201737151

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201737151 A

(43)公開日： 中華民國 106 (2017) 年 10 月 16 日

(21)申請案號：106100149 (22)申請日： 中華民國 106 (2017) 年 01 月 04 日

(51)Int. Cl.： *G06F21/62 (2013.01)*

(30)優先權：2016/01/04 美國 14/987,749

(71)申請人：克萊夫公司 (美國) CLEVX, LLC (US)
美國

(72)發明人：巴露丁 蘭夫M BOLOTIN, LEV M. (US)；雷墨爾 艾力克 LEMELEV, ALEX (CA)；辛爾 馬可 SINGER, MARC (US)

(74)代理人：洪武雄；陳昭誠

申請實體審查：無 申請專利範圍項數：25 項 圖式數：13 共 56 頁

(54)名稱

具有加密性的資料保全系統

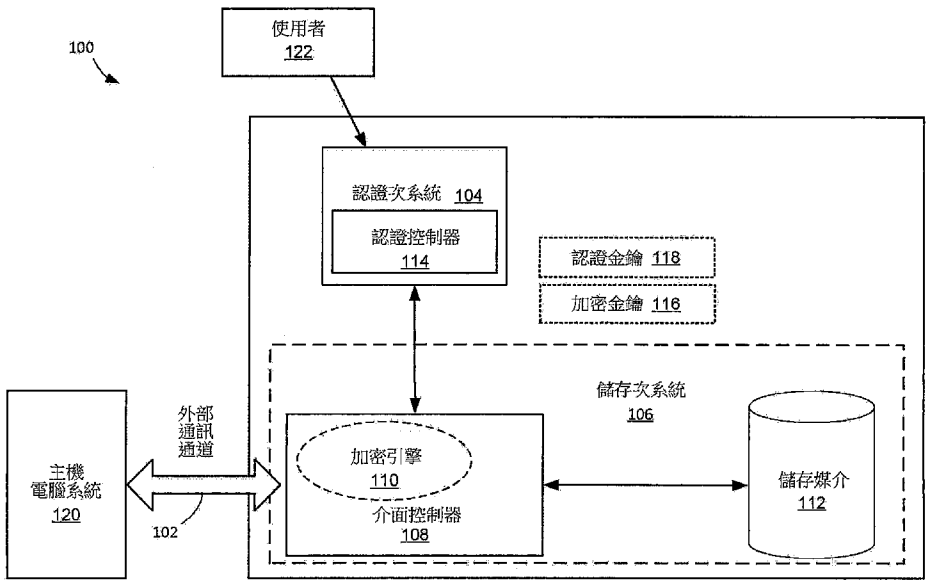
DATA SECURITY SYSTEM WITH ENCRYPTION

(57)摘要

本發明提供一種資料保全系統及其操作方法，包含：資料保全收發器或接收器；認證次系統，可操作連接至該資料保全收發器或接收器；以及儲存次系統，連接至該認證次系統。

A data security system, and a method of operation thereof, includes a data security transceiver or receiver; an authentication subsystem operatively connected to the data security transceiver or receiver; and a storage subsystem connected to the authentication subsystem.

指定代表圖：



第1圖

符號簡單說明：

100・・・資料保全系統

102・・・外部通訊通道

104・・・認證次系統

106・・・儲存次系統

108・・・介面控制器

110・・・加密引擎

112・・・儲存媒介

114・・・認證控制器

116・・・加密金鑰

118・・・認證金鑰

120・・・主機電腦系統

122・・・使用者

201737151

發明摘要

※申請案號：106100149

※申請日： 106/01/04 ※IPC 分類： G06F 21/62 (2013.01)

【發明名稱】(中文/英文)

具有加密性的資料保全系統

DATA SECURITY SYSTEM WITH ENCRYPTION

【中文】

本發明提供一種資料保全系統及其操作方法，包含：資料保全收發器或接收器；認證次系統，可操作連接至該資料保全收發器或接收器；以及儲存次系統，連接至該認證次系統。

【英文】

A data security system, and a method of operation thereof, includes a data security transceiver or receiver; an authentication subsystem operatively connected to the data security transceiver or receiver; and a storage subsystem connected to the authentication subsystem.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

100　資料保全系統

102　外部通訊通道

104　認證次系統

106　儲存次系統

108　介面控制器

110　加密引擎

112　儲存媒介

114　認證控制器

116　加密金鑰

118　認證金鑰

120　主機電腦系統

122　使用者

【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】（中文/英文）

具有加密性的資料保全系統

DATA SECURITY SYSTEM WITH ENCRYPTION

相關申請案之交互參照

【0001】本案為2010年3月29日提出之同時待審的美國專利申請號12/680,742之部分連續案，本案為2008年9月26日提出之國際申請號PCT/US2008/077766的國家階段，本案主張2007年9月27日提出之美國臨時專利申請序號60/975,814之優惠，並且該臨時專利申請之專利標的在此併入參考。

【0002】本專利申請含有由Lev M. Bolotin和Simon B. Johnson所同時提出之標題為”具有加密性的資料保全系統”之美國專利申請之相關的專利標的。該相關的申請係指定給ClevX, LLC並且以案卷編號502-018P-PCT-US.C1所標識。該美國專利申請之專利標的在此併入參考。

【技術領域】

【0003】本發明大致係關於電子裝置，並且尤其係關於記憶體裝置。

【先前技術】

【0004】保全是幾乎所有方面的電腦使用之關鍵性問題。儲存媒介（例如連結至電腦之硬碟）含有有價值的資訊，該資訊易於受到資料竊取。大量的金錢及努力是應用

在保護個人、企業及政府保全資訊。

【0005】 當可攜式記憶體儲存裝置已經變得更小、更容易遺失、更無處不在、更便宜及更大的記憶體容量時，也會造成極大的保全問題。現在能夠秘密地下載大量的資訊至可攜式記憶體儲存裝置內，諸如萬用序列匯流排（USB，Universal Serial Bus）快閃及微型隨身碟、行動電話、攝像機、數位相機、iPOD、MP3/4 播放器、智慧手機、掌上及膝上電腦、遊戲設備、認證器、代幣（含有記憶體）等等-通常為，大量儲存裝置（MSD，mass storage device）。

【0006】 具體而言，有數以百萬計的 MSD 是使用於備份、轉移、中間儲存器及主儲存器，以供資訊能夠輕易地由電腦下載並帶走。任何 MSD 之主要目的係在於儲存及提取「可攜式內容」，該「可攜式內容」是僅限於特定所有者而非特定電腦之資料及資訊。

【0007】 提供儲存保全之最常見的手法是使用電腦輸入之密碼來認證該使用者。密碼是對照 MSD 儲存的數值而有效。若發生匹配，則該磁碟機將開啟。或者，該密碼本身是使用作為加密金鑰，用以加密/解密儲存至該 MSD 內之資料。

【0008】 對於支援動態加密之磁碟機，該加密金鑰通常以加密的形式儲存於該媒介上。由於該加密金鑰儲存於該媒介上，所以對於有意規避標準介面而直接讀取該媒介之人士將變得容易取用。因此，密碼是使用作為加密該加密金鑰之金鑰。

【0009】 對於自我認證的磁碟機，本身的認證次系統是負責用於維持保全。並不需要依賴該磁碟機所連接之主機電腦。因此，密碼無法（或者不需要）由該主機發送藉以解鎖該 MSD。事實上，該加密金鑰不再需要儲存在該媒介上。該認證次系統變成用於管理加密金鑰之工具。

【0010】 因此，仍然存在用於改良保全之需求。鑑於不斷增加的商業化競爭壓力，結合不斷成長的消費者期望及對於在市場上有意義的產品差異化之該逐漸減少的機會，關鍵在於找到這些問題的答案。此外，降低成本、改善效率及效能及滿足競爭壓力之需求，對於找到這些問題的答案之關鍵必要性甚至增加了更大的急迫性。

【0011】 習知該領域者已經長期尋求對於這些問題之解決方法但是先前的開發並未教導或建議任何解決方案，因此，熟習該項技藝之人士已經長期對於這些問題之解決方法束手無策。

【發明內容】

【0012】 本發明提供一種資料保全系統之操作之方法，包含：提供具有用於與該資料保全系統連接之資料保全系統應用程式的行動裝置；啟動該資料保全系統應用程式；以及維持該資料保全系統與該行動裝置之連接。

【0013】 本發明提供一種資料保全系統，包含：資料保全收發器或接收器；認證次系統，操作上連接至該資料保全收發器或接收器；以及儲存次系統，連接至該認證次系統。

【0014】 除了或替代上述提到的目的之外，本發明之特定實施例具有其它目的。當參考附加圖式時，該目的對於熟習該項技藝之人士在閱讀該下列的詳細說明將變得顯而易見。

【圖式簡單說明】

【0015】 第 1 圖為依據本發明之實施例之資料保全系統之示意圖；

【0016】 第 2 圖為使用該資料保全系統之認證金鑰交付方法之說明；

【0017】 第 3 圖為用於讓該使用者與該資料保全系統互動之不同系統之說明；

【0018】 第 4 圖為該使用者如何能夠使用該主機電腦系統以與資料保全系統互動之說明；以及

【0019】 第 5 圖為使用用於該資料保全系統之使用者確認之資料保全方法。

【0020】 第 6 圖為例示性的資料保全通訊系統。

【0021】 第 7 圖為顯示在行動裝置與該資料保全系統之間之操作的順序之管理者排序圖。

【0022】 第 8 圖為該行動裝置是認證因素之解鎖排序圖。

【0023】 第 9 圖為顯示由該行動裝置使用 PIN 輸入而解鎖之解鎖排序圖。

【0024】 第 10 圖為經由該伺服器/控制台使用 PIN 輸入及使用者 ID/位置/時間確認而解鎖之解鎖排序圖。

【0025】 第 11 圖為顯示使用伺服器/控制台重置該資料保全系統之重置排序圖。

【0026】 第 12 圖為顯示使用該伺服器/控制台解鎖該資料保全系統之解鎖排序圖。

【0027】 第 13 圖為使用該伺服器/控制台之改變使用者的密碼排序圖。

【實施方式】

【0028】 下列實施例將以充分詳細的方式作描述以使得熟悉該項技藝之人士製作及使用本發明。應該瞭解的是，其它實施例依據本發明揭露將是顯而易見的，並且可在不違反本發明之範疇的情況下對系統、製程或機構做出改變。

【0029】 在下列的描述中，將給定各種特定的細節以提供本發明之完整的瞭解。然而，將顯而易見的是，本發明可以在未具有這些特定的細節下而實施。為了避免模糊本發明，某些已知的電路、系統配置及製程步驟並未做詳細揭露。

【0030】 同樣地，該系統之顯示實施例之圖式為半圖解及未按照比例，並且尤其，某些尺寸是為了明確呈現及誇大顯示於該圖式中。其中多個實施例為揭露及描述具有某些共同的特徵，為了該實施例之明確及容易說明、描述及理解，彼此類似及相似的特徵一般將以類似或相同的元件符號作描述。同樣地，雖然在該圖式中之視圖為了容易說明通常顯示類似的方向，但在該圖式中之說明對於大多

數部分是任意方向的。通常，本發明可以以任何方向來進行。

【0031】在此所使用之名詞「系統」係依據該名詞所使用之上下文而意指及定義為本發明之該方法及該裝置。在此所使用之名詞「方法」係意指及定義為裝置之操作步驟。

【0032】為求便利性及不做限制性，名詞「資料」是定義為能夠藉由電腦產生或儲存於電腦中之資訊。名詞「資料保全系統」是定義為意指合併儲存媒介之任何可攜式記憶體裝置。在此所使用之名詞「儲存媒介」意指及定義為任何固態、反及閘快閃及/或磁性資料記錄系統。名詞「上鎖」意指當儲存媒介不可存取時之資料保全系統並且名詞「解鎖」意指當儲存媒介是可存取時之資料保全系統。

【0033】通常有兩種方法防止儲存裝置篡改：

1.塗敷環氧樹脂於組件上-塗敷至印刷電路板之環氧樹脂可以使得在不破壞儲存媒介之情況下拆解該儲存裝置變得困難。

2.加密記憶體資料-當資料寫入儲存媒介時對資料進行加密並且該資料需要加密金鑰才得以解密。

【0034】現參考第1圖，其中依據本發明之實施例顯示資料保全系統100之示意圖。該資料保全系統100由外部通訊通道102、認證次系統104及儲存次系統106所組成。

【0035】該儲存次系統106為包含介面控制器108、

加密引擎 110 及儲存媒介 112 之電子電路。該儲存媒介 112 可以是內部或外部硬碟、USB 快閃隨身碟、固態硬碟、複合磁碟機、記憶卡、卡式磁帶及包含光碟（例如，藍光光碟、數位多功能影音光碟或 DVD 及雷射唱片或 CD）之光學媒介。該儲存媒介 112 可以包含資料保護應用、檔案儲存系統及雲端資料儲存系統。該雲端資料儲存系統可以是使用插件（plug-in 或“plugin”）應用或安裝在瀏覽器內之擴充軟體而存取，不論是在該主機電腦上或經由有線或無線網路（諸如射頻或光學）、或者透過全球資訊網（World Wide Web）連接至該主機電腦之另一個系統上。

【0036】介面控制器 108 包含電子組件，諸如具有軟體或硬體之加密引擎 110 的微控制器，但該加密引擎 110 也可以是在儲存次系統 106 中不同的控制器內。

【0037】該認證次系統 104 為包含認證控制器 114（諸如微控制器）之電子電路，該認證控制器 114 可以具有屬於自己的非揮發性記憶體，諸如電子可抹除可程式化唯讀記憶體（EEPROM，Electrically Erasable Programmable Read-Only Memory）。

【0038】該外部通訊通道 102 提供與主機電腦系統 120 交換資料之工具。萬用序列匯流排（USB）為連接該資料保全系統 100 至該主機電腦系統 120 的其中一個最普遍的工具。該外部通訊通道 102 之其它例子包含火線（Firewire）、無線 USB、序列 ATA（SATA）、高畫質多媒體介面（HDMI，High Definition Multimedia Interface）、推

