用以儲存至少一筆數位資料與一數位密鑰；以及一控制單元，設置於該殼體中並信號連接至該主機、該輸入裝置以及該資料儲存單元，其係因應一確認程序之正確完成，而進行與該資料儲存單元所儲存之該數位密鑰相關之一密鑰服務，或輸出該資料儲存單元所儲存之該筆數位資料至該主機，而該確認程序中包含有一第一實體確認程序，該第一實體確認程序為：該使用者透過該輸入裝置所輸入指令被該控制單元確認為正確地對應一第一組預設時機點。

【0005】 根據上述構想，本案所述之數位密鑰服務裝置，其中該輸入裝置為外露於該殼體之一觸控鍵或一壓力按鍵，用以讓該使用者於其上一個或多個手勢而產生符合該第一組預設時機點之一個或複數個指令。

【0006】 根據上述構想，本案所述之數位密鑰服務裝置，其中該輸入裝置為設於該殼體內之一震動感測器或一麥克風，該震動感測器用以感測該使用者於殼體之觸碰或搖晃而產生符合該第一組預設時機點之一個或複數個指令，該麥克風用以感測該指令輸入為該使用者利用身體或器具所發出之具有特定節奏而符合該第一組預設時機點的聲音。

【0007】根據上述構想，本案所述之數位密鑰服務裝置，其中該一個或複數個指令係符合一特定編碼格式之規定，進而遵循一預設的節奏被產生。

【0008】根據上述構想，本案所述之數位密鑰服務裝置，其中更包含一提示器，用以發出符合該組預設時機點之燈光或聲音信號，用以提示該使用者之輸入時機。

【0009】根據上述構想，本案所述之數位密鑰服務裝置，其中該確認程序更包含：該數位密鑰服務裝置連接至該主機後且於該第一實體確認程序進行前，先驗證該主機輸入之一個人識別碼(PIN)是否正確。

【0010】根據上述構想，本案所述之數位密鑰服務裝置，其中該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料讀取命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該資料讀取命令與該確認程序之正確完成而將該資料儲存單元所儲存之該數位資料輸出至該主機。

【0011】根據上述構想，本案所述之數位密鑰服務裝置，其中與該數位密鑰相關之一密鑰服務為利用該資料儲存單元所儲存之該數位密鑰與該主機輸入之一筆資料來製作出一數位簽章，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一數位簽章命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該數位簽章命令與該確認程序之正確完成而將該數位簽章輸出至該主機。

【0012】根據上述構想，本案所述之數位密鑰服務裝置，其中與該數位密鑰相關之一密鑰服務為利用該資料儲存單元所儲存之該數位密鑰對該主機輸入之一筆資料進行加密，或是利用該資料儲存單元所儲存之該數位密鑰與該主機輸

入之一筆已加密資料進行解密，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料加密命令或一資料解密命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該資料加密命令與該確認程序之正確完成或該資料解密命令與該確認程序之正確完成，而進行將該主機輸入之該筆資料進行加密後傳至該主機或儲存於該資料儲存單元，或是將該主機輸入之該筆已加密資料進行解密後傳至該主機或儲存於該資料儲存單元。

【0013】 根據上述構想，本案所述之數位密鑰服務裝置，其中該資料儲存單元包含有一第一資料儲存單元以及一第二資料儲存單元，用以儲存該數位密鑰之該資料儲存單元係位於一安全晶片中，而該筆數位資料儲存於該安全晶片外之該第二資料儲存單元。

【0014】 本案之另一方面一種數位密鑰服務啟動方法，應用於一主機與一數位密鑰服務裝置之間，該數位密鑰服務裝置中儲存至少一筆數位資料與一數位密鑰，該服務方法包含下列步驟：一使用者對該數位密鑰服務裝置進行指令輸入；以及該數位密鑰服務裝置因應一確認程序之正確完成，而自動啟動與該數位密鑰服務裝置中所儲存之一數位密鑰相關之一密鑰服務，或自動輸出一筆數位資料至該主機，而該確認程序中包含有一第一實體確認程序，該第一實體確認程序為：該使用者所輸入指令被該數位密鑰服務裝置確認為正確地對應一第一組預設時機點。

【0015】 根據上述構想，本案所述之數位密鑰服務啟動方法，其中該指令輸入為單個或複數個觸控手勢、單個或複數個滑動手勢、單個或複數個按壓手勢

或單個或複數個該數位密鑰服務裝置的震動，進而產生符合該第一組預設時機點之單個或多個手勢。

【0016】根據上述構想，本案所述之數位密鑰服務啟動方法，其中該指令輸入係符合一特定編碼格式之規定，進而遵循一預設的節奏被產生。

【0017】根據上述構想，本案所述之數位密鑰服務啟動方法，其中更包含下列步驟：使用該數位密鑰服務裝置上之一提示器發出符合該第一組預設時機點之燈光或聲音信號，用以提示該使用者之輸入時機。

【0018】根據上述構想，本案所述之數位密鑰服務啟動方法，其中該確認程序更包含：該數位密鑰服務裝置連接至該主機後且於該第一實體確認程序前，先驗證該主機輸入之一個人識別碼(PIN)是否正確。

