



(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 I851722 B

(45)公告日：中華民國 113 (2024) 年 08 月 11 日

(21)申請案號：109115302

(22)申請日：中華民國 109 (2020) 年 05 月 08 日

(51)Int. Cl. : A61M5/142 (2006.01)

G06F21/60 (2013.01)

G06F21/64 (2013.01)

(30)優先權：2019/05/08 美國

62/845,115

(71)申請人：美商 I C U 醫學公司 (美國) ICU MEDICAL, INC. (US)

美國

(72)發明人：維維克 S 史瑞 VIVEK, S. SREE (IN)；丹黛珂 瑞希凱西 安尼爾 DANDEKAR, HRISHIKESH ANIL (US)；斯瑞尼亞薩摩希 柴壇亞 馬特 SRINIVASAMURTHY, CHAITANYA MATTUR (US)

(74)代理人：陳長文

(56)參考文獻：

US 5681285A

US 6640145B2

US 2007/0213684A1

US 2016/0228633A1

WO 2008/052034A1

審查人員：許瑞峰

申請專利範圍項數：11 項 圖式數：6 共 44 頁

(54)名稱

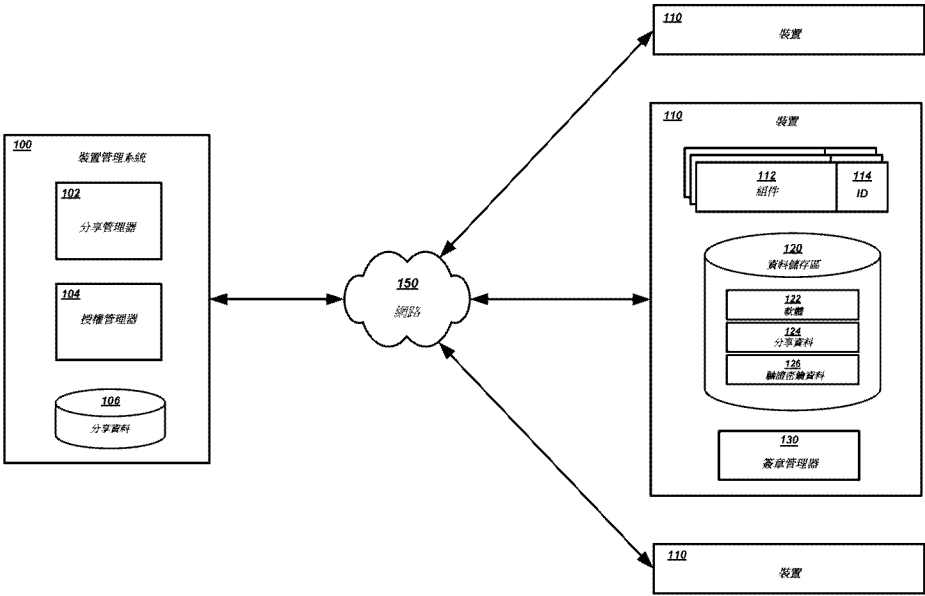
輸注泵、用於授權執行輸注系統命令之電腦實施之方法、及基於門檻簽章之醫療裝置管理之系統

(57)摘要

本發明針對於透過使用數位簽章門檻來管理裝置授權。一裝置之個別組件或一網路環境中之個別裝置與單獨秘密分享相關聯，自該等單獨秘密分享可導出一數位簽章。該數位簽章可用於授權執行一功能。使用門檻數目個此等秘密分享以便導出該數位簽章。因此，依賴於數位簽章驗證來判定對一功能授權之一授權處理程序將在授權時有門檻數目個秘密分享可用之情況下來進行。

The present disclosure is directed to managing device authorization through the use of digital signature thresholds. Individual components of a device, or individual devices in a network environment, are associated with separate secret shares from which a digital signature can be derived. The digital signature may be used to authorize performance of a function. A threshold number of such secret shares are used in order to derive the digital signature. Therefore, an authorization process that relies on digital signature verification to determine that a function is authorized will do so if a threshold number of secret shares are available at authorization time.

指定代表圖：



【圖1】

符號簡單說明：

- 100:裝置管理系統
- 102:分享管理器
- 104:授權管理器
- 106:資料儲存區
- 110:裝置
- 112:組件/處理器組件/記憶體組件/長期儲存組件/原始組件/初始組的組件
- 114:識別符
- 120:資料儲存區
- 122:作業系統
- 124:分享資料
- 126:驗證密鑰資料
- 130:簽章管理器
- 150:通信網路/網路

公告本

I851722

【發明摘要】**【中文發明名稱】**

輸注泵、用於授權執行輸注系統命令之電腦實施之方法、及基於門檻簽章之醫療裝置管理之系統

【英文發明名稱】

INFUSION PUMP, COMPUTER-IMPLEMENTED METHOD FOR AUTHORIZING EXECUTION OF INFUSION SYSTEM COMMANDS, AND SYSTEM FOR THRESHOLD SIGNATURE BASED MEDICAL DEVICE MANAGEMENT

【中文】

本發明針對於透過使用數位簽章門檻來管理裝置授權。一裝置之個別組件或一網路環境中之個別裝置與單獨秘密分享相關聯，自該等單獨秘密分享可導出一數位簽章。該數位簽章可用於授權執行一功能。使用門檻數目個此等秘密分享以便導出該數位簽章。因此，依賴於數位簽章驗證來判定對一功能授權之一授權處理程序將在授權時有門檻數目個秘密分享可用之情況下來進行。

【英文】

The present disclosure is directed to managing device authorization through the use of digital signature thresholds. Individual components of a device, or individual devices in a network environment, are associated with separate secret shares from which a digital signature can be derived. The digital signature may be used to authorize performance of a function. A threshold number of such secret shares are used in order to derive the digital signature. Therefore, an authorization process that relies on digital signature verification to determine that a function is authorized will do so if a threshold number of secret shares are

available at authorization time.