薦標準 232（RS-232，Recommended Standard 232）及射頻無線網路。

【0039】 該介面控制器 108 是能夠將 USB 封包資料轉譯成為可以寫入 USB 快閃隨身碟中之該儲存媒介 112 的資料。

【0040】 該加密引擎 110 是實作該介面控制器 108 之一部分並且從該主機電腦系統 120 取得明確的文字及/或資料（資訊）然後轉換該文字及/或資料成為寫入該 MSD 或該儲存媒介 112 之加密形式。該加密引擎 110 亦將來自該儲存媒介 112 之加密資訊轉換並且解密成為明確的資訊給該主機電腦系統 120。該加密引擎 110 亦可以是一個雙控制器次系統，其具有：加密控制器，具有動態加密/解密資料連同管理通訊協定、記憶體及其它操作條件的加密能力；以及通訊/保全控制器，用於處理該通訊、加密金鑰管理及與該加密控制器通訊。

【0041】加密引擎 110 需要加密金鑰 116 來加密/解密資訊。該加密金鑰 116 是使用於一種演算法（例如，256 位元高級加密標準（AES，Advanced Encryption Standard）加密）中，該演算法藉由加密演算法分別地加密/解密資料以使資料成為不可讀的或可讀的。該加密金鑰 116 可以儲存至該認證控制器 114 內部或外部。

【0042】 一旦具有身份識別號碼或金鑰之使用者 122 已經對照認證金鑰 118 進行確認，該加密金鑰 116 就會藉由該認證次系統 104 傳輸至該加密引擎 110。

【0043】 已經發現到，藉由使用該認證金鑰 118 及該加密金鑰 116，本發明之各種實施例之可攜式記憶體儲存裝置可以提供先前在此類裝置中無法獲得之極高程度的保全。

【0044】 當該資料保全系統 100 被上鎖時，該認證金鑰 118 仍然在該認證次系統 104 內部並且無法由外部讀取。隱藏該認證金鑰 118 的其中一個方法是將該認證金鑰 118 儲存於該認證次系統 104 內之該認證控制器 114 中。該認證控制器 114 設置安全熔絲使得無法存取該認證金鑰 118，除非該使用者 122 已被確認時該認證控制器 114 允許提取。很多微控制器配備有當燒斷時避免存取任何內部記憶體之安全熔絲。這是眾所周知及廣泛使用的保全特徵。此類微控制器可以使用於該認證控制器 114。該認證控制器 114 可以是微控制器或微處理器。

【0045】 該認證金鑰 118 可以用作為數種功能形式：

1．作為該加密金鑰 116，用以直接加密/解密該資訊。

2．作為金鑰，用以回復儲存於可以由該介面控制器 108 所存取之該資料保全系統 100 中之該加密金鑰 116。

3．用於供該介面控制器 108 直接比較以啟動該外部通訊通道 102。

【0046】 現參考第 2 圖，其中顯示配合該資料保全系統 100 所使用之認證金鑰交付方法之說明。在這個說明中，該認證金鑰 118 及該加密金鑰 116 合在一起並且相同。該加密引擎 110 使用該認證金鑰 118 作為該加密金鑰 116。

【0047】該使用者 122 必須藉由提供使用者身份識別 202、號碼或金鑰至該認證次系統 104 而與該認證次系統 104 互動。該認證次系統 104 對照該認證金鑰 118 驗證該使用者 122。該認證次系統 104 接著傳輸該認證金鑰 118 作為該加密金鑰 116 至該介面控制器 108。

【0048】在該介面控制器 108 中之該加密引擎 110 使用該認證金鑰 118 以沿著通道 206 將明確的資訊轉換成為加密的資訊及將加密的資訊轉換成為明確的資訊。在沒有該加密金鑰 116 的情況下，任何從該儲存媒介 112 讀取加密資訊的嘗試通常會造成任何電腦無法採用之資訊。

【0049】現參考第 3 圖，其中顯示供該使用者 122 與資料保全系統 300 互動之不同的系統。該互動可以是藉由通訊組合 301，該通訊組合 301 可以是與行動電話、智慧手機、智能手錶、穿戴應用或其它無線裝置之實體接觸、有線連接或無線連接。

【0050】在其中一個認證系統中，行動收發器 302 係用以傳輸使用者身份識別 304 至位於認證次系統 310 中之資料保全收發器 306。為了例示性之目的，收發器是用於雙向通訊的靈活性，但是也可使用單向的傳輸之發送器-接收器組合。該認證次系統 310 包含該認證控制器 114，該認證控制器 114 是連接至位於該儲存次系統 106 中之該介面控制器 108。該使用者身份識別 304 是藉由來自該資料保全系統 300 之該儲存次系統 106 外部之該行動收發器 302 提供至該認證次系統 310 內之該資料保全收發器 306。

該無線通訊可以包含無線保真（WiFi，Wireless Fidelity）、藍芽（BT，Bluetooth）、藍芽智能、近場通訊（NFC，Near Field Communication）、全球定位系統（GPS，Global Positioning System）、光學、行動通訊（例如，長期演進技術（LTE，Long-Term Evolution）、先進長期演進技術（LTE-A，Long-Term Evolution Advanced））、分碼多重存取（CDMA，Code Division Multiple Access）、寬頻分碼多重存取（WCDMA，Wideband Code Division Multiple Access）、通用移動電信系統（UMTS，Universal Mobile Telecommunications System）、無線寬帶（WiBro，Wireless Broadband）或全球移動通訊系統（GSM，Global System for Mobile Communications）及類似技術。

【0051】 該認證次系統 310 藉由從對照該認證金鑰 118 而被驗證之該行動收發器 302 所發送之碼而驗證對照該認證金鑰 118 之該使用者 122。該認證次系統 310 接著跨越該通訊組合 301 傳輸該加密金鑰 116 給該介面控制器 108。

【0052】 該加密引擎 110 接著使用該加密金鑰 116 沿著該通道 206 以將明確的資訊轉換成為加密的資訊及將加密的資訊轉換成為明確的資訊。在沒有該加密金鑰 116 的情況下，任何從該儲存媒介 112 讀取加密資訊的嘗試都會造成該主機電腦系統 120 無法使用之資訊。

【0053】 在視需要的第二認證機制中，藉由讓該使用者 122 使用生物識別感測器 320 提供生物識別輸入 322 而

確認他/她的身份識別是授權的使用者，該認證次系統 310 便能對照該認證金鑰 118 驗證該使用者 122。生物識別的類型包含指紋、虹膜掃描、聲紋等等。

【0054】 在視需要的第三認證機制中，藉由讓該使用者 122 使用電機輸入機制 330 提供唯一碼 332 而確認他/她的身份識別是授權的使用者，該認證次系統 310 便能對照該認證金鑰 118 驗證該使用者 122。該唯一碼 331 可以包含數字碼、字母與數字組成的碼或字母碼，例如 PIN。該電機輸入機制 330 是位在該認證次系統 310 內部。該電機輸入機制 330 從該資料保全系統 300 外部接收來自該使用者 122 之唯一碼 332。該唯一碼 332 是提供給位在該資料保全系統 300 之該儲存次系統 106 外部之該認證次系統 310 內之該電機輸入機制 330。

【0055】 不論使用哪個方法驗證該使用者 122，該認證金鑰 118 及該加密金鑰 116 仍然維持隱藏直到該使用者獲得授權。

【0056】 現參考第 4 圖，其中顯示該使用者 122 如何可以使用該主機電腦系統 120 與資料保全系統 400 互動之說明。

【0057】 該主機電腦系統 120 設有主機應用程式 402。該主機應用程式 402 為軟體或韌體，透過該資料保全系統 400 之外部通訊通道 102 進行通訊。

【0058】 該主機應用程式 402 交付與其環境相關聯之主機識別碼 406，諸如內部組件序號（例如，硬碟）、網路

卡之媒體存取控制（MAC，Media Access Control）位址、使用者之登入名稱、網際網路協定（IP，Internet Protocol）位址、由該資料保全系統所建立並儲存至該主機之 ID、由該資料保全系統所建立並儲存至該網路之 ID 等等。該主機識別碼 406 是由位於該資料保全系統 400 中之認證次系統 408 所使用。

【0059】 當該認證次系統 408 藉由確認該主機識別碼 406 而對照該認證金鑰 118 驗證該使用者 122 時，該資料保全系統 400 將解鎖。

【0060】 例如，使用者 122 將被上鎖之資料保全系統 400 連接至主機電腦系統 120。主機應用程式 402 發送本身的網路卡之 MAC 位址給該資料保全系統 400。該資料保全系統 400 認知這個 MAC 位址是合法的並解鎖而不需要第 1 圖之該使用者 122 必須輸入使用者身份識別。這種實作並不需要與該使用者 122 做任何互動。在這個例子中，被驗證的是該主機電腦系統 120 以及與其相關聯的環境。

【0061】 該資料保全系統 400 包含：提供儲存於該認證次系統 104 內之該認證金鑰 118；藉由該認證次系統 104 提供該主機電腦系統 120 之確認；藉由該認證次系統 104 提交該保加密金鑰 116 給該儲存次系統 106；以及藉由該儲存次系統 106 解密該儲存媒介內容而提供存取該儲存媒介 112。

【0062】 該資料保全系統更包含用於判讀該生物識別輸入並確認該使用者 122 的該認證次系統 104。

【0063】該資料保全系統更包含直接使用該認證金鑰118作為該加密金鑰116。

【0064】該資料保全系統更包含使用該認證金鑰118以解密及提取用以解碼內部內容的該加密金鑰116。

【0065】該資料保全系統更包含用於判讀訊號輸入及確認發送單元的該認證次系統104。

【0066】該資料保全系統更包含用於判讀人工鍵入的輸入並確認該使用者122的該認證次系統104。

【0067】該資料保全系統更包含用於判讀由主機常駐軟體應用程式所發送之輸入來確認該主機電腦系統120的該認證次系統104。

【0068】該資料保全系統更包含在該介面控制器108外部但連接至該外部通訊通道102之該加密引擎110，用於將明確資料轉換成為加密資料以用於解鎖該資料保全系統100。

【0069】現參考第5圖，其中顯示針對該資料保全系統100之使用者確認之資料保全方法500。該資料保全方法500包含：在步驟方塊502中對照認證金鑰而確認使用者；在步驟方塊504中使用該認證金鑰用於提取加密金鑰；以及在步驟方塊506中使用該加密金鑰用於透過在主機電腦系統與儲存媒介之間之儲存次系統允許未加密的通訊。

【0070】現參考第6圖，其中顯示例示性的資料保全通訊系統600。例示性的資料保全通訊系統600包含行動

裝置 610、資料保全系統 620、主機電腦 630 及伺服器/控制台 640。該行動裝置 610 及該伺服器/控制台 640 是透過雲端 650 而以有線或無線方式連接，該雲端 650 可以是網際網路雲端。該行動裝置 610 及該資料保全系統 620 是藉由該通訊組合 301 所連接。

【0071】 在該例示性的資料保全通訊系統 600 中，該通訊組合 301 包含位於該行動裝置 610 中之行動收發器 612，其具有天線 614 與位在該資料保全系統 620 中之資料保全收發器 624 之天線 622 無線地通訊。

【0072】 在其中一項實施例中，該行動裝置 610 可以是智慧手機。在該行動裝置 610 中，該行動收發器 612 可以連接至習知的行動裝置組件及連接至資料保全系統應用程式 618，該行動收發器 612 提供資訊給該資料保全系統 620 使用。

【0073】 該資料保全收發器 624 是連接至保全控制器 626，該保全控制器 626 可以含有身份識別、密碼、個人資料或包含可以存取該資料保全系統 620 之不同的行動裝置之資訊。該保全控制器 626 為連接至類似該認證次系統 310、該儲存次系統 106（在某些實施例中，該儲存次系統 106 可以具有加密以加密資料）及該外部通訊通道 102 之次系統。

【0074】 該外部通訊通道 102 可連接至該主機電腦 630 以允許在特定環境下存取在該儲存次系統 106 中之資料。

【0075】該資料保全系統620之其中一項實施例可以僅利用無線連接至該行動裝置610，諸如智慧手機，從而消除第3圖之該生物識別感測器320及該電機輸入機制330。已經發現到，這種實作使得該資料保全系統620更加安全及有用。

【0076】該資料保全系統應用程式618允許該行動裝置610找到位在該行動裝置610附近之所有資料保全系統並且顯示出他們的狀態（上鎖/解鎖/空白、配對/未配對等等）。

【0077】該資料保全系統應用程式618允許該行動裝置610連接/配對、上鎖、解鎖、改變名稱及密碼，並且重置位在該資料保全系統620上之所有資料。

【0078】該資料保全系統應用程式618允許該行動裝置610設定閒置自動上鎖（inactivity auto-lock），以便在預定的閒置時間週期後使該資料保全系統620自動地上鎖，或者設定感應自動上鎖（proximity auto-lock），使得當該行動裝置610沒有位於預定感應距離內持續預定的時間週期時，該資料保全系統620將會上鎖（以改良可靠度及避免訊號彈跳）。

【0079】該資料保全系統應用程式618允許該行動裝置610記住密碼、使用TouchID及Apple手錶（在此所提及的TouchID及Apple手錶兩者僅為例子，有很多能夠以類似模式使用之具有生物識別感測器及可穿戴裝置的其它行動裝置）以便資料保全系統620可以解鎖而不需要在該

行動裝置上輸入重新進入的密碼。

【0080】該資料保全系統應用程式618允許該行動裝置610經由設定使得僅與特定的行動裝置產生操作，諸如該行動裝置610，以便該資料保全系統620無法用其它行動裝置解鎖（1Phone）。