【0019】根據上述構想，本案所述之數位密鑰服務啟動方法，其中該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料讀取命令後啟動，用以確認是否於一第二組預設時機點上正確地輸入指令，進而因應該資料讀取命令與該確認程序之正確完成而將該數位密鑰服務裝置所儲存之該數位資料輸出至該主機。

【0020】根據上述構想，本案所述之數位密鑰服務啟動方法，其中與該數位密鑰相關之一密鑰服務為利用該數位密鑰與該主機輸入之一筆資料來製作出一數位簽章，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一數位簽章命令後啟動，用以確認該使用者是否於一第二組預設時機點上正確輸入指令，並因應該數位簽章命令與該確認程序之正確完成而將該數位簽章輸出至該主機。

【0021】 根據上述構想，本案所述之數位密鑰服務啟動方法，其中與該數位密鑰相關之一密鑰服務為利用該數位密鑰對該主機輸入之一筆資料進行加密，或是利用該數位密鑰與該主機輸入之一筆已加密資料進行解密，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料加密命令或一資料解密命令後啟動，用以確認該使用者是否於該第二組預設時機點上正確輸入指令，並因應該資料加密命令與該確認程序之正確完成或該資料解密命令與該確認程序之正確完成，而進行將該主機輸入之該筆資料進行加密後傳至該主機或儲存於該數位密鑰服務裝置，或是將該主機輸入之該筆已加密資料進行解密後傳至該主機或儲存於該數位密鑰服務裝置。

【0022】 根據上述構想，本案所述之數位密鑰服務啟動方法，其中該指令輸入為使用者利用身體或器具所發出之具有特定節奏而符合該第一組預設時機點的聲音。

【0023】 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】

【0024】 圖 1，其係本案所發展出來關於一種數位密鑰服務裝置的第一較佳實施例功能方塊示意圖。

圖 2，其係本案所發展出來之數位密鑰服務裝置與主機間進行認證之較佳實施例方法之流程示意圖。

圖 3，其係本案所發展出來關於數位密鑰服務裝置的第二較佳實施例功能方塊示意圖。

圖 4，其係本案所發展出來之資料讀取方法流程示意圖。

圖 5，其係本案所發展出來之資料加密／解密方法流程示意圖。

圖 6，其係本案所發展出來關於數位密鑰儲存裝置的第三較佳實施例功能方塊示意圖。

【實施方式】

【0025】 請參見圖 1，其係本案所發展出來關於一種數位密鑰服務裝置的第一較佳實施例功能方塊示意圖，該數位密鑰服務裝置 10，可信號連接(例如是有線方式的通用序列匯流排（Universal Serial Bus，以下簡稱 USB）介面的接頭與插座配合、記憶卡接腳與插座配合或是無線方式的藍芽傳輸)至一主機 11，該數位密鑰服務裝置 10 中包含殼體 100、輸入裝置 101、資料儲存單元 102 以及控制單元 103，資料儲存單元 102 以及控制單元 103 設置於該殼體 100 中，該資料儲存單元 102 可以用來儲存至少一筆數位資料與一數位密鑰；而於本實施例之輸入裝置 101 則設置於該殼體 100 之附近且外露，用以提供使用者進行指令輸入，舉例來說，該輸入裝置 101 可以是外露於該殼體 100 之一觸控鍵或一壓力按鍵，用以感測該使用者於其上所進行之觸碰手勢、滑動手勢或是按壓手勢。而上述之數位密鑰服務裝置 10 可以包裝成一個 USB 隨身碟的外觀，用以插置在一電腦主機上。當然也可以是一個安全數位卡(Secure Digital Memory Card)的外觀，用以安裝在筆記型電腦、平板電腦或智慧手機上。

【0026】 再請參見圖 2，其係本案所發展出來之數位密鑰服務裝置 10 與主機 11 間進行認證之較佳實施例方法之流程示意圖，首先，主機 11 先進行步驟 201，對已連接其上之數位密鑰服務裝置 10 輸入一個人識別碼(PIN)，接著步驟 202，數位密鑰服務裝置 10 驗證該主機輸入之該個人識別碼(PIN)是否正確，若

判斷“正確”，數位密鑰服務裝置 10 便進入步驟 203，進入“等待使用者的下一步輸入動作”的狀態。在此狀態中，使用者可利用輸入裝置 101 來產生符合第一組預設時機點之指令(步驟 204)，而控制單元 103 對上述使用者利用輸入裝置 101 所產生之指令進行第一實體確認程序(步驟 205)，若確認正確無誤，則由數位密鑰服務裝置 10 對該主機 11 發出一認證成功的通知(步驟 206)。如此一來，透過上述方法，數位密鑰服務裝置 10 與主機 11 間便可以有效完成認證，而且透過個人識別碼(PIN)與第一實體確認程序的雙向雙重確認，可以確保不會被駭客從遠端入侵。