【指定代表圖】

圖1

【代表圖之符號簡單說明】

100: 裝置管理系統

102: 分享管理器

104: 授權管理器

106: 資料儲存區

110: 裝置

112: 組件/處理器組件/記憶體組件/長期儲存組件/原始組件/初始組的組件

114: 識別符

120: 資料儲存區

122: 作業系統

124: 分享資料

126: 驗證密鑰資料

130: 簽章管理器

150: 通信網路/網路

【發明說明書】

【中文發明名稱】

輸注泵、用於授權執行輸注系統命令之電腦實施之方法、及基於門檻簽章之醫療裝置管理之系統

【英文發明名稱】

INFUSION PUMP, COMPUTER-IMPLEMENTED METHOD FOR AUTHORIZING EXECUTION OF INFUSION SYSTEM COMMANDS, AND SYSTEM FOR THRESHOLD SIGNATURE BASED MEDICAL DEVICE MANAGEMENT

【技術領域】

【0001】 本發明係關於醫療裝置管理領域，且特定而言係關於用於醫療裝置之安全授權之系統及方法。

【先前技術】

【0002】 計算系統(諸如具有處理器及其他計算組件之醫療裝置)執行控制由計算系統執行之功能之軟體。軟體通常儲存於一永久資料儲存區(例如，硬碟、快閃記憶體等)中且載入至揮發性記憶體(例如，隨機存取記憶體或RAM)中以供執行。計算系統通常在執行之前驗證軟體是否被授權。舉例而言，計算系統可判定是否已獲得授權執行軟體之一特許。若已獲得一有效特許，則可准許執行軟體。若尚未獲得特許，則可阻止軟體之執行。

【發明內容】

【0003】 本文中闡述用於使用基於門檻簽章之授權管理裝置之操作之各種技術。此等技術可包含形成數位簽章產生密鑰之若干分享，及將該等分享指派給裝置或裝置之個別組件。然後，可使用該等分享來授權執行特定功能，只要在授權程序期間門檻數目個分享或門檻量的經加權分享可用即可。舉例而言，可使用基於門檻簽章之授權來確證有效特許、確證某

些組件之存在、對安全事件作出回應、確保裝置在既定環境中使用等。下文參考圖1至圖6更詳細地闡述此等及其他實施例。儘管在醫療裝置、功能及環境(包含輸注泵、藥物施配功能及醫院或臨床環境)之內容脈絡中闡述諸多實例，但本文中所闡述之技術可適用於其他類型之裝置、功能及環境。

【圖式簡單說明】

【0004】 遍及圖式，可重複使用參考編號來指示所參考元件之間的對應性。圖式經提供以圖解說明本文中所闡述之實例實施例且不意欲限制本發明之範疇。

【0005】 圖1係根據某些實施例包含一裝置管理系統及各種裝置之一實例網路環境之一方塊圖。

【0006】 圖2係圖解說明根據某些實施例在預授權設置期間之資料流及一裝置與一裝置管理系統之間的互動之一方塊圖。

【0007】 圖3係根據某些實施例用於一裝置之門檻簽章授權之一說明性處理程序之一流程圖。

【0008】 圖4係圖解說明根據某些實施例在經加權授權期間之資料流及由一裝置執行之處理之一方塊圖。

【0009】 圖5係圖解說明根據某些實施例在基於群組之授權期間之資料流及所執行處理之一方塊圖。

【0010】 圖6係圖解說明根據某些實施例在動態經加權授權期間之資料流及由一裝置執行之處理之一方塊圖。

【實施方式】

相關申請案之交叉參考

【0011】本申請案主張在2019年5月8日提出申請且標題為「Threshold Signature Based Medical Device Management」之美國臨時專利申請案第62/845,115號之優先權，該臨時專利申請案以引用方式併入本文中。

【0012】本發明針對於透過使用數位簽章門檻來管理裝置授權。一裝置之個別組件或一網路環境中之個別裝置與可自其產生一數位簽章之資料之單獨分享相關聯。舉例而言，可使用資料之分享來產生一數位簽章之分享，且可使用該數位簽章來授權執行一功能。資料之分享可稱為「秘密分享」或為了方便簡稱為「分享」。在一說明性實施例中，需要門檻數目個秘密分享以便執行任何私密操作，諸如產生一數位簽章、恢復秘密資料等。因此，依賴於數位簽章驗證來判定對一功能授權之一授權處理程序將僅在授權時有門檻數目個秘密分享可用之情況下如此做。若少於門檻數目個秘密分享可用，則阻止所請求功能(或裝置作為一整體之操作)。以此方式，一裝置可需要維持門檻數目個原始或經授權組件來繼續使用經特許軟體或繼續全部執行。以一類似方式，可禁止一裝置操作，除非門檻數目個經連接裝置參與一授權程序或裝置之門檻數目個組件參與一授權程序。

【0013】本發明之某些態樣係關於產生一醫療裝置(例如，一輸注泵)之個別組件之秘密分享及使用該等秘密分享來判定是否對該醫療裝置之一功能授權。在某些實施例中，軟體可安裝於一醫療裝置上，且可需要一有效特許以便執行該軟體。在安裝或初始特許期間，特許可與醫療裝置之當前組態相聯繫，使得僅在醫療裝置之至少門檻數目個組件保持不變之情況下准許執行軟體。為了實施此特許要求，可將一不同秘密分享指派給裝置之各種個別組件。舉例而言，可存在此所產生資料之 n 個秘密分享，

針對裝置之 n 個不同組件中之每一者有一個秘密分享。在將執行軟體時，可執行一授權程序。一說明性授權程序可涉及：(1)使用同一訊息及與仍存在之裝置組件相關聯之秘密分享中之每一者產生一數位簽章之一不同部分或「簽章分享」；(2)使用簽章分享產生一數位簽章；及(3)驗證數位簽章之真實性(例如，驗證數位簽章係使用門檻數目個秘密分享及該訊息產生的)。然而，可僅在授權時有至少門檻數目 t 個秘密分享可用時產生一有效數位簽章，其中 $0 < t < n$ 。若太多組件已被改變或移除，則可獲得少於 t 個秘密分享，無法產生一有效數位簽章，且對數位簽章之驗證將失敗。以此方式，若軟體已被複製至一不同裝置上或若已發生某一其他事件(例如，軟體可不再與醫療裝置在處於該裝置之當前組態時相容)，則可阻止一醫療裝置執行軟體(或以其他方式執行一現在未授權功能)。