【0081】該資料保全系統應用程式618允許該行動裝置610設定該資料保全系統620為唯讀。

【0082】該資料保全系統應用程式618允許該行動裝置610以使用者模式或管理者模式（管理者的模式覆蓋使用者的設定）操作並且使用該伺服器/控制台640。該伺服器/控制台640為電腦與控制台的組合，該控制台用於輸入資訊進入該電腦。

【0083】該伺服器/控制台640含有使用者管理資料庫642，該使用者管理資料庫642含有可以經由雲端650傳輸至該行動裝置610之額外資訊，以提供額外的功能性給該行動裝置610。

【0084】該使用者管理資料庫642允許該伺服器/控制台640建立及確認使用UserID（使用者名稱及密碼）之使用者及阻擋/允許解鎖該資料保全系統620及提供遠端輔助。

【0085】該使用者管理資料庫642允許該伺服器/控制台640遠端重置或解鎖該資料保全系統620。

【0086】該使用者管理資料庫642允許該伺服器/控制台640遠端變更該資料保全系統使用者的PIN。

【0087】 該使用者管理資料庫 642 允許該伺服器/控制台 640 從特定位置（藉由使用地理圍欄）限制/允許解鎖資料保全系統 620。

【0088】 該使用者管理資料庫 642 允許該伺服器/控制台 640 限制/允許在特定的時間週期及不同的時間區域中解鎖資料保全系統 620。

【0089】 該使用者管理資料庫 642 允許該伺服器/控制台 640 限制解鎖在特定團隊/組織/網路等等外部之資料保全系統 620。

【0090】 現參考第 7 圖，其中顯示呈現在該行動裝置 610 及該資料保全系統 620 之間之操作順序之管理者排序圖。

【0091】在該資料保全系統 620 及該行動裝置 610 之間的連接 700 首先建立和其它裝置或系統的彼此發現、配對該裝置及系統及連線該裝置與系統。該連接 700 是使用共享秘密而保全，接著使用該共享秘密以保全（加密）在該資料保全系統 620 及該行動裝置 610 之間之通訊而用於所有的未來通訊對話。標準加密演算法係被選擇成既可在該資料保全系統 620 上有效執行又可被全球保全標準所認可。

【0092】 只要該資料保全系統 620 及該行動裝置 610 是在彼此之預定距離內，該連接 700 便由該資料保全系統應用程式 618 或該保全控制器 628 或兩者一起操作所維持。再者，若超過該預定距離時，該連接 700 會維持預定

的時間週期，在該時間週期之後該資料保全系統 620 便上鎖。

【0093】 在該行動裝置 610 及該資料保全系統 620 連接之後，資料保全系統管理者應用程式啟動操作 702 於該行動裝置 610 中產生。接著管理者於管理者密碼操作 704 中設定密碼。而且在該行動裝置 610 與該資料保全系統 620 連接之後，該資料保全系統 620 在資料保全系統連接、啟動及發現操作 706 中是連接至第 6 圖之該主機電腦 630 而由該主機電腦 630 啟動及發現。

【0094】 在該管理者密碼操作 704 之後，該行動裝置 610 發送設定管理者密碼及解鎖訊號 708 給該資料保全系統 620。該設定管理者密碼及解鎖訊號 708 造成管理者密碼設定及資料保全系統解鎖操作 716 於該資料保全系統 620 中產生。

【0095】 當該管理者密碼設定及資料保全系統解鎖操作 716 完成時，確認：資料保全系統解鎖訊號 712 是發送至該行動裝置 610，在該行動裝置 610 中，確認：資料保全系統解鎖作為管理者操作 714 操作。該確認：資料保全系統解鎖作為管理者操作 714 允許設定其它限制操作 716 使用該行動裝置 610 而執行。該設定其它限制操作 716 造成設定管理者限制訊號 718 發送至該資料保全系統 620，其中該管理者限制被設定並且確認：限制設定訊號 720 回到該行動裝置 610。之後，該行動裝置 610 及該資料保全系統 620 是在完全可操作的通訊中。

【0096】因為能夠在不與該資料保全系統 620 實體接觸的情況下與該資料保全系統 620 通訊，所以與該資料保全系統 620 的大量互動是需要有資料保全系統唯一識別碼來完成，而該資料保全系統唯一識別碼是印在該資料保全系統 620 上或是附帶在該資料保全系統 620 封包，並且對於該資料保全系統 620 擁有者而言是輕易可取得的。

【0097】在做出可能影響使用者資料之請求時（諸如解鎖或重置該資料保全系統 620），需要這種唯一識別碼（unique ID）。未具有正確識別碼而執行這種操作的嘗試將會被忽略並且不造成傷害。該唯一識別碼是用來以一種需要使用者對該資料保全系統 620 有實體控制的方式對該行動裝置 610 識別該資料保全系統 620，以及用來確認該連接 700 是建立在已授權、先前已配對之裝置及系統之間，諸如該行動裝置 610 及該資料保全系統 620。一旦這些裝置被配對，便可使用該共享祕密以使通訊加密。

【0098】配對意味著行動裝置及資料保全系統具有建立在過去某個時間並且持續之唯一且定義的關係。

【0099】當使用者具有該資料保全系統之實體控制時，該唯一識別碼能夠給予該使用者對該資料保全系統有某些控制。

【0100】在行動裝置 610 是智慧手機的情況下，為了增加與資料保全系統 620 通訊之保全，使用者可以選擇啟用功能，例如在此稱為 1Phone 之功能。此功能將與資料保全系統 620 的大量使用者互動限制給一個且只有一個行動

裝置 610。這是藉由以在該資料保全系統 620 與該行動裝置 610 之間保全地共享之隨機識別碼取代上文所描述之該資料保全系統唯一識別碼而完成。因此，例如，當該使用者解鎖該資料保全系統 620 時，必須改為給定該 1Phone 識別碼，而不是呈現該資料保全系統唯一識別碼。在效果上，除了 PIN 或密碼之外，這方式使得使用者的行動裝置 610 成為用於使用該資料保全系統 620 之第二個認證因素。例如，經選擇做為「1Phone」之已配對的使用者手機可以在沒有 PIN 的情況下使用，並且作為使用者認證單一因素及/或在與任何其它使用者認證因素之組合中。若選擇了此類功能（1Phone），除了之前管理者的解鎖有被啟用，否則該資料保全系統 620 無法以任何其它手機開啟。

【0101】 將會瞭解的是，其它實施例可能會在該資料保全系統 620 上要求管理者的密碼以利於使用該 1Phone 功能。另一個實施例可能要求在在該行動裝置 610 上的 1Phone 資料遺失的情況下，該伺服器/控制台 640 能夠回復該資料保全系統 620。

【0102】 該使用者對於該資料保全系統 620 可以啟用感應自動上鎖功能。在通訊對話期間，第 6 圖之該資料保全收發器 624 回報給資料保全系統 620 對於該行動裝置 610 之訊號強度量測。在該行動裝置 610 上之該資料保全系統應用程式 618 發送給該資料保全系統 620 該初始訊號功率水準及用於感應之閾值兩者。

【0103】 因為該訊號強度會因為該收發器周圍之環境

條件而變動，所以該資料保全系統 620 會以數學方式平滑化該訊號強度量測以降低假陽性(false positive)的可能性。當該資料保全系統 620 偵測到所接收的訊號功率已經降到低於預定閾值持續預定的時間週期時，將會立即上鎖該資料保全系統 620 及避免存取第 6 圖之該儲存次系統 106。

【0104】該資料保全系統 620 可以使用於三個不同模式中：使用者模式，其中該資料保全系統 620 之功能性是由使用者所決定；管理者模式，其中管理者可以設定管理者密碼及強制某些限制於該資料保全系統 620（例如，在預定的無活動週期後自動上鎖、唯讀、1Phone）上並且限制不能被使用者移除；以及伺服器模式，其中管理者角色被設定，該伺服器/控制台 640 可以遠端重置該資料保全系統 620、變更使用者密碼或只是解鎖該資料保全系統 620。

【0105】現參考第 8 圖，其中顯示該行動裝置 610 為認證因素之解鎖排序圖。該圖顯示由來自特定行動裝置(該行動裝置 610）之該資料保全系統應用程式 618 所初始化之該資料保全系統 620 之自動解鎖程序。使用者可以使用僅其中一個與該資料保全系統 620 初始配對之行動裝置。若該配對的行動裝置 610 遺失，則該資料保全系統 620 可能無法解鎖（除非之前設定有如第 7 圖中所顯示的管理者密碼）。

【0106】類似於第 7 圖，在該連接 700 建立之後，資料保全系統應用程式啟動操作 800 產生。在資料保全系統

連接、啟動及發現操作 706 之後，需要行動裝置 ID 解鎖訊號 802 便從該行動裝置 610 發送至該資料保全系統 620。資料保全系統解鎖操作 804 產生，然後從該資料保全系統 620 發送確認：資料保全系統解鎖訊號 712。在確認：資料保全系統解鎖操作 806 之後，該行動裝置 610 及該資料保全系統 620 便在完全可操作的通訊中。

【0107】若個人身份識別碼（PIN，Personal Identification Number）並未設定，則已配對的行動裝置是使用作為單一認證因素(1-authentication factor)。

【0108】現參考第 9 圖，其中顯示呈現從該行動裝置 610 使用 PIN 輸入而解鎖之解鎖排序圖。該圖顯示藉由輸入 PIN 於該行動裝置 610 中之該資料保全系統應用程式 618 內而解鎖該資料保全系統 620 之流程。

【0109】雖然類似於第 7 及 8 圖，但輸入使用者名稱/密碼操作 900 在該資料保全系統應用程式啟動操作 800 之後產生。在該輸入使用者稱/密碼操作 900 之後，該行動裝置 610 發送確認使用者 ID 訊號 902 給該伺服器/控制台 640。該伺服器/控制台 640 接著做出使用者名稱/密碼有效判定 904。

【0110】當該使用者名稱/密碼有效判定 904 確認該使用者時，有效使用者訊號 906 是發送至該行動裝置 610 以供使用者於行動裝置 610 中之輸入 PIN 操作 908 輸入正確的 PIN。該行動裝置 610 接著發送確認解鎖訊號 910 以判定是否正確的 PIN 已經輸入至該伺服器/控制台 640。

【0111】 該伺服器/控制台 640 做出使用者授權判定 912 而判定是否該使用者被授權使用該 PIN 被授權的特定資料保全系統，例如該資料保全系統 620。若被授權，則將解鎖允許訊號 914 發送至該行動裝置 610，該行動裝置 610 便傳遞解鎖請求訊號 916 至該資料保全系統 620。

【0112】 該資料保全系統解鎖操作 804 將進行並將確認：資料保全系統解鎖訊號 712 發送至將進行確認：資料保全系統解鎖操作 806 的該行動裝置 610。

【0113】 現參考第 10 圖，其中顯示呈現經由該伺服器/控制台 640 使用 PIN 輸入及使用者 ID/位置/時間確認而解鎖之解鎖排序圖。該圖藉由從該行動裝置 610 輸入 PIN 於該資料保全系統應用程式 618 中、使用 UserID（使用者名稱/密碼）於該伺服器/控制台 640 伺服器中認證及藉由確認地理圍欄允許而於特定位置及於特定時間範圍解鎖該資料保全系統 620，顯示解鎖該資料保全系統 620 之最安全的流程。在沒有輸入 PIN、使用者名稱及密碼及讓行動裝置 610 位於特定（預定）位置及特定（預定）時間的情況下，該資料保全系統 620 無法解鎖。

【0114】 雖然類似於第 7-9 圖，但在該伺服器/控制台 640 處，將執行解鎖特定資料保全系統操作 1000 以允許所需的條件之設定，在該條件之下將操作特定資料保全系統，例如該資料保全系統 620，。例如，該條件可以在特定的地理區域內及/或特定的時間範圍內。

【0115】 在該行動裝置 610 處，將作出目前條件的判

定，例如獲得的位置及/或目前的時間操作 1002。將進行此操作以判定該行動裝置 610 位在何處或該行動裝置 610 所在處之目前時間為何。亦可以判定關於該行動裝置 610 之其它的目前條件並藉由確認解鎖訊號 1004 發送至做出條件符合判定 1006 之該伺服器/控制台 640。

【0116】 當所需的條件符合時，解鎖允許訊號 1008 便發送至該行動裝置 610 以供執行輸入 PIN 操作 908。在輸入該 PIN 之後，確認解鎖訊號 1010 是連同 PIN 及在操作上感應該行動裝置 610 之該資料保全系統 620 之身份識別一起發送。該確認解鎖訊號 1010 是被該伺服器/控制台 640 所接收並且做出資料保全系統允許判定 1012 以判定特定的資料保全系統是允許由授權的使用者所解鎖。該伺服器/控制台 640 確認這個「特定的」使用者是經過授權以使用該特定的資料保全系統。

【0117】 在判定已經提供正確的資訊之後，該伺服器/控制台 640 將提供解鎖允許訊號 914 至該行動裝置 610，該行動裝置 610 將提供解鎖請求訊號 916。該解鎖請求訊號 916 造成該資料保全系統 620 進行操作。

【0118】 現參考第 11 圖，其中顯示使用該伺服器/控制台 640 重置該資料保全系統 620 之重置排序圖。此圖顯示經由該伺服器/控制台 640 遠端地重置該資料保全系統 620 的能力。該資料保全系統 620 可以經由無線連接僅從該行動裝置 610 接收指令。然而，藉由設定「重置」旗標於該伺服器/控制台 640 上用於特定的資料保全系統（使用

本身的序號（S/N）），在該行動裝置 610 上運行之該資料保全系統應用程式 618 將向該伺服器/控制台 640 查詢於該使用者管理資料庫 642 中之任何旗標/未決的請求。當該使用者連接該資料保全系統 620 時，在該行動裝置 610 上之該資料保全系統應用程式 618 將執行等待「重置」指令。在成功的重置（所有使用者資料及憑證消失）之後，該伺服器/控制台 640 將移除該重置旗標以便當該行動裝置 610 連接至該特定資料保全系統時，該重置在下一次將不會執行。