【0027】 舉例來說，即使駭客可以從遠端駭入主機 11 並能對數位密鑰服務裝置 10 發出正確的個人識別碼(PIN)，但是仍然需要現場的使用者在數位密鑰服務裝置 10 的輸入裝置 101 上實際操作，而且正確地產生符合該第一組預設時機點之指令後，才能通過控制單元 103 所進行第一實體確認程序的驗證。而這將對遠端的駭客造成無法完成的困擾，進而阻斷其惡意行為。而上述該輸入裝置 101 可以是外露於該殼體 100 之一觸控鍵、觸控面板或一壓力按鍵，用以讓該使用者進行單次或一連串複數個觸碰手勢、單次或一連串複數個滑動手勢或是單次或一連串複數個按壓手勢，進而產生符合該第一組預設時機點之一個或複數個指令。以複數個指令為例，符合該第一組預設時機點之複數個指令可以是下列幾種實施例：在觸控面板上滑出符合特定圖案與順序的多個筆劃，在觸控鍵或壓力按鍵上點擊(tap)出符合一特定編碼格式(例如摩斯電碼)規定之一特定敲擊節奏樣式，或是在觸控面板上滑出符合特定節奏的多個筆劃。舉例來說，特定節奏可以類似是短-短-長---短-短-長---等容易被辨識的節奏。而這些預設時機點之該複數個指

令，使用者可以在預設階段來自行定義上述特定圖案、節奏或其組合。當然，上述預設時機點之該複數個指令也可以是出廠便預設完成。

【0028】另外，該輸入裝置 101 還可以改以設於該殼體 100 內之一震動感測器(例如加速度感測器(accelerometer)或是壓電式震動感測器等)，不外露之該震動感測器可用以感測該使用者於殼體之觸碰或直接搖晃殼體而產生符合該第一組預設時機點之該複數個震動指令，如此同樣可以確認使用者是否在數位密鑰服務裝置的現場。

【0029】再請參見圖 3，其係本案所發展出來關於數位密鑰服務裝置 10 的第二較佳實施例功能方塊示意圖，其與第一較佳實施例的不同處在另設有一提示器 300，用以發出符合該第一組預設時機點之燈光或聲音信號，用以提示該使用者之輸入時機。舉例來說，為能提高指令輸入的正確率，該提示器 300 可以是外露於該殼體 100 之顯示器或 LED 燈，用以發出有特定節奏的閃光或顏色變化，用以提示按壓或是釋放該按鍵。另外，提示器 300 也可以是發出特定節奏聲響的蜂鳴器或揚聲器。主要可以達到提示使用者輸入時機的目的即可。如此一來，該第一實體確認程序可以簡化成：控制單元 103 確認該使用者透過該輸入裝置，對應第一組預設時機點來正確地輸入單一個指令。例如，使用者可以遵循提示器 300 之單一燈光閃動的提示，而於該提示後之一預設時機點完成單次觸碰手勢、單次滑動手勢、單次按壓手勢或是單次搖晃手勢，進而產生符合該第一組預設時機點之一個指令。當然，也可以是：使用者遵循提示器 300 之一連串燈光閃動的提示，而於該提示後之一預設時間內，完成符合該第一組預設時機點之一連串觸碰手勢、一連串滑動手勢、一連串按壓手勢或是一連串搖晃手勢，進而產生符合該組預設時機點之多個指令。而上述之輸入裝置 101 的類型，除了是可以感測各

種手勢的觸控鍵、觸控面板、壓力按鍵或是震動感測器之外，還可以是用以感測聲音的麥克風裝置，當然也可以是上述元件的各種組合。而使用者所輸入之符合上述預設時機點之單一或該複數個指令便可以是使用者利用身體(唱歌、拍手或彈指)或器具(例如敲擊桌面)所發出具有特定節奏而符合該組預設時機點的聲音。而確認節奏是否正確的方法，已存在各種技術手段可以完成，常見的伴唱系統中的自動評分功能中對於節奏準確度的判斷便可轉用至本案的實施例中，故不再贅述。相關技術的論文範例，可以參見 IEEE Transactions on Audio Speech and Language Processing 於 2012 年五月在下列網址所公開之技術：https://www.researchgate.net/publication/254062640_Automatic_Evaluation_of_Karaoke_Singing_Based_on_Pitch_Volume_and_Rhythm_Features。

【0030】而在圖 2 所示之方法完成數位密鑰服務裝置 10 與主機 11 之間的個人識別碼(PIN)確認程序以及第一實體確認程序後，還可以再接續進行其他程序來共同組成一確認程序。例如圖 4 之所示，其係本案所發展出來之資料讀取方法流程示意圖，其中表達了由控制單元 103 所進行之一第二實體確認程序，其與該個人識別碼(PIN)確認程序以及該第一實體確認程序來共同組成該確認程序。舉例來說，當該第一實體確認程序完成且該主機 11 發出一特定位址索引之一資料讀取命令(步驟 401)，收到該資料讀取命令之數位密鑰服務裝置 10 便進入步驟 402，用以等待使用者的下一步輸入動作，此時便可開始進行下列兩個步驟(步驟 403、404)所構成之第二實體確認程序。而當使用者利用輸入裝置 101 來產生符合一第二組預設時機點之複數個指令(步驟 403)後，便可再次確認該使用者在現場而正確完成該確認程序(步驟 404)。而該控制單元 103 係因應兩個條件“收到該資料讀取命令”與“該確認程序之正確完成”皆成立後，便可以自動將特定位址索