【0014】本發明之額外態樣係關於在一授權處理程序期間以不同於其他裝置組件之方式處理某些裝置組件。以不同方式處理組件之機制可係使用指派給組件之加權因子。加權因子亦可出於方便簡稱為「權重」。在某些實施例中，可判定一特定組件或組件之子集比其他組件更重要。可給較重要組件指派比不那麼重要之組件高之一權重。當隨後執行一授權處理程序時，可獲得與醫療裝置當前可用之裝置組件相關聯之各種秘密分享及權重。在自權重及秘密分享產生一數位簽章時，可需要門檻量的經加權秘密分享以便產生一有效數位簽章。舉例而言，若相對重要組件不存在但所有其他組件存在，則授權程序將失敗。然而，若一相比而言不那麼重要之組件不存在但所有其他組件存在，則授權程序可成功地完成。以此方式，可在以下情況下阻止一醫療裝置操作：存在關鍵組件之太多替代，關鍵替代組件並非係正確類型，存在太少關鍵組件之原始或經授權版本等。此類

限制可改良安全性及可靠性。在某些實施例中，可給不同組件指派不同數目個分享而非具有不同值之權重，以指示組件之相對重要性。

【0015】 本發明之其他態樣係關於一網路環境中之個別醫療裝置之基於群組之授權。基於群組之授權亦可稱為「群集鑑認」。在某些實施例中，可禁止嘗試執行一特定功能(例如，連接至一網路伺服器或施配藥物)之一醫療裝置如此做，除非門檻數目個其他醫療裝置能夠參與授權。此可阻止可能已丟失或被偷竊之一醫療裝置之惡意或在其他方面不合意之使用，乃因醫療裝置可能不在其中門檻數目個其他裝置可用於參與授權程序之一網路環境(例如，一醫院或診所)中操作。舉例而言，可給每一醫療裝置提供或以其他方式指派一秘密分享。當一特定裝置嘗試執行需要授權之一功能時，一網路伺服器可判定哪些其他裝置連接至網路伺服器且獲得或以其他方式存取可用裝置中之每一者之秘密分享。若門檻數目個秘密分享可用，則可成功地產生一有效數位簽章，可成功地驗證該數位簽章，且然後可授權裝置執行該功能。否則，可阻止裝置執行該功能。因此，可阻止已丟失或被偷竊之一醫療裝置操作，乃因其可能不能夠連接至正確臨床網路且基於群組之授權處理程序可能不能夠獲得門檻數目個秘密分享。

【0016】 本發明之又一些態樣係關於安全授權中之系統範圍參與。一多組件系統(諸如一醫療裝置)可實施動態加權之基於門檻之授權來授權執行特定功能(或裝置全部之操作)。舉例而言，可給系統之個別組件指派一開始權重或一定數目個秘密分享。當一個別組件偵測到安全事件(例如，無效登入嘗試、系統安全更動嘗試等)時，該組件可動態地降低其貢獻給系統範圍授權之權重。其他組件可以一類似方式執行。當系統嘗試授權執行一特定功能時，可需要門檻數目個經加權秘密分享以便產生一有效

數位簽章且成功地對該功能授權。若門檻量的經加權秘密分享歸因於動態降低之權重而不可用，則授權處理程序將失敗。以此方式，一系統之個別組件可主動地參與由系統作出之授權判定，即使某些組件不以其他方式執行安全功能。

【0017】 儘管本發明中所闡述之某些實施例之態樣將出於圖解說明之目的而集中於裝置、密碼秘密、基於門檻之授權演算法及諸如此類之特定實例，但該等實例僅係說明性的且不意欲係限制性的。在某些實施例中，本文中所闡述之系統及方法可應用於額外或替代裝置、密碼秘密、基於門檻之授權演算法等。現在將關於意欲圖解說明而非限制本發明之某些實例及實施例闡述本發明之各項態樣。

實例網路環境之概述

【0018】 圖1圖解說明其中一裝置管理系統100經由一通信網路150與一或多個裝置110通信之網路環境。以圖解說明方式，該環境可包含一或多個醫療保健機構(例如，醫院)，其中裝置110係醫療裝置且裝置管理系統100係一本機託管系統或基於雲端之系統(或其部分)以管理醫療裝置之使用。

【0019】 在某些實施例中，一通信網路150 (亦簡稱為一「網路」)可係可能由各種不同方操作之經連結網路之一可公開存取網路，諸如網際網路。在某些情形中，網路150可係或包含一私人網路、個人區域網路、區域網路、廣域網路、全域網路、纜線網路、衛星網路、蜂巢式資料網路等或者其一組合，其中之某些或全部可以或可以不具有向及/或來自網際網路之存取。

【0020】 裝置管理系統100可係一或多個計算裝置之一邏輯關聯以

用於管理分享之產生及分發、授權程序之執行及諸如此類。舉例而言，裝置管理系統100可包含一或多個分享管理器102。一分享管理器102可對應於用於產生秘密分享且將秘密分享分發至使用其之各種裝置110之一或多個伺服器計算裝置。在某些實施例中，秘密分享亦可或另一選擇係儲存於對應於一或多個資料儲存裝置之一資料儲存區106中。裝置管理系統100亦可包含一或多個授權管理器104。一授權管理器104可對應於經組態以使用由分享管理器102產生之秘密分享來執行授權程序之一或多個計算裝置。

【0021】 在某些實施例中，由裝置管理系統100提供之特徵及服務可作為可經由一或多個通信網路消費之web服務來實施。在其他實施例中，裝置管理系統100及/或其個別組件可由在一託管計算環境中實施之一或多個虛擬機提供。託管計算環境可包含一或多個迅速佈建及發佈之計算資源，諸如計算裝置、網路連線裝置及/或儲存裝置。一託管計算環境亦可稱為一「雲端」計算環境。