【0119】 雖然類似於第 7-11 圖，但該行動裝置 610 回應於有效使用者訊號 906 以發送任何指令等待訊號 1100 至該伺服器/控制台 640 以做出重置指令判定 1102。當該重置指令出現時，執行重置訊號 1104 將發送至該行動裝置 610。

【0120】 該行動裝置 610 將發送重置保全系統訊號 1106 至該資料保全系統 620 以開始資料保全系統重置操作 1108。一旦該資料保全系統重置操作 1108 完成之後，該資料保全系統 620 將發送確認：資料保全系統重置訊號 1110 至該行動裝置 610 以設定確認：資料保全系統重置操作 1112 進入操作。之後，該行動裝置 610 及該資料保全系統 620 便與該資料保全系統 620 重置在完全可操作的通訊狀態下。

【0121】 現參考第 12 圖，其中顯示使用該伺服器/控制台 640 解鎖該資料保全系統 620 之解鎖排序圖。此圖顯示經由該伺服器/控制台 640 遠端地解鎖該資料保全系統

620 的能力。該資料保全系統 620 可以經由無線連接僅從該行動裝置 610 接收指令。然而，藉由設定「管理者解鎖」旗標於該伺服器/控制台640控制台上用於特定資料保全系統（使用本身的序號（S/N）），在該行動裝置 610 上運行之該資料保全系統應用程式 618 將向該伺服器/控制台 640 查詢任何旗標/未決的請求。當該使用者連接該資料保全系統 620 時，在該行動裝置 610 上之該資料保全系統應用程式 618 將執行等待”管理者解鎖”指令。在成功的管理者解鎖之後，該使用者的資料維持不變，但是該使用者的密碼會被移除（該資料保全系統 620 無法由該使用者解鎖）。該伺服器/控制台 640 將移除用於該資料保全系統 620 之重置旗標，因此當該行動裝置 610 連接至該資料保全系統 620 時，該重置在下一次將不會執行。

【0122】 雖然類似於第 7-11 圖，但在接收任何指令等待訊號 1100 之後，當有以管理者的密碼解鎖的指令時，該伺服器/控制台 640 執行解鎖 1200。以管理者的密碼解鎖訊號 1202 是發送至該行動裝置 610，該行動裝置 610 提供以管理者的密碼解鎖訊號 1204 至該資料保全系統 620 以開始該資料保全系統解鎖操作 804。之後，該行動裝置 610 及該資料保全系統 620 便在完全可操作的通訊狀態下。

【0123】 現參考第 13 圖，其中顯示使用該伺服器/控制台 640 之變更使用者密碼的排序圖。此圖顯示經由該伺服器/控制台 640 遠端地變更用於資料保全系統 620 之使用者密碼的能力。即使資料保全系統 620 可以經由無線連

接僅從該行動裝置 610 接收指令，但藉由設定「變更使用者密碼」旗標於該伺服器/控制台 640 控制台上用於特定的資料保全系統（使用本身的序號（S/N）），在該行動裝置 610 上運行之該資料保全系統應用程式 618 將向該伺服器/控制台 640 查詢任何旗標/未決的請求。當使用者將連接他的資料保全系統 620 時，在行動裝置 610 上之資料保全系統應用程式 618 將執行等待「變更使用者密碼」指令。在成功的解鎖及變更密碼之後，該使用者的資料維持不變並且該資料保全系統 620 可以用新的使用者密碼解鎖。該伺服器/控制台 640 將移除用於該資料保全系統 620 之「變更使用者密碼」旗標，因此當該行動裝置 610 是連接至該特定資料保全系統時，該變更使用者密碼旗標在下一次將不會執行。

【0124】 雖然類似於第 7-12 圖，該伺服器/控制台 640 藉由做出變更密碼判定 1300 以回應於任何指令等待訊號 1100。當在該伺服器/控制台 640 處已經有密碼變更時，變更使用者密碼訊號 1302 是發送至該行動裝置 610，該行動裝置 610 發送變更使用者密碼訊號 1304 至該資料保全系統 620。之後，該行動裝置 610 及該資料保全系統 620 是以新的密碼在完全可操作的通訊狀態下。

【0125】 資料保全系統之操作之方法包括：提供具有用於與該資料保全系統連接之資料保全系統應用程式之行動裝置；開始該資料保全系統應用程式；以及維持該資料保全系統與該行動裝置之連接。

【0126】 如同上文所描述之方法，其中，維持該連接是當該資料保全系統在該行動裝置之預定感應距離內時維持連接。

【0127】 如同上文所描述之方法，其中，維持該連接之是當該資料保全系統在該行動裝置之預定感應距離內持續預定的時間週期時維持連接。

【0128】 如同上文所描述之方法，其中，建立該連接包含使用在該資料保全系統與該行動裝置之間之雙向通訊。

【0129】 如同上文所描述之方法，其中，建立該連接包含使用在該資料保全系統與該行動裝置之間之單向通訊。

【0130】 如同上文所描述之方法，更包括在具有該資料保全系統應用程式之該行動裝置與含有使用者管理資料庫之伺服器之間之通訊。

【0131】 如同上文所描述之方法，更包括提供在該資料保全系統中之保全控制器內之保全資訊。

【0132】 如同上文所描述之方法，更包括：提供具有特定資料保全系統之身份識別之伺服器；提供具有特定身份識別之該資料保全系統；以及當該特定資料保全系統之該身份識別是相同於該資料保全系統之該特定身份識別時，解鎖該資料保全系統。

【0133】 如同上文所描述之方法，其中，提供具有該資料保全系統應用程式之行動裝置提供資料保全系統管理

者的應用程式並且更包含：設定管理者的密碼於該行動裝置中；從該行動裝置傳輸該管理者的密碼至該資料保全系統；以及設定該管理者的密碼於該資料保全系統中並解鎖該資料保全系統。

【0134】 如同上文所描述之方法，更包括：提供結合來自該行動裝置之行動裝置身份識別之解鎖請求至該資料保全系統；以及接收該資料保全系統中之該解鎖請求並解鎖該資料保全系統。

【0135】 如同上文所描述之方法，更包括：輸入使用者名稱或密碼於該行動裝置中；在由該行動裝置接收該使用者名稱或密碼之後，判定何時該使用者名稱或密碼於伺服器中是有效的；當該使用者名稱或密碼有效時，由該伺服器至該行動裝置產生通訊；以及當該使用者名稱或密碼有效而解鎖該資料保全系統時，由該行動裝置至該資料保全系統產生通訊。

【0136】 如同上文所描述之方法，更包括：輸入使用者名稱或密碼於行動裝置中；在由該行動裝置接收該使用者名稱或密碼之後，判定何時該使用者名稱或密碼於伺服器中是有效的；當該使用者名稱或密碼有效時，由該伺服器與該行動裝置產生通訊；在接收來自該行動裝置之身份識別號碼之後，判定何時該身份識別號碼於該伺服器中是有效的；以及當該伺服器判定該身份識別號碼有效時，透過該行動裝置解鎖該資料保全系統。

【0137】 如同上文所描述之方法，更包括：提供該行

動裝置之有效位置至伺服器；判定於該伺服器中何時該行動裝置是在該有效位置內；以及當該伺服器判定該行動裝置是在該有效位置內時，透過該行動裝置解鎖該資料保全系統。

【0138】 如同上文所描述之方法，更包括：提供在該行動裝置處用於該資料保全系統之操作的目前時間給伺服器；判定於該伺服器中何時該行動裝置是在該目前時間內；以及當該伺服器判定該行動裝置具有該目前時間時，透過該行動裝置解鎖該資料保全系統。

【0139】 如同上文所描述之方法，更包括：提供於伺服器中之指令；由該伺服器提供該指令至該行動裝置以回應來自該行動裝置之指令等待訊號；以及當該指令是由該伺服器所提供時，透過該行動裝置執行於該資料保全系統中之該指令。

【0140】 如同上文所描述之方法，更包括：提供於伺服器中之變更密碼指令；由該伺服器提供該變更密碼指令至該行動裝置以回應於來自該行動裝置的變更密碼訊號；以及使用在該資料保全系統中之該變更密碼解鎖該資料保全系統。

【0141】 如同上文所描述之方法，更包括連接該資料保全系統至主機電腦用於啟動並可由該主機電腦發現。

【0142】 資料保全系統包括：資料保全收發器或接收器；可操作地連接至該資料保全收發器或接收器之認證次系統；以及連接至該認證次系統之儲存次系統。

【0143】如同上文所描述之該系統更包括連接至該資料保全收發器或該接收器及連接至該認證次系統之保全控制器。

【0144】如同上文所描述之系統更包括具有資料保全系統應用程式之行動裝置，當該資料保全系統是在該行動裝置的預定感應距離內時，與該保全控制器一起操作以用於維持連接。

【0145】如同上文所描述之該系統更包括具有資料保全系統應用程式之行動裝置，當該資料保全系統是在該行動裝置的預定感應距離內持續預定的時間週期時，與該保全控制器一起操作用於維持連接。

【0146】如同上文所描述之該系統更包括具有用於維持連接之行動收發器或接收器之行動裝置，包含在該資料保全系統與該行動裝置之間使用雙向通訊。

【0147】如同上文所描述之該系統更包括具有用於維持連接之行動收發器或接收器之行動裝置，包含在該資料保全系統與該行動裝置之間使用單向通訊。

【0148】如同上文所描述之該系統更包括在具有資料保全系統應用程式之行動裝置與含有使用者管理資料庫之伺服器之間之有線或無線連接通訊。

【0149】如同上文所描述之該系統，其中，該資料保全系統包含用於連接至主機電腦之外部通訊通道。

【0150】雖然本發明已經結合特定最佳模式做描述，應該瞭解的是很多替代、修正及變化對於熟習該項技藝之

人士依據先前的描述將是顯而易見的。因此，本發明意在涵括落在該包含的申請專利範圍之範疇內之所有此類的替代、修正及變化。在此所提出或顯示於該附加的圖式中之所有的事項應當解讀為說明及限定的意義。