引對應之該資料儲存單元 102 所儲存之該數位資料輸出至該主機 11(步驟 405)，而上述的數位資料可以是一般的數據資料或是用戶憑證(User credentials)。如此一來，透過上述方法而有效完成整個確認程序後，數位密鑰服務裝置 10 與主機 11 間才可以進行一般的數據資料讀取或是把用戶憑證(User credentials)送去主機來完成用戶的身份驗證。如此將可以確保不會被駭客從遠端入侵來取走資料或是任意登入主機。而第二組預設時機點與上述之第一組預設時機點可以是相同內容，也可以是不同的內容，就看使用者如何去定義。

【0031】再請參見圖 5，其係本案所發展出來之資料加密方法流程示意圖，其中也是由控制單元 103 所進行該個人識別碼(PIN)確認程序、該第一實體確認程序以及第二實體確認程序來組成該確認程序，當該第一實體確認程序完成且該主機 11 發出一帶有一筆待加密資料之一資料加密命令(步驟 501)，該資料加密命令可以是數位簽章命令，收到帶有該筆待加密資料之該資料加密命令之數位密鑰服務裝置 10 進入步驟 502。數位密鑰服務裝置 10 使用該數位密鑰來對該筆待加密資料進行加密而生成一加密資料，然後等待使用者的下一步輸入動作(步驟 503)來進行第二實體確認程序，而當使用者利用輸入裝置 101 來產生符合一第二組預設時機點之複數個指令(步驟 504)後，便可再次確認該使用者在現場而正確完成該確認程序(步驟 505)。而該控制單元 103 係因應該資料加密命令與該確認程序之正確完成而將該加密資料輸出至該主機 11(步驟 506)。而上述加密資料可以是一個數位簽章檔案或是一般加密檔案，除了將該數位簽章檔案輸出至該主機 11 之外，也可以把加密檔案儲存在資料儲存單元 102 中。同樣的，第二組預設時機點與上述之第一組預設時機點可以是相同內容，也可以是不同的內容，就看使用者如何去定義。關於步驟 501 中該主機 11 所發出之帶有一筆待加密資料

之資料加密命令，還可以是其他與該數位密鑰相關之一密鑰服務。例如，可以是利用該資料儲存單元所儲存之該數位密鑰與該主機輸入之一筆已加密資料進行解密，而該第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料解密命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該資料解密命令與該確認程序之正確完成，而進行將該主機輸入之該筆已加密資料進行解密後傳至該主機或儲存於該資料儲存單元。

【0032】 另外，如圖 6 之所示，其係本案所發展出來關於數位密鑰服務裝置的第三較佳實施例功能方塊示意圖，其與上述實施例之主要不同處在於上述用以儲存該數位密鑰之第一資料儲存單元 601 係可設於獨立的安全晶片 60 中，而一般資料則可以儲存於安全晶片 60 外之第二資料儲存單元 602 中。上述安全晶片 60 可以是通過資訊技術安全評估共同準則評估保證等級 (Common Criteria Evaluation Assurance Level，簡稱 CC EAL)5+認證的安全晶片(Secure Element)，而第二資料儲存單元 602 則可以是一般記憶卡中之快閃記憶體。

【0033】 從上述說明可以看出，本案之數位密鑰服務裝置 10 與主機 11 間透過個人識別碼(PIN)與第一實體確認程序的雙向雙重確認，可以確保不會被駭客從遠端入侵。而再透過第二實體確認程序，可以再次確認後續的密鑰服務不被盜用，讓現存的各式主機與資訊裝置可以方便地新增資料安全儲存的功能，達成發展本案之主要目的。

【0034】 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，本案提出的數位密鑰服務裝置，其相關技術概念當然可以運用到各式個樣的資訊裝置上，同樣可以達到資訊安全性大幅提昇，具有重要的資料不被輕易取得的優點。

【0035】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】

【0036】

10：數位密鑰服務裝置

11：主機

100：殼體

101：輸入裝置

102：資料儲存單元

103：控制單元

300：提示器

60：安全晶片

601：第一資料儲存單元

602：第二資料儲存單元

【發明申請專利範圍】

【請求項1】一種數位密鑰服務裝置，可信號連接至一主機，該數位密鑰服務裝置包含：

一殼體；

一輸入裝置，其設置於該殼體之附近，提供一使用者進行指令輸入；

一資料儲存單元，設置於該殼體中，用以儲存至少一筆數位資料與一數位密鑰；以及

一控制單元，設置於該殼體中並信號連接至該主機、該輸入裝置以及該資料儲存單元，其係因應一確認程序之正確完成，而進行與該資料儲存單元所儲存之該數位密鑰相關之一密鑰服務，或輸出該資料儲存單元所儲存之該筆數位資料至該主機，而該確認程序中包含有一第一實體確認程序，該第一實體確認程序為：該使用者透過實際操作該輸入裝置所輸入具有一特定節奏而符合一第一組預設時機點的指令被該控制單元確認為該特定節奏正確地對應該第一組預設時機點。