【0022】 裝置110可對應於利用或經受基於門檻之授權之各種裝置中之任一者。個別裝置110可包含各種組件112，諸如處理器、網路介面卡、揮發性記憶體、長期儲存裝置、顯示器及諸如此類。組件112中之某些或全部可與對應識別符114相關聯。舉例而言，一處理器組件112可具有充當對應識別符114之一唯一序號。一記憶體組件112可與充當對應識別符114之一不同唯一序號相關聯。一長期儲存組件112（諸如一磁碟機）可與其自己的充當對應識別符114之唯一序號相關聯。在某些實施例中，具有一對應識別符之一組件可係一軟體組件。舉例而言，一作業系統122可儲存於一資料儲存區120（諸如一硬碟機）中。如同其他組件112，作業

系統122可與其自己的唯一識別符相關聯，且可因此被視為類似於其他組件112 (例如，經指派分享、權重等)。如同其他組件112，資料儲存區120可與其自己的唯一識別符相關聯。

【0023】 裝置110亦可包含用於執行秘密分享處理及/或授權處理程序之組件。在某些實施例中，一裝置110可包含一簽章管理器130。簽章管理器130可係一基於硬體之組件，或在裝置110之一處理器上運行之一基於軟體之應用程式或子系統。簽章管理器130可執行特定秘密分享處理及授權處理程序，如下文更詳細地闡述。舉例而言，簽章管理器130可從資料儲存區120存取分享資料124及一驗證密鑰資料126以供在秘密分享處理及授權處理程序中使用。在某些實施例中，分享資料124及/或驗證密鑰資料126可儲存於簽章管理器130中或與資料儲存區120分開的某一其他安全位置中。

【0024】 在某些實施例中，裝置110可係或包含具有各種組件112之醫療裝置，諸如輸注泵。舉例而言，一輸注泵可包含經組態以控制施配藥物之馬達之一馬達控制器單元(「MCU」)、經組態以管理去往/來自泵之通信之一通信引擎(「CE」)、操作軟體及各種其他輸注泵特有或醫療裝置特有組件，其中的任一者或全部可與各別識別符114相關聯。另外，裝置110自身可包含不同類型之特定裝置，諸如不同類型之輸注泵。每一類型之輸注泵及甚至同一類型之輸注泵之不同版本可與一不同作業系統一起操作，使用一不同類型之MCU及/或CE等。

秘密分享產生及分發處理程序

【0025】 圖2係在預授權設置期間之說明性資料流及一裝置110與一裝置管理系統100之間的互動之一方塊圖。所顯示互動可在軟體(或某一其

他組件)之安裝或初始特許期間發生。舉例而言，軟體可安裝於裝置110上。為了驗證軟體被特許在裝置110上使用，軟體可執行(或致使執行)一授權處理程序，該授權處理程序僅在存在於裝置110上之門檻數目個組件112a...112n在軟體安裝期間仍存在於該裝置上之情況下授權執行軟體。為了促成此授權處理程序，可獲得用於數位簽章產生之一組秘密分享，將其指派給組件112a...112n，且將其儲存於裝置110上。在某些實施例中，秘密分享可各自係供與一密碼函數一起使用之一私密加密密鑰或其他密鑰。

【0026】在[A]處，裝置110可判定裝置110之一組 n 個組件之識別符。 n 之值可取決於所安裝之軟體、存在於裝置110中之組件112之數目、軟體之要求等。舉例而言， n 可係4，且該組 n 個組件可包含一處理器、記憶體、網路介面及電池。該等組件中之每一者可具有其已與之關聯的一識別符(例如，一序號)。在某些實施例中，可作為預授權設置之部分給組件指派識別符。該等識別符可係全域唯一識別符或至少針對其被指派給的組件類型係唯一的識別符(例如，與諸如型號等其他資料組合地提供各別組件之實質上唯一標識之識別符)。

【0027】在[B]處，裝置110可將識別符發送至裝置管理系統100。舉例而言，裝置110可將識別符序列地、異步地或在一批次中傳輸至裝置管理系統100。

【0028】在[C]處，分享管理器102或裝置管理系統100之某一其他模組或組件產生秘密分享，諸如個別數位簽章分享產生密鑰。可針對已接收之 n 個組件識別符中之每一者產生一不同秘密分享。可產生秘密分享使得至少門檻數目 t (其中 $n \geq t > 0$)個秘密分享必須可用，以便產生一數位

簽章且繼續一授權處理程序。分享管理器102亦可產生一驗證密鑰，該驗證密鑰用於在授權處理程序期間驗證使用已經使用秘密分享產生之簽章分享產生之一數位簽章。

【0029】在某些實施例中，可使用拉格朗日內插(Lagrange interpolation)及沙米爾(Shamir)的秘密分享判定依據其產生秘密分享之一隨機多項式函數來產生秘密分享。不同秘密分享可對應於針對不同輸入值(例如， x_1 、 x_2 、 $\dots$ 、 x_n)的多項式函數之值。數位簽章產生密鑰可對應於針對一特定預定輸入值(例如， $x = 0$)的多項式函數之一值。在授權時，若至少 t 個秘密分享可用(對應於針對 t 個不同輸入值的多項式函數之至少 t 個不同值)，則多項式函數自身可自秘密分享導出而不需要多項式函數之任何其他先前知識。然後，可針對用於判定數位簽章產生密鑰之預定輸入值評估多項式函數。若數位簽章產生密鑰係正確的，則將使用由分享管理器102產生之驗證密鑰來驗證使用該數位簽章產生密鑰產生之一數位簽章。若至少 t 個不同秘密分享不可用，則要判定多項式函數或以其他方式導出正確數位簽章產生密鑰可係不可能的或計算上不可行的。舉例而言，若有 $t-1$ 個分享可用，則可存在可自該等分享導出之無限數目個可能多項式函數。

【0030】本文中所闡述之秘密分享之實例產生僅係說明性的，且不意欲係窮盡性或限制性的。在某些實施例中，可使用用於產生秘密分享之其他方法，諸如可驗證秘密分享、布萊克利(Blakely)之秘密分享及諸如此類。在Amos Beimel之「Secret-Sharing Schemes: A Survey」及Adi Shamir之「How to Share a Secret」中闡述實例秘密分享方案，該兩個文獻之內容以引用方式併入本文中且構成本說明書之部分。