【符號說明】

【0151】

100 資料保全系統

102 外部通訊通道

104 認證次系統

106 儲存次系統

108 介面控制器

110 加密引擎

112 儲存媒介

114 認證控制器

116 加密金鑰

118 認證金鑰

120 主機電腦系統

122 使用者

202 使用者身份識別

206 通道

300 資料保全系統

301 通訊組合

302 行動收發器

304 使用者身份識別

306 資料保全收發器

310 認證次系統

320 生物識別感測器

322 生物識別輸入

330 電機輸入機制

332 唯一碼

400 資料保全系統

402 主機應用程式

406 主機識別碼

408 認證次系統

500 資料保全方法

502 步驟方塊

504 步驟方塊

506 步驟方塊

600 資料保全通訊系統

610 行動裝置

612 行動收發器

614 天線

618 資料保全系統應用程式

620 資料保全系統

622 天線

624 資料保全收發器

626 保全控制器

630 主機電腦

640 伺服器/控制台

642 使用者管理資料庫

650 雲端

700 連接

706 資料保全系統連接、啟動及發現操作

712 確認：資料保全系統解鎖訊號

714 管理者操作

716 設定其它限制操作

800 資料保全系統應用程式啟動操作

802 行動裝置 ID 解鎖訊號

804 資料保全系統解鎖操作

806 確認：資料保全系統解鎖操作

900 輸入使用者名稱/密碼操作

902 確認使用者 ID 訊號

904 使用者名稱/密碼有效判定

906 有效使用者訊號

908 輸入 PIN 操作

910 確認解鎖訊號

912 使用者授權判定

914 解鎖允許訊號

916 解鎖請求訊號

1000 解鎖特定資料保全系統操作

1002 獲得的位置及/或目前的時間操作

1004 確認解鎖訊號

1006 條件符合判定

1008 解鎖允許訊號

1010 確認解鎖訊號

1012 資料保全系統允許判定

1100 任何指令等待訊號

1102 重置指令判定

1104 執行重置訊號

1106 重置保全系統訊號

1108 資料保全系統重置操作

1110 確認：資料保全系統重置訊號

1112 確認：資料保全系統重置操作

1200 解鎖

1202 管理者的密碼解鎖訊號

1204 管理者的密碼解鎖訊號

1300 變更密碼判定

1302 變更使用者密碼訊號

1304 變更使用者密碼訊號

申請專利範圍

1. 一種資料保全系統之操作之方法，包括：

提供具有用於與該資料保全系統連接之資料保全系統應用程式之行動裝置；

開始該資料保全系統應用程式；以及

維持該資料保全系統與該行動裝置之連接。

2. 如申請專利範圍第 1 項所述之方法，其中，維持該連接是維持當該資料保全系統在該行動裝置的預定感應距離內時之該連接。

3. 如申請專利範圍第 1 項所述之方法，其中，維持該連接是維持當該資料保全系統在該行動裝置的預定感應距離內持續預定時間週期時之該連接。

4. 如申請專利範圍第 1 項所述之方法，其中，建立該連接包含在該資料保全系統與該行動裝置之間使用雙向通訊。

5. 如申請專利範圍第 1 項所述之方法，其中，建立該連接包含在該資料保全系統與該行動裝置之間使用單向通訊。

6. 如申請專利範圍第 1 項所述之方法，更包括在具有該資料保全系統應用程式之該行動裝置與含有使用者管理資料庫之伺服器之間之通訊。

7. 如申請專利範圍第 1 項所述之方法，更包括提供保全資訊於該資料保全系統內之保全控制器中。

8. 如申請專利範圍第 1 項所述之方法，更包括：

提供伺服器具有特定資料保全系統之身份識別；

提供該資料保全系統具有特定身份識別；以及

當該特定資料保全系統之該身份識別相同於該資料保全系統之該特定身份識別時，解鎖該資料保全系統。

9. 如申請專利範圍第 1 項所述之方法，其中，提供具有該資料保全系統應用程式的行動裝置提供資料保全系統管理者的應用程式並且更包含：

設定管理者的密碼於該行動裝置中；

從該行動裝置傳輸該管理者的密碼至該資料保全系統；以及

設定該管理者的密碼於該資料保全系統中及解鎖該資料保全系統。

10. 如申請專利範圍第 1 項所述之方法，更包括：

提供解鎖請求連同來自該行動裝置之行動裝置身份識別至該資料保全系統；以及

於該資料保全系統中接收該解鎖請求並解鎖該資料保全系統。

11. 如申請專利範圍第 1 項所述之方法，更包括：

輸入使用者名稱或密碼於該行動裝置中；

在接收來自該行動裝置之該使用者名稱或密碼之後，判定何時該使用者名稱或密碼於伺服器中是有效的；

當該使用者名稱或密碼有效時，由該伺服器通訊至

該行動裝置；以及

當該使用者名稱或密碼有效而解鎖該資料保全系統時，由該行動裝置通訊至該資料保全系統。

12. 如申請專利範圍第 1 項所述之方法，更包括：

輸入使用者名稱或密碼於該行動裝置中；

在接收來自該行動裝置之該使用者名稱或密碼之後，判定何時該使用者名稱或密碼於伺服器中是有效的；

當該使用者名稱或密碼有效時，由該伺服器通訊至該行動裝置；

在接收來自該行動裝置之身份識別號碼之後，判定何時該身份識別號碼於該伺服器中是有效的；以及

當該伺服器判定該身份識別號碼有效時，透過該行動裝置解鎖該資料保全系統。

13. 如申請專利範圍第 1 項所述之方法，更包括：

提供該行動裝置之有效位置給伺服器；

於該伺服器中判定何時該行動裝置是在該有效位置內；以及

當該伺服器判定該行動裝置是在該有效位置內時，透過該行動裝置解鎖該資料保全系統。

14. 如申請專利範圍第 1 項所述之方法，更包括：

提供在該行動裝置處用於該資料保全系統之操作的目前時間至伺服器；

判定於該伺服器中何時該行動裝置是在該目前時

間內；以及

當該伺服器判定該行動裝置具有該目前時間時，透過該行動裝置解鎖該資料保全系統。

15. 如申請專利範圍第 1 項所述之方法，更包括：

提供於伺服器中之指令；

由該伺服器提供該指令至該行動裝置以回應來自該行動裝置之指令等待訊號；以及

當該指令是由該伺服器所提供時，透過該行動裝置執行於該資料保全系統中之該指令。

16. 如申請專利範圍第 1 項所述之方法，更包括：

提供於伺服器中之變更密碼指令；

由該伺服器提供該變更密碼指令至該行動裝置以回應於來自該行動裝置的變更密碼訊號；以及

使用在該資料保全系統中之該變更密碼解鎖該資料保全系統。

17. 如申請專利範圍第 1 項所述之方法，更包括連接該資料保全系統至主機電腦用於啟動及可被該主機電腦發現。

18. 一種資料保全系統，包括：

資料保全收發器或接收器；

認證次系統，可操作地連接至該資料保全收發器或接收器；以及

儲存次系統，連接至該認證次系統。

19. 如申請專利範圍第 18 項所述之系統，更包括保全控制器，連接至該資料保全收發器或該接收器及連接至該認

證次系統。

20. 如申請專利範圍第 18 項所述之系統，更包括具有資料保全系統應用程式之行動裝置，當該資料保全系統在該行動裝置的預定感應距離內時，操作具有用於維持連接之該保全控制器。

21. 如申請專利範圍第 18 項所述之系統，更包括具有資料保全系統應用程式之行動裝置，當該資料保全系統是在該行動裝置的預定感應距離內持續預定時間週期時，操作具有用於維持連接之該保全控制器。

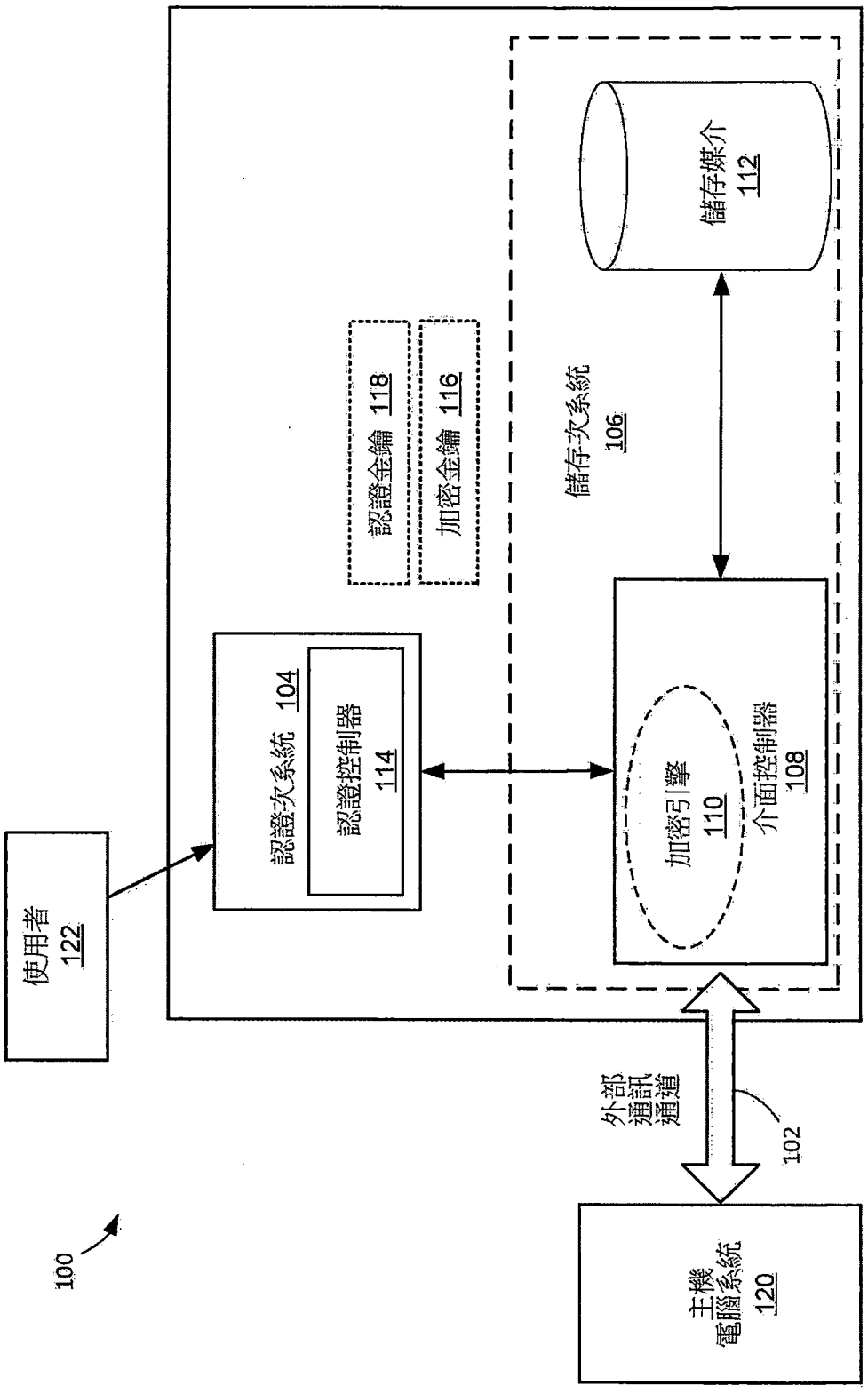
22. 如申請專利範圍第 18 項所述之系統，更包括具有用於維持連接之行動收發器或接收器之行動裝置，包含在該資料保全系統與該行動裝置之間使用雙向通訊。

23. 如申請專利範圍第 18 項所述之系統，更包括具有用於維持連接之行動收發器或接收器之行動裝置，包含在該資料保全系統及該行動裝置之間使用單向通訊。

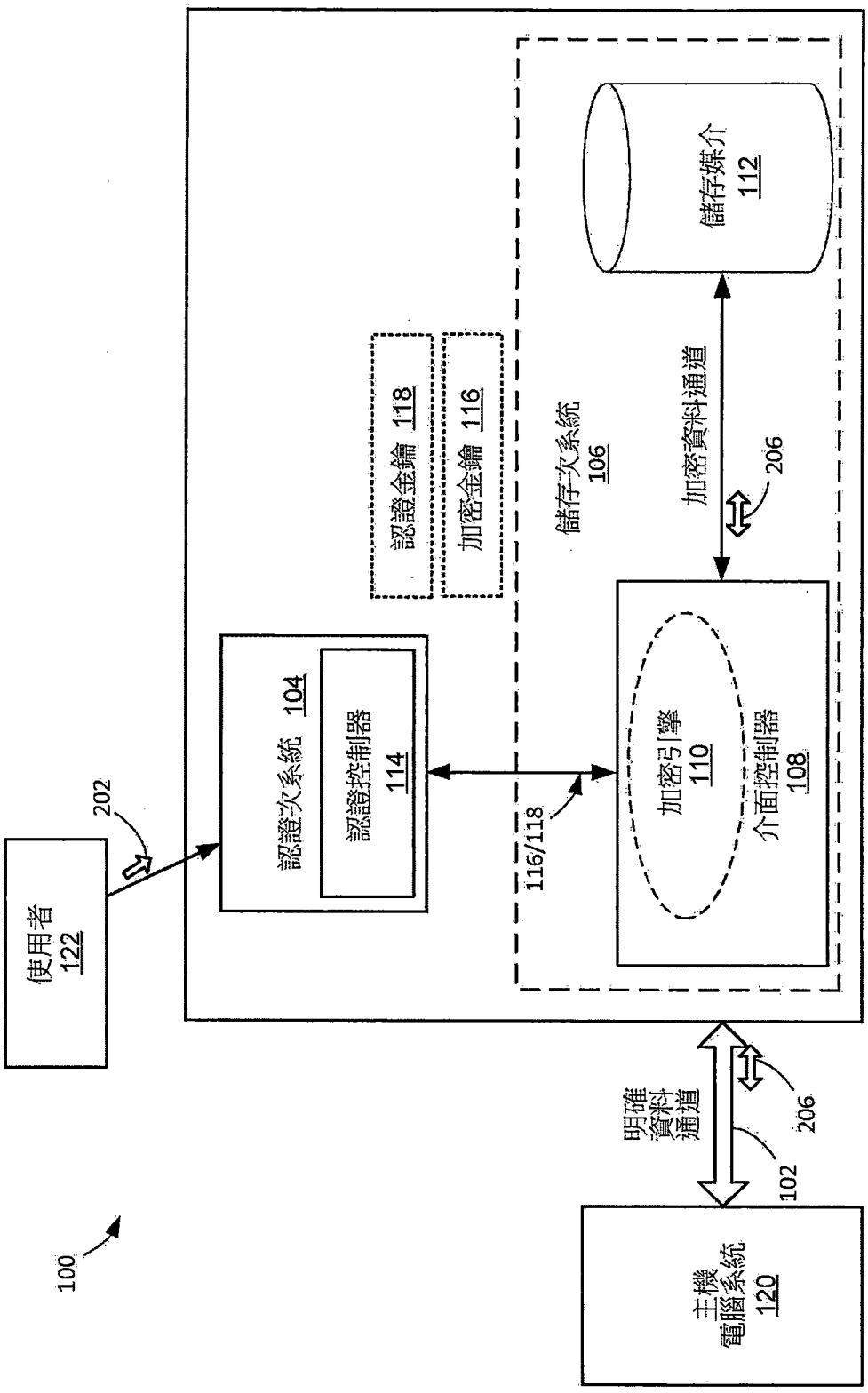
24. 如申請專利範圍第 18 項所述之系統，更包括在具有資料保全系統應用程式之行動裝置與含有使用者管理資料庫之伺服器之間的有線或無線連接通訊。