【請求項2】如請求項1所述之數位密鑰服務裝置，其中該輸入裝置為外露於該殼體之一觸控鍵或一壓力按鍵，用以讓該使用者於其上一個或多個手勢而產生符合該第一組預設時機點之一個或複數個指令。

【請求項3】如請求項1所述之數位密鑰服務裝置，其中該輸入裝置為設於該殼體內之一震動感測器或一麥克風，該震動感測器用以感測該使用者於殼體之觸碰或搖晃而產生符合該第一組預設時機點之一個或複數個指令，該麥克風用以感測之該指令輸入為該使用者利用身體或器具所發出之具有該特定節奏而符合該第一組預設時機點的聲音。

【請求項4】 如請求項2、3中任一所述之數位密鑰服務裝置，其中該一個或複數個指令係符合一特定編碼格式之規定，進而遵循一預設的節奏被產生。

【請求項5】 如請求項2、3中任一所述之數位密鑰服務裝置，其中更包含一提示器，用以發出符合該組預設時機點之燈光或聲音信號，用以提示該使用者之輸入時機。

【請求項6】 如請求項1所述之數位密鑰服務裝置，其中該確認程序更包含：該數位密鑰服務裝置連接至該主機後且於該第一實體確認程序進行前，先驗證該主機輸入之一個人識別碼(PIN)是否正確。

【請求項7】 如請求項1所述之數位密鑰服務裝置，其中該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料讀取命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該資料讀取命令與該確認程序之正確完成而將該資料儲存單元所儲存之該數位資料輸出至該主機。

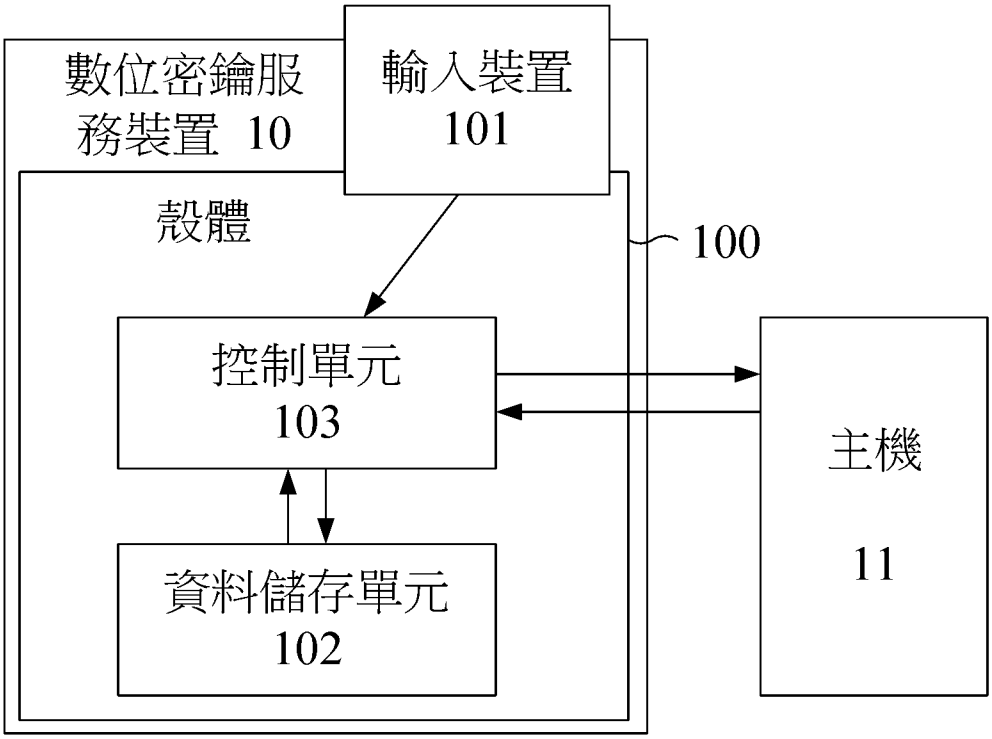
【請求項8】 如請求項1所述之數位密鑰服務裝置，其中與該數位密鑰相關之一密鑰服務為利用該資料儲存單元所儲存之該數位密鑰與該主機輸入之一筆資料來製作出一數位簽章，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一數位簽章命令後啟動，用以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該數位簽章命令與該確認程序之正確完成而將該數位簽章輸出至該主機。

【請求項9】 如請求項1所述之數位密鑰服務裝置，其中與該數位密鑰相關之一密鑰服務為利用該資料儲存單元所儲存之該數位密鑰對該主機輸入之一筆資料進行加密，或是利用該資料儲存單元所儲存之該數位密鑰與該主機輸入之一筆已加密資料進行解密，而該確認程序更包含一第二實體確認程序，於該第一實體確認程序完成且該主機發出一資料加密命令或一資料解密命令後啟動，用