【0031】 在[D]處，分享管理器102或裝置管理系統100之某一其他模組或組件可將表示秘密分享之分享資料及表示驗證密鑰之驗證密鑰資料發送至裝置110。舉例而言，分享管理器102可將分享資料及驗證密鑰資料序列地、異步地或在一批次中傳輸至裝置110。

【0032】 在[E]處，裝置110可儲存分享資料及驗證密鑰資料。舉例而言，可將表示與對應識別符114a...114n相關聯之秘密分享之分享資料124a...124n及表示驗證密鑰之驗證密鑰資料126儲存於資料儲存區120中。在某些實施例中，簽章管理器130可以一安全方式儲存分享資料124及驗證密鑰資料126。舉例而言，可儲存分享資料124使得其不可在簽章管理器130外部存取，或使得個別分享僅可藉由使用一有效識別符查詢簽章管理器130而存取。

【0033】 一旦已產生且儲存秘密分享及驗證密鑰，裝置110可準備好執行一授權處理程序以授權執行一特定功能(諸如執行經特許軟體)。

基於門檻之授權處理程序

【0034】 圖3係可由一簽章管理器130或某一其他組件執行以判定是否對一特定功能授權之一說明性處理程序300之一流程圖。有利地，若能夠獲得門檻數目 t 個秘密分享，則處理程序300可對該功能授權，該門檻數目 t 對應於在執行預授權設置處理程序時係裝置110之部分之組件之一門檻數目 t 。否則，若不能獲得門檻數目 t 個秘密分享，則處理程序300無法對該功能授權。以此方式，授權處理程序可確保一經授權功能與組件之一門檻數目相聯繫，且若軟體安裝於一不同裝置110上、若太多原始組件112已被替代或移除等，則將不對功能(例如，軟體之執行)授權。

【0035】 圖3中所展示之處理程序300在方塊302處開始。處理程序

300可回應於一事件(諸如在一軟體應用程式開始執行時)或將要執行某一其他操作而開始。當起始處理程序300時，可將儲存於一或多個非暫時性電腦可讀媒體(例如，硬碟機、快閃記憶體、可抽換式媒體等)上之一組可執程式指令載入至裝置110之記憶體(例如，隨機存取記憶體或「RAM」)中。然後，可由計算裝置之一基於硬體之電腦處理器(例如，一中央處理單元或「CPU」)執行該等可執行指令。在某些實施例中，處理程序300或其部分可在多個處理器上序列地或並列地實施。

【0036】在方塊304處，簽章管理器130或裝置110之某一其他模組或組件可獲得存在於裝置110中之組件112之識別符。在某些實施例中，簽章管理器130可獲得裝置110之所有組件112或僅某些組件112(例如， n 個最重要組件或為了功能被授權而指定之組件)之識別符114。

【0037】在方塊306處，簽章管理器130或裝置110之某一其他模組或組件可獲得在方塊304處獲得之識別符之秘密分享。在某些實施例中，簽章管理器130可查詢資料儲存區120以得到表示對應於所獲得識別符114之秘密分享之分享資料124。資料儲存區120中之秘密分享可多於識別符(例如，在一組件112被移除但未被替代之情況下)，識別符可多於資料儲存區120中之秘密分享(例如，在添加一組件112而不移除另一組件之情況下)，或秘密分享之數目可與組件相同(例如，分別地，在未移除相同數目個組件之情況下根本未添加組件，或在未添加相同數目個組件之情況下未移除任何組件)。

【0038】在方塊308處，簽章管理器130或裝置110之某一其他模組或組件可使用上文在方塊306處擷取之秘密分享產生數位簽章分享，亦簡單地稱為「簽章分享」。在某些實施例中，簽章管理器130可使用每一秘

密分享及同一資料項目產生一單獨簽章分享。舉例而言，一預定義加密函數可使用一秘密分享來將一資料項目(諸如一訊息或某一其他符記)加密。該符記可係一隨機產生值、提供至授權處理程序之一符記或將充當待被數位簽章之未加密訊息之某一其他輸入。可將符記直接加密，或可首先處理符記(例如，可使用一雜湊演算法產生一雜湊)。加密函數之輸出可係輸入值(或經雜湊輸入值)之一經加密版本。以圖解說明方式，簽章管理器130可使用一第一秘密分享來將一符記加密且產生一第一簽章分享。簽章管理器130亦可使用一第二秘密分享來將同一符記加密且產生一第二簽章分享。可針對每一可用秘密分享重複此處理程序以產生一組簽章分享，自該組簽章分享將產生一數位簽章，如下文所闡述。

【0039】 在方塊310處，簽章管理器130或裝置110之某一其他模組或組件可獲得表示驗證密鑰之驗證密鑰資料126，該驗證密鑰將用於驗證使用利用秘密分享產生之簽章分享而產生之一數位簽章。

【0040】 在方塊312處，簽章管理器130或裝置110之某一其他模組或組件可使用上文在方塊308處產生之簽章分享來產生一數位簽章。在某些實施例中，可組合簽章分享以產生數位簽章。舉例而言，可端視所使用之數位簽章門檻方案而將簽章分享共同相乘或相加以獲得一數位簽章。如一般闡述，簽章分享可充當至使用簽章分享產生一數位簽章之一函數之輸入。該函數之輸出可係自其產生簽章分享之符記之一經加密版本。

【0041】 在方塊314處，簽章管理器130或裝置110之某一其他模組或組件可使用驗證密鑰驗證數位簽章。在某些實施例中，簽章管理器130可使用一預定義解密函數及驗證密鑰作為解密密鑰來將上文在方塊312處產生之訊息解密。若經解密訊息匹配原始資料項目(或原始資料項目之雜

湊)，則判定正確數位簽章。否則，若經解密訊息不匹配原始資料項目(或其雜湊)，則判定一不正確數位簽章。

【0042】在決策方塊316處，簽章管理器130或裝置110之某一其他模組或組件可判定上文在方塊314處是否驗證了數位簽章。若如此，則處理程序可進行至方塊318，在方塊318處對功能授權。舉例而言，可准許執行將要執行之軟體。若簽章管理器130判定上文在方塊314處未驗證數位簽章，則處理程序可進行至方塊320，在方塊320處不對功能授權。舉例而言，可不准許執行將要執行之軟體。