25. 如申請專利範圍第 18 項所述之系統，其中，該資料保全系統包含用於連接至主機電腦之外部通訊通道。

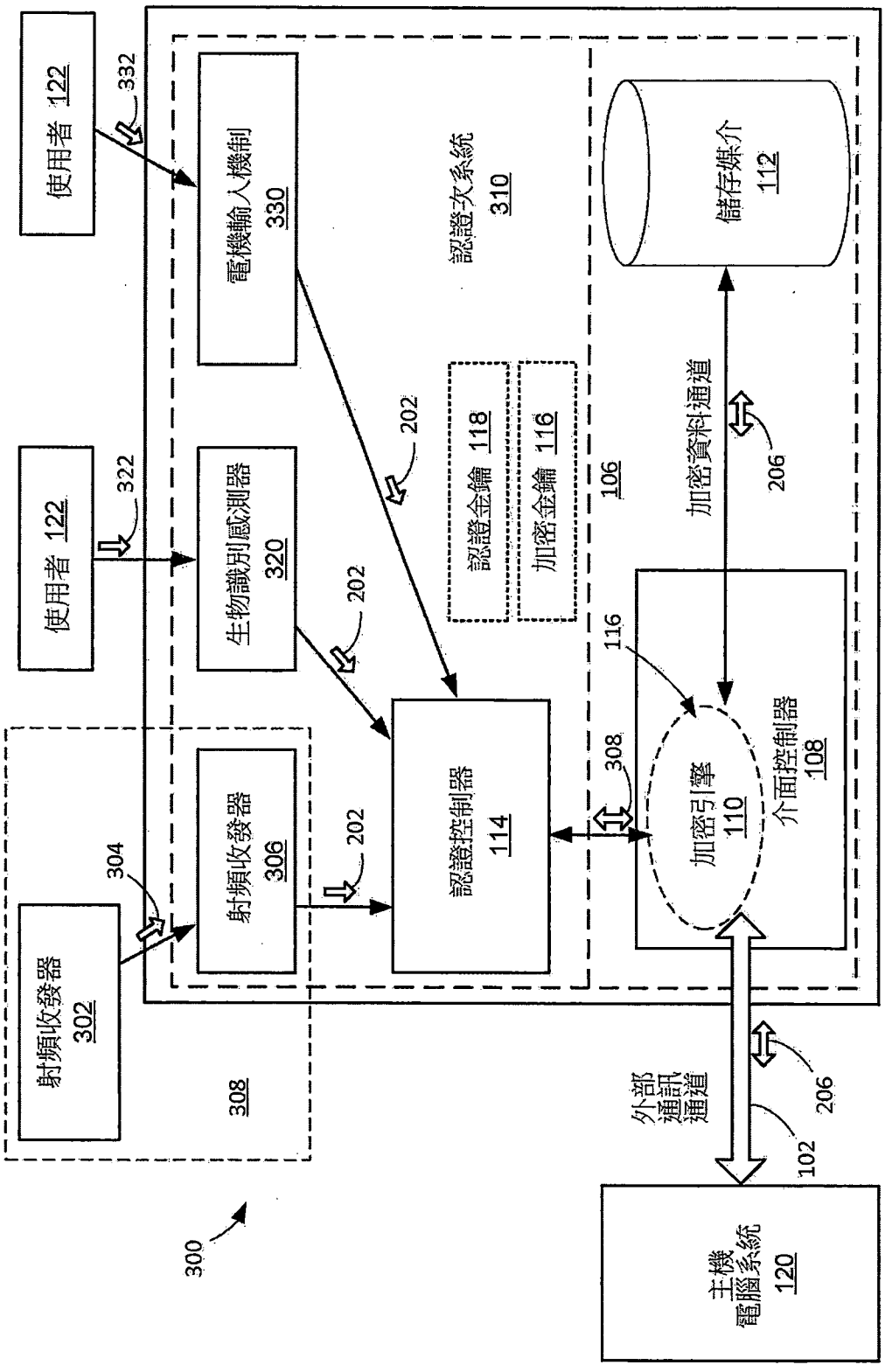
圖式


100
使用者
122
認證次系統 104
認證控制器
114
認證金鑰 118
加密金鑰 116
儲存次系統
106
儲存媒介
112
加密引擎
110
介面控制器
108
外部
通訊
通道
102
主機
電腦系統
120

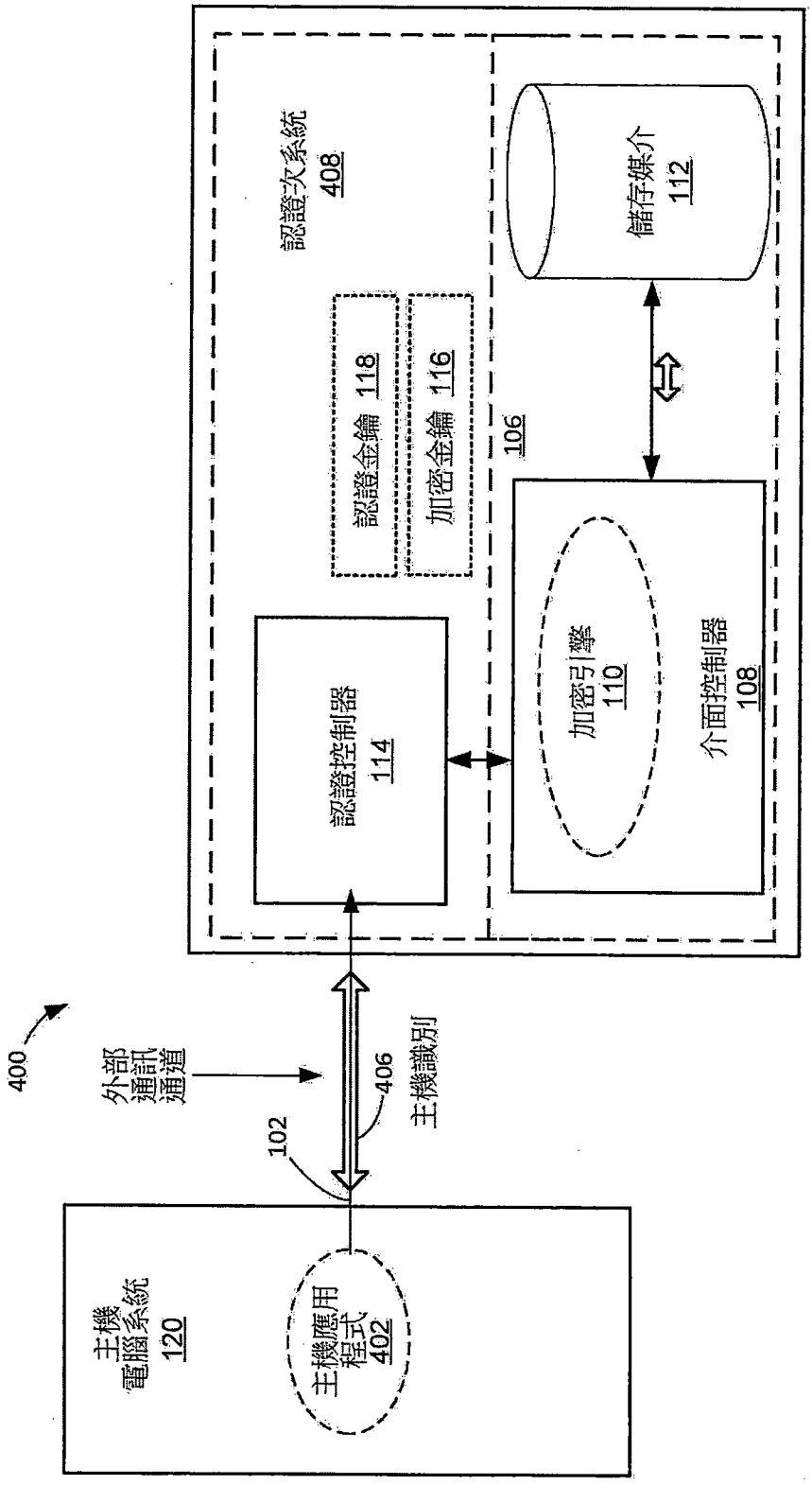
第1圖


100
使用者
122
202
認證次系統 104
認證控制器
114
認證金鑰 118
加密金鑰 116
116/118
儲存次系統
106
加密引擎
110
介面控制器
108
加密資料通道
206
儲存媒介
112
明確
資料
通道
206
102
主機
電腦系統
120

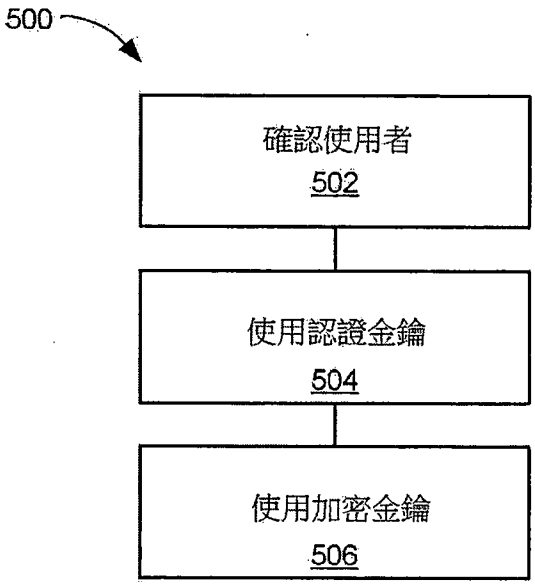
第2圖


使用者 122
332
電機輸入機制 330
認證次系統 310
儲存媒介 112
使用者 122
322
生物識別感測器 320
202
202
認證金鑰 118
加密金鑰 116
106
加密資料通道
206
116
射頻收發器 306
304
202
認證控制器 114
308
加密引擎 110
介面控制器 108
射頻收發器 302
308
外部通訊通道
206
102
主機電腦系統 120
300

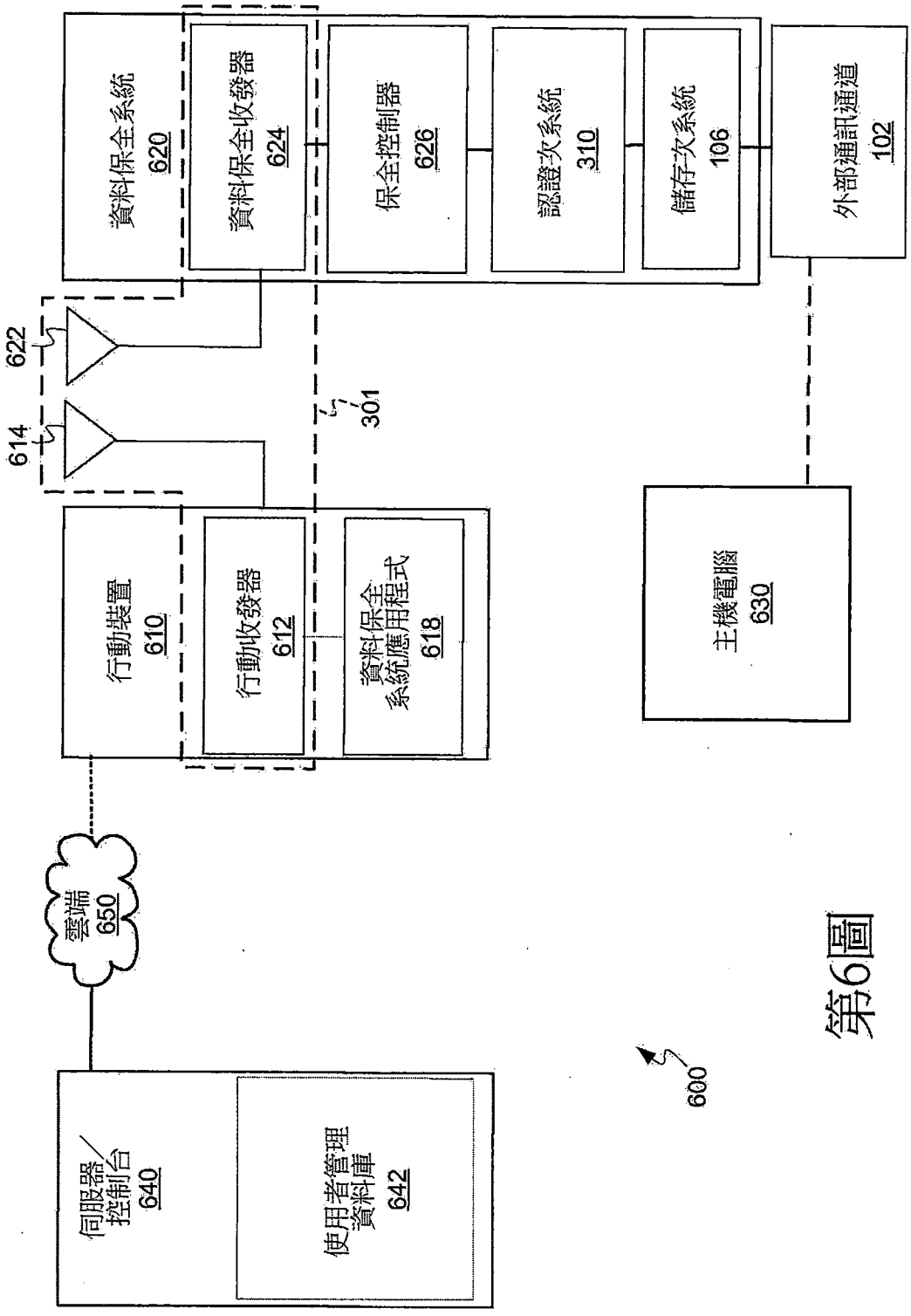
第3圖


400
外部通訊通道
406
主機識別
102
主機電腦系統 120
主機應用程式 402
認證次系統 408
認證控制器 114
106
加密引擎 110
介面控制器 108
認證金鑰 118
加密金鑰 116
儲存媒介 112