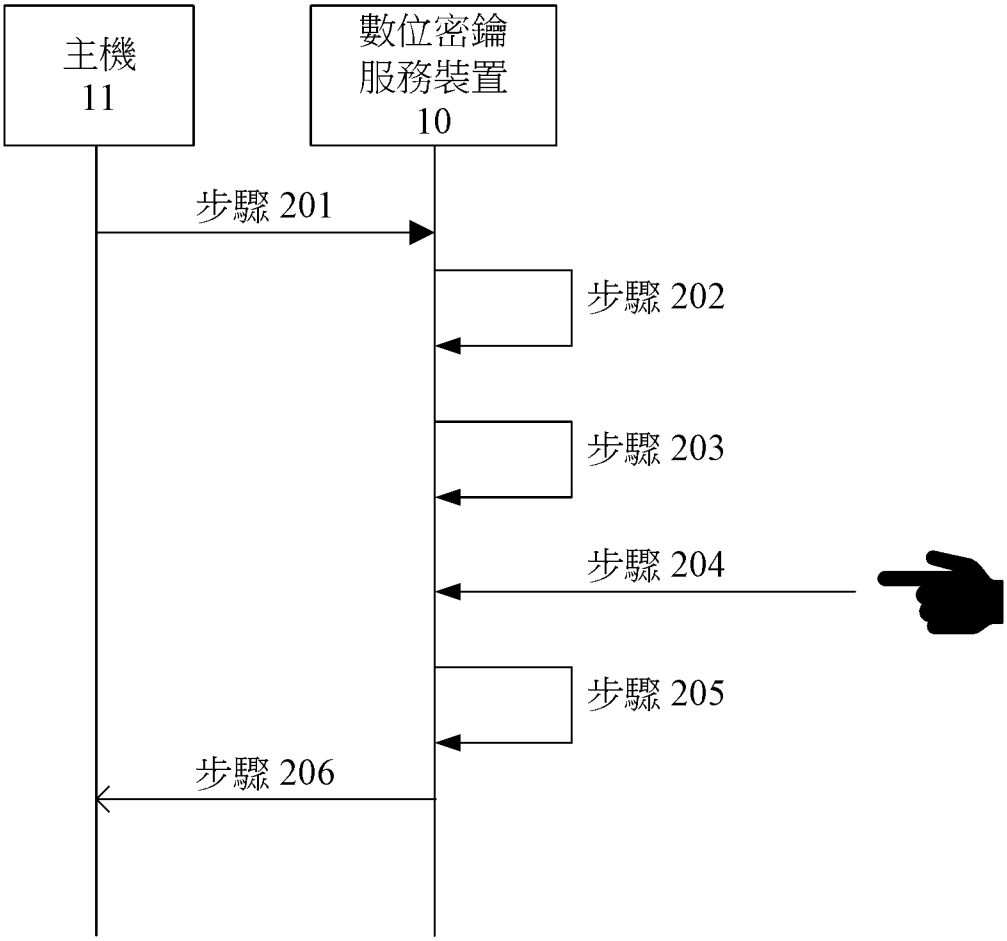
以確認該使用者透過該輸入裝置是否於一第二組預設時機點上正確輸入指令，該控制單元係因應該資料加密命令與該確認程序之正確完成或該資料解密命令與該確認程序之正確完成，而進行將該主機輸入之該筆資料進行加密後傳至該主機或儲存於該資料儲存單元，或是將該主機輸入之該筆已加密資料進行解密後傳至該主機或儲存於該資料儲存單元。

【請求項10】 如請求項1所述之數位密鑰服務裝置，其中該資料儲存單元包含有一第一資料儲存單元以及一第二資料儲存單元，用以儲存該數位密鑰之該資料儲存單元係位於一安全晶片中，而該筆數位資料儲存於該安全晶片外之該第二資料儲存單元。