【0043】在方塊322處，處理程序300可終止。

使用經加權秘密分享之基於門檻之授權

【0044】圖4係在使用經加權秘密分享之基於門檻之授權期間之說明性資料流及一裝置110之操作之一方塊圖。所顯示互動可在一功能之授權或裝置110自身之操作之授權期間發生。舉例而言，一裝置110可製造有一初始組的組件112。某些組件112可對裝置110之操作更重要，使得裝置110在不具有該等物項之情況下或在不具有該等物項之特定版本(例如，原始設備製造商或「OEM」版本)之情況下不被准許操作。以圖解說明方式，一輸注泵之MCU可被視為重要的，使得泵在不具有一OEM版本之情況下不被准許操作。在不連接至一有線電源時為泵提供電力之一電池可被視為不那麼重要，使得泵被准許使用電池之一非OEM版本來操作。然而，若除電池外亦有太多其他部件係非OEM的，則甚至在存在如MCU等「重要」組件之情況下，泵可能不被准許操作。為了基於組件之經表徵重要性促成此處理，可基於個別組件之經表徵重要性給個別組件指派加權因子或賦予可變數目個秘密分享。當執行一授權處理程序時，所需秘密分享

之門檻量可係指派給每一當前組件之基於加權因子之經加權秘密分享或秘密分享組之一門檻量。

【0045】 在[1]處，簽章管理器130或裝置110之某一其他模組或組件可獲得存在於裝置110中之組件之識別符。在某些實施例中，簽章管理器130可獲得裝置110之所有組件112或僅某些組件112 (例如， n 個最重要組件或為了功能被授權而指定之組件)之識別符114。

【0046】 在[2]處，簽章管理器130或裝置110之某一其他模組或組件可獲得與在[1]處獲得之組件識別符相關聯之秘密分享及權重。權重及秘密分享可自一資料儲存區120、簽章管理器130中之一單獨資料儲存區或裝置110之某一其他模組或組件獲得。在某些實施例中，權重及秘密分享可能在製造裝置110時已被設定且儲存於裝置110中。舉例而言，製造商可根據藉由將較高權重(例如，介於0.75與1.0之間的權重)指派給被認為較重要之組件且將較低權重(例如，介於0.5與0.75之間的權重)指派給被認為不那麼重要之組件而使某些組件優先於其他組件之一啟發學習法來判定權重。表示秘密分享之分享資料124a...124n及表示權重之權重資料402a...402n可儲存於資料儲存區120或裝置110之某一其他模組或組件中。在某些實施例中，可替代地端視組件之相對重要性給組件指派不同數目個秘密分享(例如，可給較重要組件指派比不那麼重要之組件多之秘密分享)而不是使用不同權重來表示組件之相對重要性。舉例而言，若一組件具有一權重5，則可將5個不同秘密分享分配給該組件，而具有一權重1之另一組件可僅被分配1個分享。本文中所闡述之實例加權方法僅係說明性的且不意欲係限制性的。在某些實施例中，可使用用於使用經加權秘密分享之其他方法。

【0047】 在[3]處，簽章管理器130或裝置110之某一其他模組或組件可在可能之情況下使用秘密分享及權重產生數位簽章分享。在某些實施例中，簽章管理器130可使用同一符記及不同秘密分享中之每一者產生一不同簽章分享，如上文更詳細地闡述。

【0048】 在[4]處，簽章管理器130或裝置110之某一其他模組或組件可使用上文所判定之簽章分享產生一數位簽章。在某些實施例中，一預定義函數可使用簽章分享來產生數位簽章。該函數之輸出可係自其產生簽章分享之輸入值(或經雜湊輸入值)之一經加密版本。

【0049】 在[5]處，簽章管理器130或裝置110之某一其他模組或組件可獲得表示驗證密鑰之驗證密鑰資料126，該驗證密鑰將用於驗證使用簽章分享產生之數位簽章。

【0050】 在[6]處，簽章管理器130或裝置110之某一其他模組或組件可使用上文所獲得之驗證密鑰來驗證訊息。在某些實施例中，簽章管理器130可使用一預定義解密函數及驗證密鑰作為解密密鑰來將訊息解密。若經解密訊息匹配原始資料項目(或原始資料項目之雜湊)，則判定正確數位簽章。否則，若經解密訊息不匹配原始資料項目(或其雜湊)，則判定一不正確數位簽章。

【0051】 在[7]處，簽章管理器130或裝置110之某一其他模組或組件可判定上文在方塊314處是否驗證了數位簽章。若如此，則對功能(或裝置110自身之操作)授權。舉例而言，可准許裝置110進入其中可正常地使用裝置110之一就緒狀態。若簽章管理器130判定未驗證數位簽章，則不對功能(或裝置110自身之操作)授權。舉例而言，裝置110可進入其中阻止正常操作之一經阻止狀態。

基於門檻之多組件授權

【0052】圖5係在基於門檻之多組件授權(亦稱為「群集(swarm)」鑑認)期間之說明性資料流及各種裝置110a、110b、…110n(分別具有資料儲存區120a、120b、…120n)、一裝置管理系統100及一應用程式伺服器500之間的互動之一方塊圖。所顯示互動可在一裝置(諸如裝置110a，其可與識別符502a及秘密分享504a相關聯)連接至一應用程式伺服器500或以其他方式嘗試執行一網路操作時發生。應用程式伺服器500(或網路環境之某一其他組件)可阻止裝置110a連接至應用程式伺服器500或執行某一其他網路功能，直至裝置110a被授權為止。授權處理程序可需要門檻數目個其他裝置110b、…110n主動地或被動地參與。藉由要求使用多個其他裝置對裝置110a授權，可阻止裝置110a操作，除非其與門檻數目個其他裝置一起連接至一網路。此阻止單一裝置或小數目個裝置(例如，可能丟失或被偷竊或以其他方式在一多裝置網路環境(諸如一醫院)外部使用之裝置)之使用。