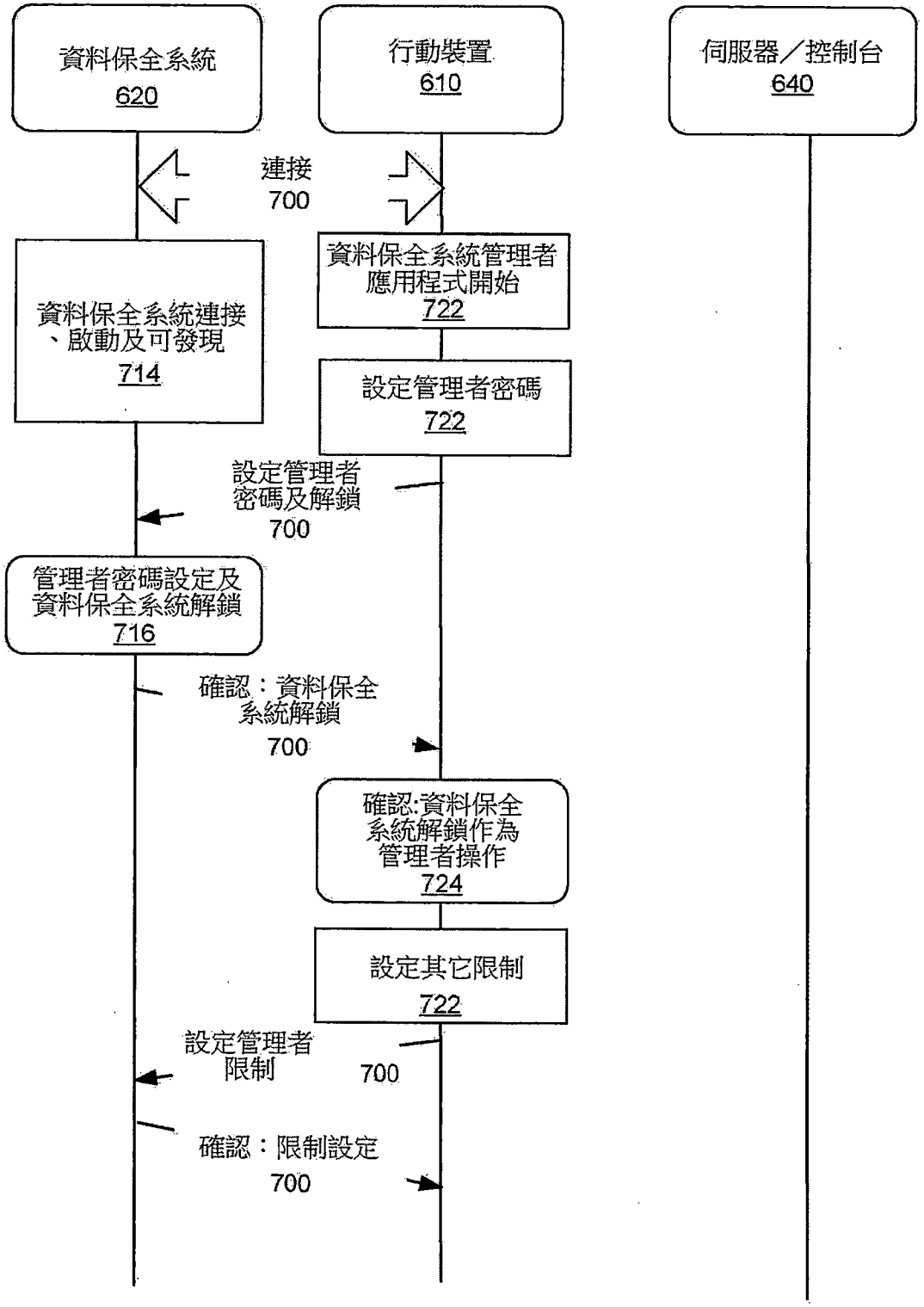
第4圖



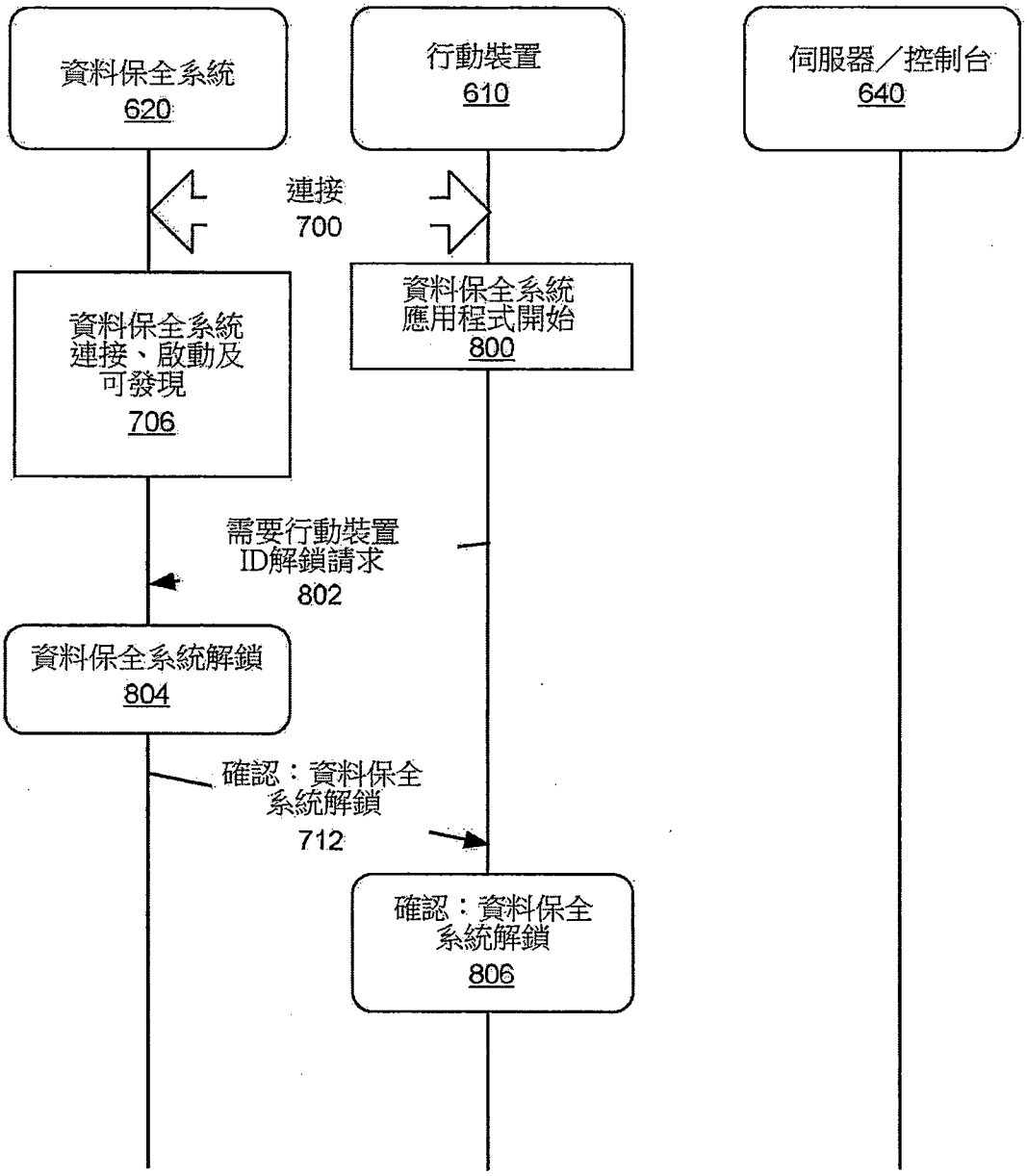
第5圖


資料保全系統
620
資料保全收發器
624
保全控制器
626
認證次系統
310
儲存次系統
106
外部通訊通道
102
622
614
301
行動裝置
610
行動收發器
612
資料保全
系統應用程式
618
主機電腦
630
雲端
650
伺服器/
控制台
640
使用者管理
資料庫
642
600

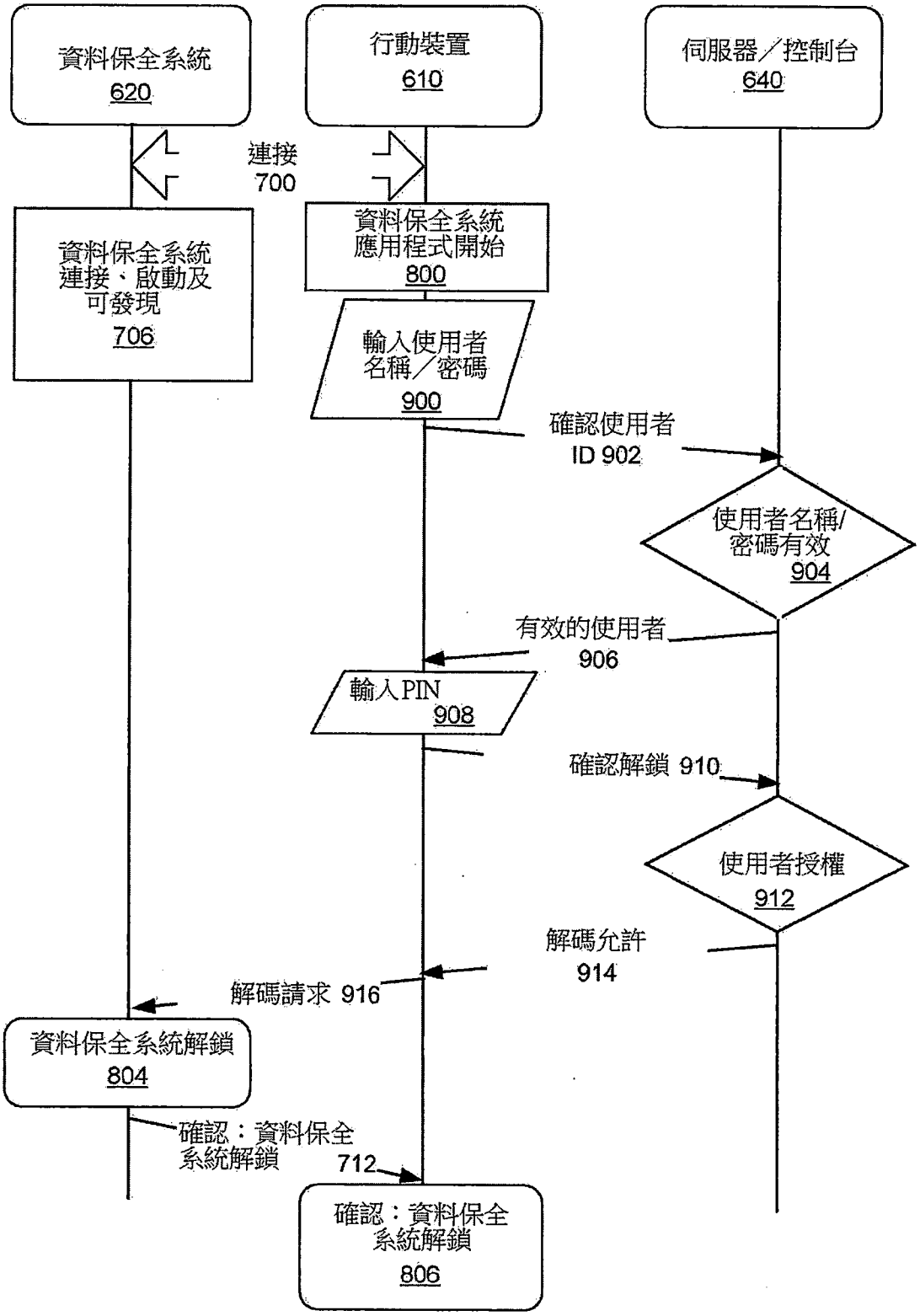
第6圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
資料保全系統連接、啟動及可發現
714
資料保全系統管理者應用程式開始
722
設定管理者密碼
722
設定管理者密碼及解鎖
700
管理者密碼設定及資料保全系統解鎖
716
確認：資料保全系統解鎖
700
確認:資料保全系統解鎖作為管理者操作
724
設定其它限制
722
設定管理者限制
700
確認：限制設定
700

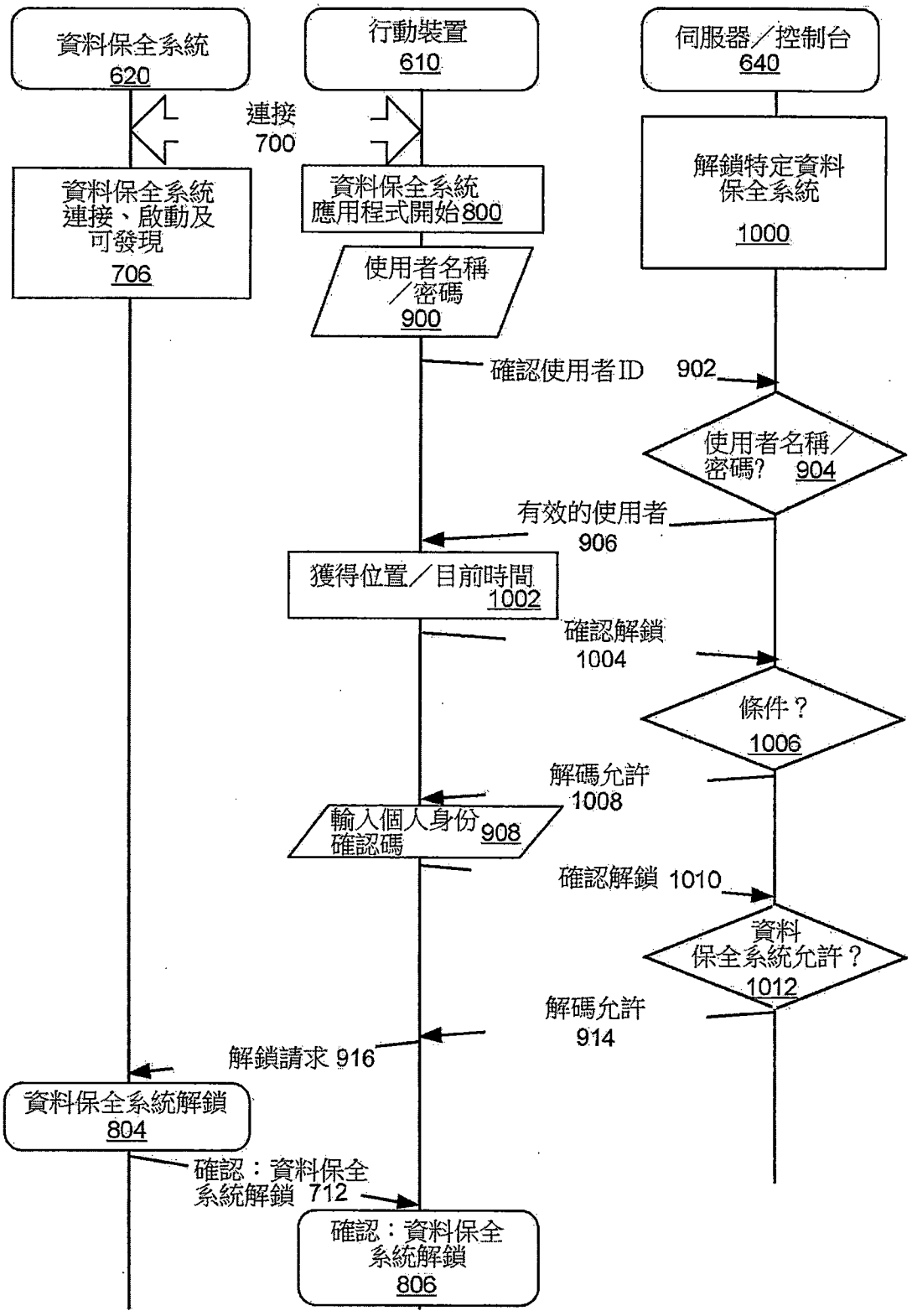
第7圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始
800
需要行動裝置
ID解鎖請求
802
資料保全系統解鎖
804
確認：資料保全
系統解鎖
712
確認：資料保全
系統解鎖
806