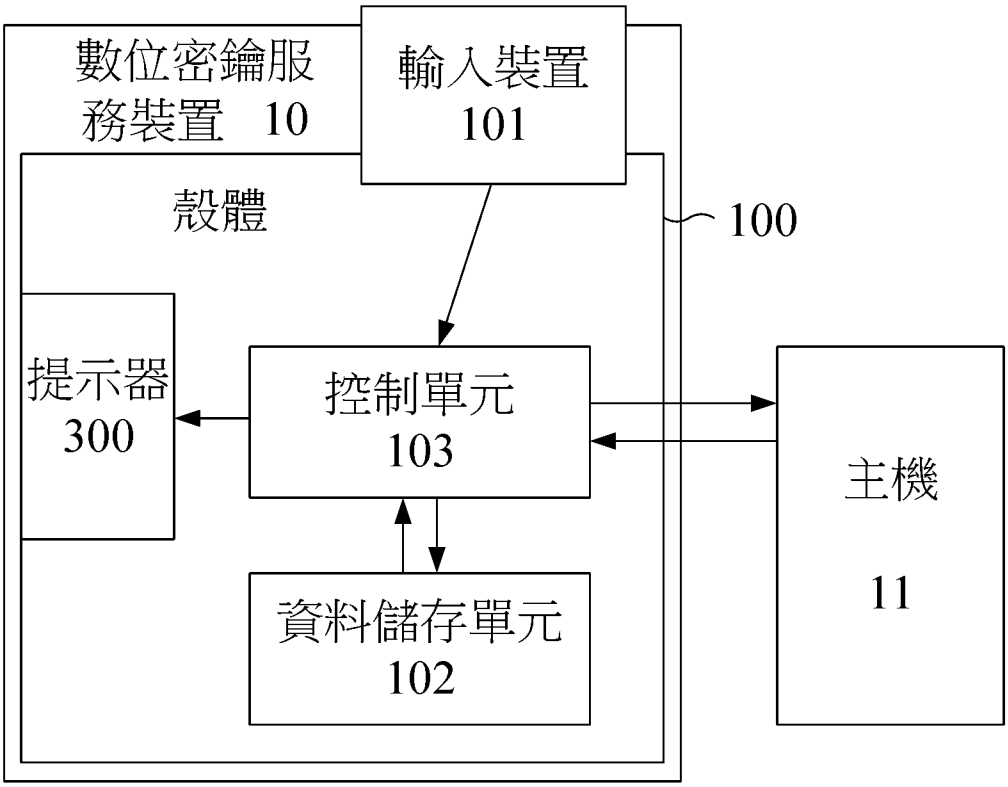
【發明圖式】



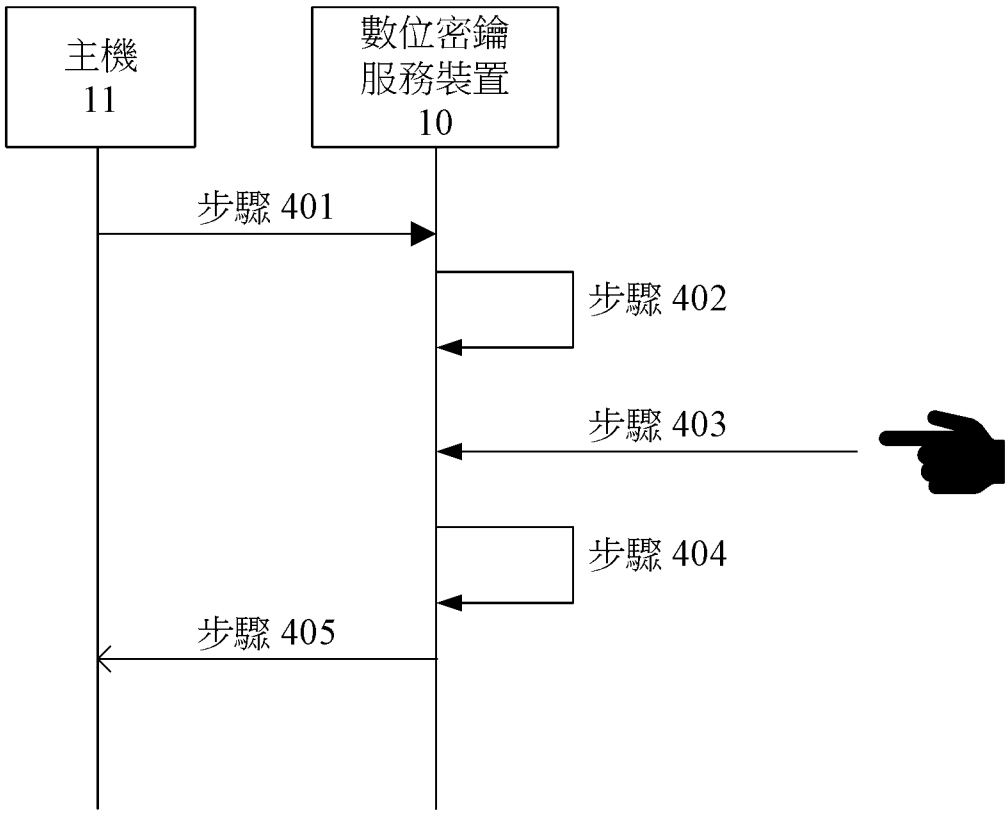
【圖 1】



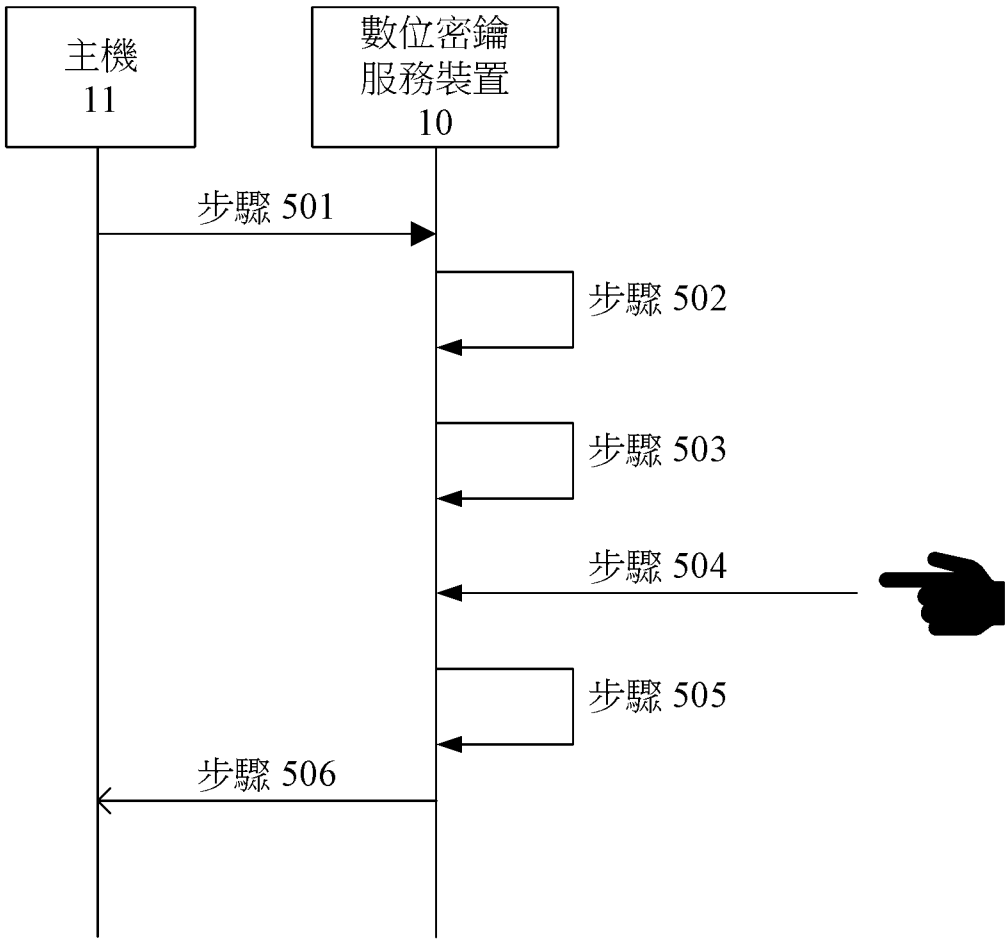
【圖 2】