【0053】在[a]處，一裝置110a嘗試連接至應用程式伺服器500或執行要求首先鑑認裝置110a之某一其他網路操作。在某些實施例中，裝置110a可係醫療裝置(諸如一輸注泵)，且應用程式伺服器500可係一相關臨床系統(諸如一輸注控制伺服器)。以圖解說明方式，輸注控制伺服器可關於待施配之藥物、待治療之病人、待輸注之劑量、待實施之安全措施等對輸注泵作出指示。因此，輸注泵製造商之關注點可在於阻止輸注泵之操作(例如，阻止泵接收藥物施配資訊)，除非且直至輸注泵可首先驗證其係一恰當臨床環境(諸如具有門檻數目個其他此類泵之一環境)之部分。

【0054】在[b]處，應用程式伺服器500可採用裝置管理系統100之

服務來鑑認裝置110a。應用程式伺服器500可產生待由裝置管理系統100簽章之一符記或其他資料。應用程式伺服器500可儲存或以其他方式存取一驗證密鑰，該驗證密鑰可用於驗證自裝置管理系統100接收之經簽章訊息，如下文更詳細地論述。在某些實施例中，應用程式伺服器500可執行下文闡述為由裝置管理系統100執行之功能中之某些或全部，或裝置管理系統100可執行闡述為由應用程式伺服器500執行之功能中之某些或全部。舉例而言，應用程式伺服器500及裝置管理系統100可係包含經組態以執行所揭示操作之一或多個計算裝置之一較大整合式系統之子系統。

【0055】在[c]處，裝置管理系統100可獲得將參與多裝置授權之裝置110b...110n之識別符及/或對應秘密分享。舉例而言，當個別裝置110b...110n啟動、連接至網路環境、連接至應用程式伺服器500、自身被授權或發生諸如此類情況時，裝置110b...110n可各自將其秘密分享504b...504n提供至裝置管理系統100。作為另一實例，裝置110b...110n可提供其識別符502b...502n (例如，序號、網際網路協定或「IP」位址、媒體存取控制或「MAC」位址、特殊應用識別符等)。在[d]處，裝置管理系統100可使用識別符來存取對應於裝置之秘密分享。作為另一實例，裝置管理系統100可回應於自應用程式伺服器500接收到一符記及鑑認請求而自裝置110b...110n擷取秘密分享及/或識別符。

【0056】可在製造裝置時、在於網路環境中實施裝置時、在使用一多裝置授權處理程序鑑認裝置時等將秘密分享指派給裝置。在某些實施例中，可將秘密分享指派給裝置達若干時間週期，或可回應於特定事件之發生而撤銷秘密分享。舉例而言，可給一裝置110b指派一秘密分享達一預定或動態判定之時間週期(例如，1小時、1天、1年、1網路通信工作階段

等)，此後必須給裝置110b重新指派一分享或更新其秘密分享(例如，在針對裝置110b之一多裝置授權處理程序完成時)。

【0057】 在[e]處，授權管理器104或裝置管理系統100之某一其他模組或組件可在可能之情況下使用秘密分享產生簽章分享，如上文更詳細地論述。在某些實施例中，一預定義加密函數可使用個別秘密分享來將同一資料項目加密，從而產生一組簽章分享。該資料項目可係自應用程式伺服器500接收之符記或其他資料。可將資料項目直接加密，或可首先處理資料項目(例如，可使用一雜湊演算法產生一雜湊)。可針對每一可用秘密分享重複此處理程序，如上文所闡述。

【0058】 在[f]處，授權管理器104或裝置管理系統100之某一其他模組或組件可使用上文所判定之簽章分享產生一數位簽章。可僅在當執行授權處理程序時對應於門檻數目個裝置110a...110n之門檻數目個秘密分享可用之情況下產生一有效數位簽章。若存在少於門檻數目個秘密分享，則要判定一有效數位簽章可係不可能的或計算上不可行的。在此例項中，可中止授權處理程序，及/或可將一錯誤訊息或其他失敗訊息傳回至應用程式伺服器500。

【0059】 在[g]處，授權管理器104或裝置管理器100之某一其他模組或組件可將數位簽章(例如，經加密符記)發送至應用程式伺服器500。

【0060】 在[h]處，應用程式伺服器500可存取表示驗證密鑰之驗證密鑰資料504，且使用一預定義解密函數及驗證密鑰作為解密密鑰來將訊息解密。若經解密訊息匹配發送至裝置管理器100之原始符記(或自其導出之資料，諸如一雜湊)，則判定正確數位簽章。在此例項中，裝置110a可被視為被授權，此乃因至少門檻數目個其他裝置參與了授權處理程序。否

則，若經解密訊息不匹配原始資料項目(或其雜湊)，則判定一不正確數位簽章。在此例項中，應用程式伺服器500可因裝置110a尚未被授權而阻止裝置110a執行裝置110a正嘗試執行之功能。此可在少於門檻數目個裝置參與該處理程序時(諸如在裝置110係在一既定臨床環境外部使用(例如，該裝置丟失、被偷竊或被銷售)時)發生。

使用經加權秘密分享之基於門檻之安全實施

【0061】圖6係在基於門檻之安全實施期間之說明性資料流及一裝置110與一裝置管理系統100之間的互動之一方塊圖。在基於門檻之安全實施中，一多組件系統之不同組件可參與識別安全風險及實施安全策略。舉例而言，單一裝置110之不同組件112可參與，一分散式系統之不同裝置110可參與等。有利地，可給個別組件各自指派一權重。在組件(或組件與其相關聯之單獨安全模組)偵測到發生影響系統安全之安全事件時，組件可調整其加權因子以反映該影響。舉例而言，若一個安全監測模組(亦稱為一安全監測器或安全模組)判定已發生或可能發生一安全風險，則安全模組可減小安全模組被指派給的組件之加權因子。使用各種組件之秘密分享及加權因子來對系統功能授權。若足夠的組件已被提供較低權重使得在授權處理程序期間不使用門檻量之經加權秘密分享，則授權處理程序將失敗。

【0062】所顯示互動可在一裝置110連接至裝置管理系統100或以其他方式嘗試執行一網路操作時發生。在某些實施例中，當裝置110與一應用程式伺服器(諸如上文所闡述之應用程式伺服器500)通信時，可使用基於門檻之安全實施。