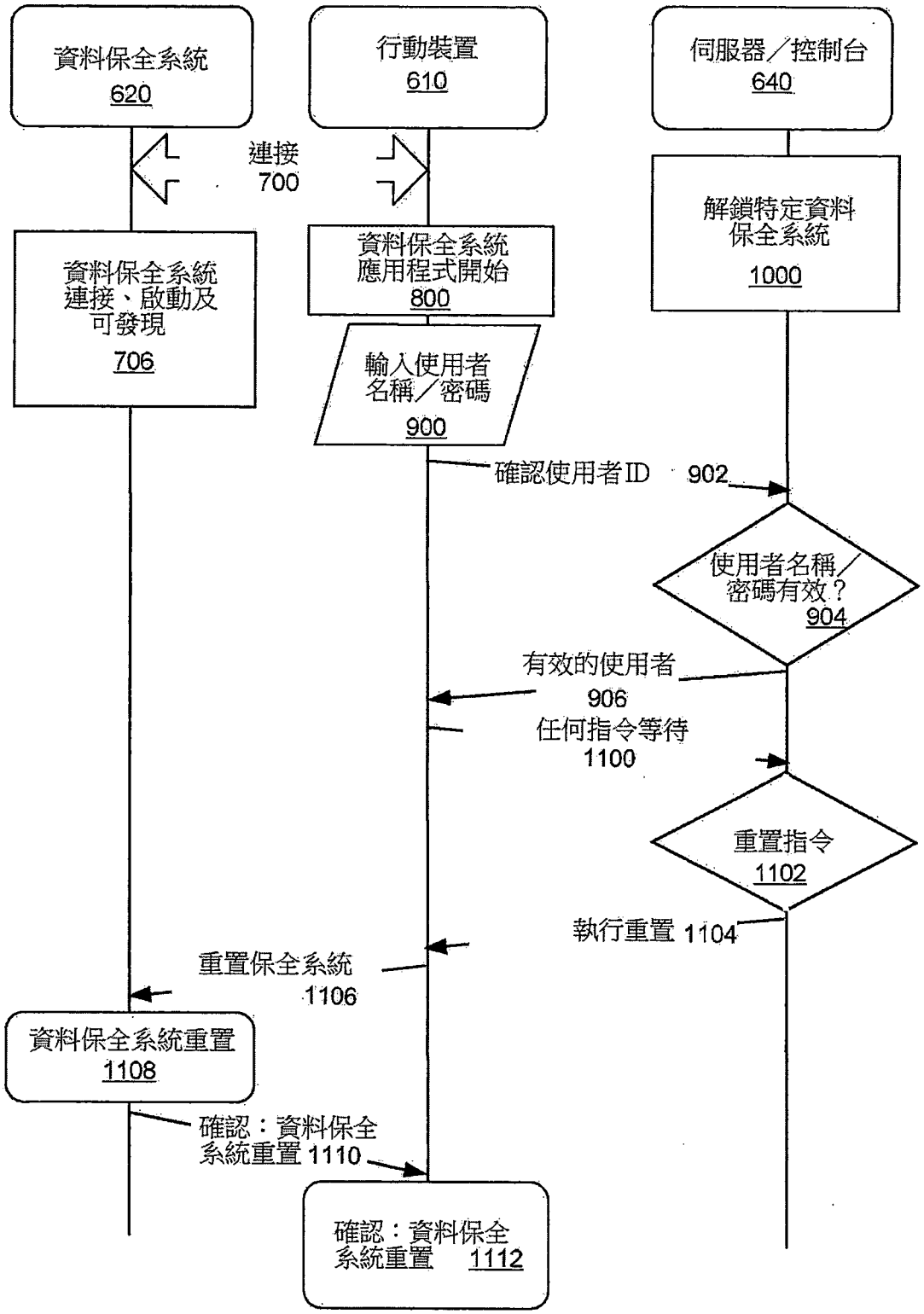
第8圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始
800
輸入使用者
名稱／密碼
900
確認使用者
ID 902
使用者名稱/
密碼有效
904
有效的使用者
906
輸入PIN
908
確認解鎖 910
使用者授權
912
解碼允許
914
解碼請求 916
資料保全系統解鎖
804
確認：資料保全
系統解鎖
712
確認：資料保全
系統解鎖
806

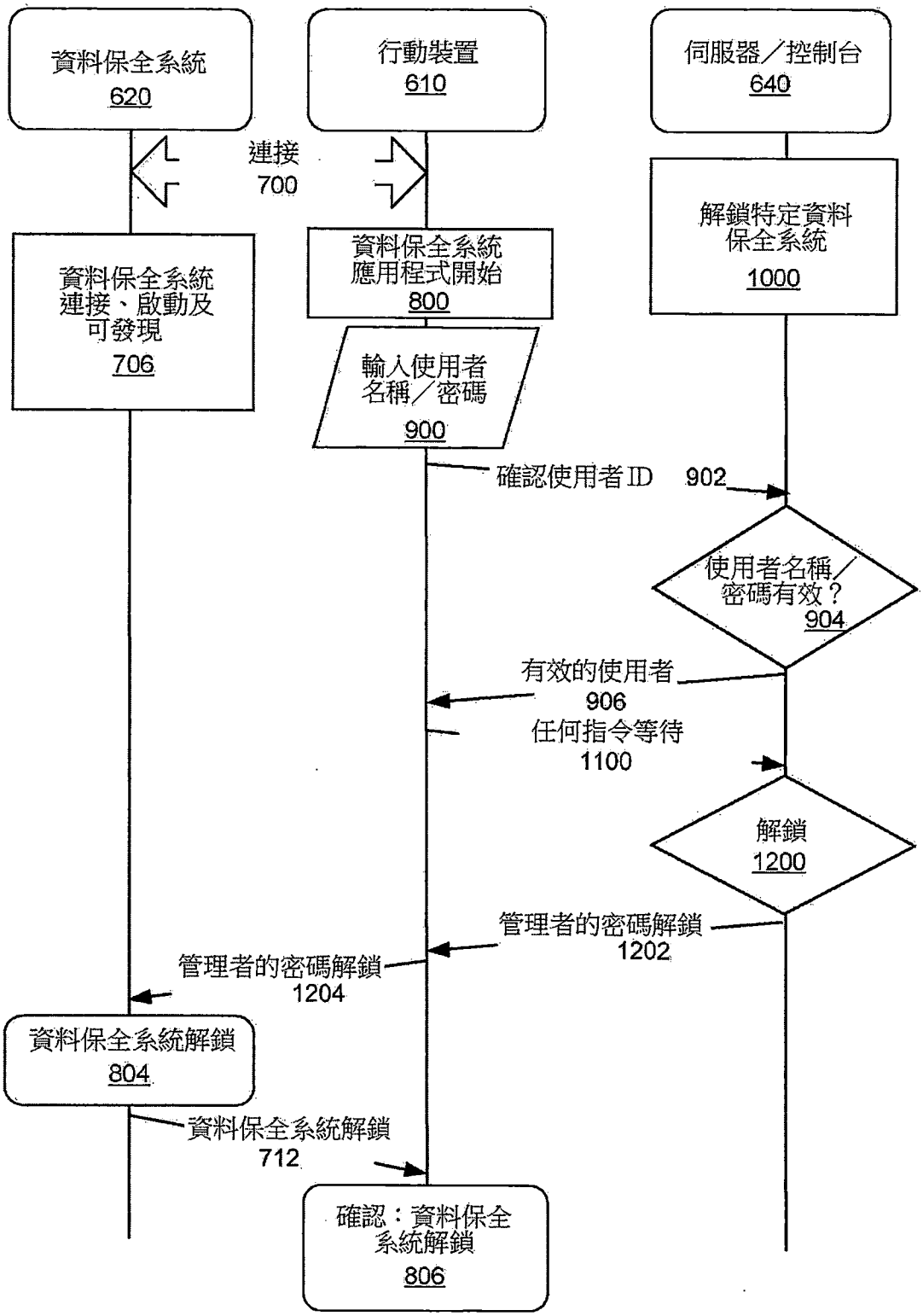
第9圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始800
解鎖特定資料
保全系統
1000
使用者名稱
／密碼
900
確認使用者ID 902
使用者名稱／
密碼? 904
有效的使用者
906
獲得位置／目前時間
1002
確認解鎖
1004
條件？
1006
解碼允許
1008
輸入個人身份
確認碼 908
確認解鎖 1010
資料
保全系統允許？
1012
解碼允許
914
解鎖請求 916
資料保全系統解鎖
804
確認：資料保全
系統解鎖 712
確認：資料保全
系統解鎖
806

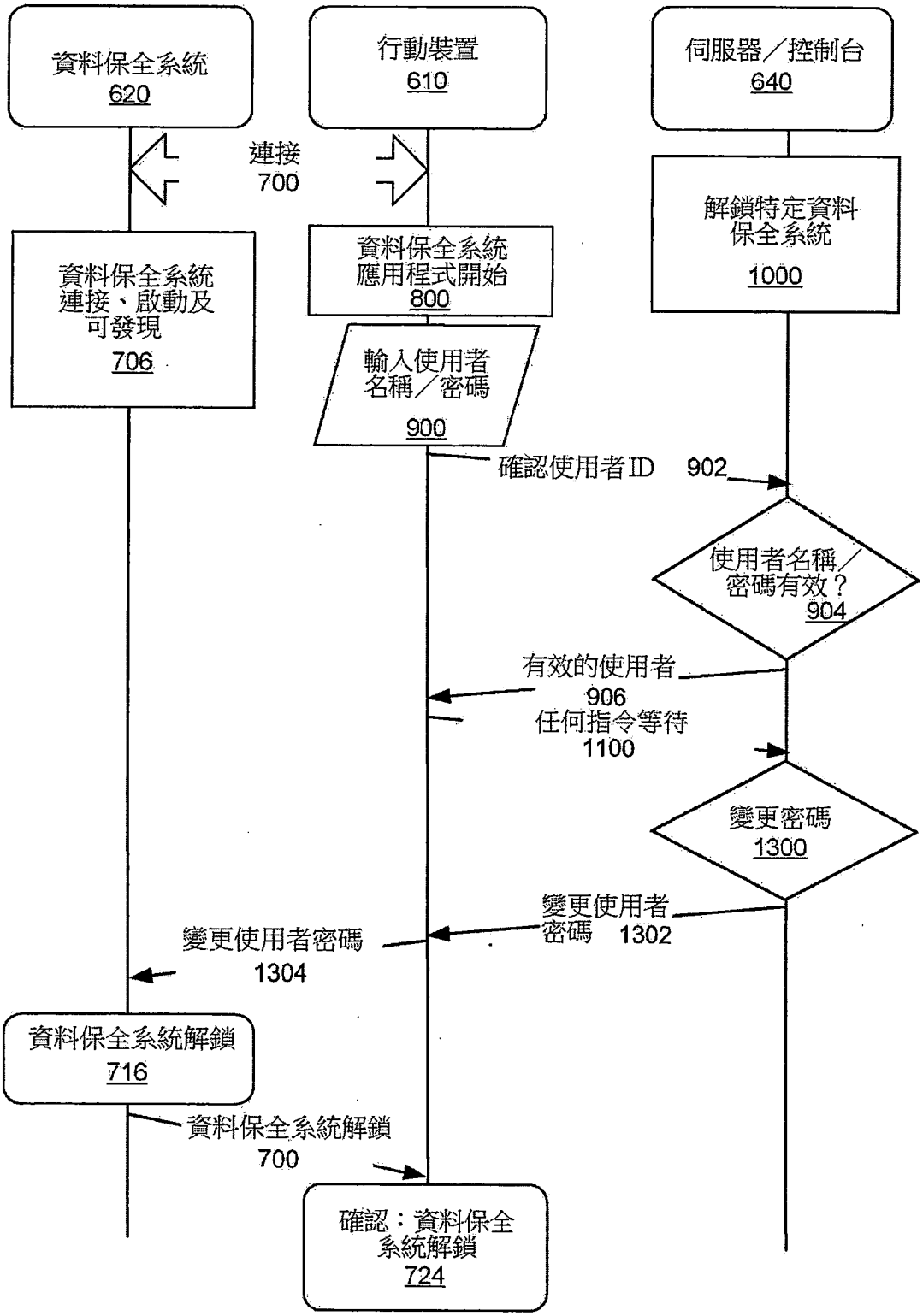
第10圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
解鎖特定資料
保全系統
1000
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始
800
輸入使用者
名稱／密碼
900
確認使用者ID 902
使用者名稱／
密碼有效？
904
有效的使用者
906
任何指令等待
1100
重置指令
1102
執行重置 1104
重置保全系統
1106
資料保全系統重置
1108
確認：資料保全
系統重置 1110
確認：資料保全
系統重置 1112

第11圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
解鎖特定資料
保全系統
1000
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始
800
輸入使用者
名稱／密碼
900
確認使用者ID 902
使用者名稱／
密碼有效？
904
有效的使用者
906
任何指令等待
1100
解鎖
1200
管理者的密碼解鎖
1202
管理者的密碼解鎖
1204
資料保全系統解鎖
804
資料保全系統解鎖
712
確認：資料保全
系統解鎖
806

第12圖


資料保全系統
620
行動裝置
610
伺服器／控制台
640
連接
700
解鎖特定資料
保全系統
1000
資料保全系統
連接、啟動及
可發現
706
資料保全系統
應用程式開始
800
輸入使用者
名稱／密碼
900
確認使用者ID 902
使用者名稱／
密碼有效？
904
有效的使用者
906
任何指令等待
1100
變更密碼
1300
變更使用者
密碼 1302
變更使用者密碼
1304
資料保全系統解鎖
716
資料保全系統解鎖
700
確認：資料保全
系統解鎖
724

第13圖