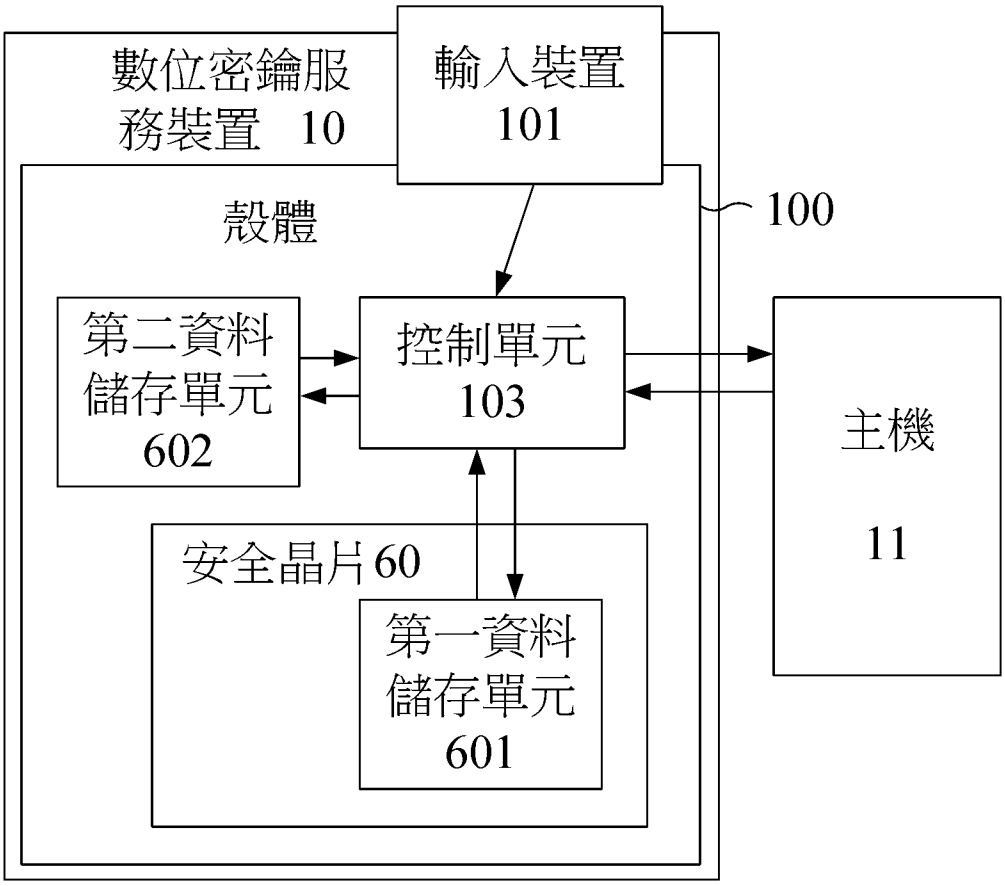
【圖 3】



【圖 4】



【圖 5】


數位密鑰服務裝置 10
輸入裝置 101
100
殼體
第二資料儲存單元 602
控制單元 103
主機 11
安全晶片 60
第一資料儲存單元 601

【圖 6】