【0063】在[i]處，與裝置110之一特定組件(例如個別的組件112a或

112n)相關聯之一安全模組(例如安全模組602a或602n)可判定已發生一安全事件。舉例而言，安全模組602a可偵測安全事件，諸如失敗的登入嘗試、藥物或配量警報、安全更動事件、重複試通、網路掃描活動、拒絕服務條件、其他警報或錯誤及諸如此類。在某些實施例中，裝置110可係一醫療裝置，諸如一輸注泵。在此例項中，組件112a可係輸注泵之一組件(諸如一MCU)，且安全模組602a可被指派給MCU或與MCU整合在一起。安全模組602a可偵測安全事件，諸如要輸注藥物之無效嘗試、指示要輸注一不安全劑量之一嘗試之警報或諸如此類。

【0064】在[ii]處，安全模組602a可基於安全模組602a偵測到的安全事件而修改權重604a。調整權重604a之程度可係遞增的，或可基於所偵測到的特定事件而動態判定。舉例而言，在裝置110開始操作時，權重604a可具有一開始或預設值(例如，1.0)。安全模組602a可經組態以針對所偵測到的每一安全風險按一遞增量降低權重604a (例如，針對每一失敗的登入嘗試、每一藥物劑量警報等將權重降低0.05)。作為另一實例，安全模組602a可經組態以端視所識別出的特定安全風險按一變化量降低權重(例如，在三次失敗的登入嘗試之後將權重降低0.1，在兩次藥物劑量警報之後將權重降低0.2等)。

【0065】在某些實施例中，安全模組602a可在經過一預定或動態判定之時間週期等之後回應於某些事件而增加權重604a。舉例而言，安全模組602a可在已經過一時間週期(例如，10分鐘、1小時等)之後在無一負面安全事件發生之情況下增加權重604a。作為另一實例，安全模組602a可回應於一管理員登入至系統而將權重604a重設至其預設值。在某些實施例中，安全模組602a可僅在最大值與最小值之間調整一權重604a (例如，不

可准許權重降低至低於0.0或升高至高於1.0)。

【0066】 本文中所闡述之實例安全事件、加權因子值及調整規則僅係說明性的，且不意欲係限制性的。在某些實施例中，可使用較少、額外及/或替代事件、加權因子值及調整規則。

【0067】 在[iii]處，裝置110可嘗試執行一特定功能，諸如連接至裝置管理系統100或執行要求首先確證裝置110之安全狀態之某一其他網路操作。舉例而言，若裝置110係一醫療裝置(諸如一輸注泵)，則該裝置可嘗試輸注藥物、連接至一網路伺服器以獲得關於藥物、劑量或病人之資料等。因此，輸注泵之製造商之關注點可在於阻止輸注泵之操作(例如，阻止泵接收藥物施配資訊)除非且直至可首先確證輸注泵之安全狀態。

【0068】 在[iv]處，裝置管理系統100可產生待由裝置110簽章之一符記或其他資料。裝置管理系統100可儲存或以其他方式存取一驗證密鑰，該驗證密鑰可用於驗證自裝置110接收之經簽章訊息，如下文更詳細地論述。

【0069】 在[v]處，簽章管理器130或裝置110之某一其他模組或組件可獲得組件112a...112n之識別符以及對應秘密分享及權重。舉例而言，簽章管理器130可判定組件112a...112n之識別符114a...114n。然後，簽章管理器130可自資料儲存區120獲得對應秘密分享124a...124n及權重604a...604n。

【0070】 在[vi]處，簽章管理器130或裝置110之某一其他模組或組件可使用秘密分享124a...124n及權重604a...604n產生簽章分享，如上文更詳細地論述。然後，可使用簽章分享產生一數位簽章。若經加權秘密分享之量不能滿足門檻量，則要判定一有效數位簽章可係不可能的或在計算

上不可行的。在此例項中，可中止授權處理程序，及/或可傳回一錯誤訊息或其他失敗訊息。

【0071】 若產生了門檻數目個簽章分享，則簽章管理器130可產生數位簽章，如上文更詳細地闡述。

【0072】 在[vii]處，裝置110可將經簽章訊息(例如，經加密符記)發送至裝置管理系統100。

【0073】 在[viii]處，裝置管理系統100可獲得表示驗證密鑰之驗證密鑰資料606，且使用一預定義解密函數及驗證密鑰作為解密密鑰來將訊息解密。若經解密訊息匹配發送至裝置管理系統100之原始符記(或自其導出之資料，諸如一雜湊)，則判定正確數位簽章。在此例項中，裝置110可被視為處於一安全狀態，此乃因由裝置110之各種組件維持之至少門檻量之經加權秘密分享可用於授權處理程序。否則，若經解密訊息不匹配原始資料項目(或其雜湊)，則判定一不正確數位簽章。在此例項中，裝置管理系統100可阻止裝置110與裝置管理系統100、其他網路系統(例如，應用程式伺服器500)通信以執行特定操作等。

其他考量

【0074】 應理解，未必可根據本文中所闡述之任一特定實施例來達成所有目標或優點。因此，舉例而言，熟習此項技術者將認識到，某些實施例可經組態而以達成或最佳化如本文中所教示之一個優點或優點群組而不必達成如本文中可教示或建議之其他目標或優點之一方式來操作。

【0075】 除本文中所闡述之彼等外的諸多變化形式將自本發明顯而易見。舉例而言，端視實施例，本文中所闡述之演算法中之任一者之某些動作、事件或功能可以一不同順序執行、可被添加、合併或共同忽視(例

如，並非所有所闡述動作或事件皆對演算法之實踐係必要的)。此外，在某些實施例中，動作或事件可例如透過多執行緒處理、中斷處理或多個處理器或處理器核心或者在其他並列架構上同時執行而非依序執行。另外，不同任務或處理程序可由可一起工作之不同機器及/或計算系統執行。

【0076】 結合本文中所揭示之實施例闡述之各種說明性邏輯區塊、模組及演算法元素可實施為電子硬體、電腦軟體或兩者之組合。為清楚圖解說明硬體與軟體之此可互換性，上文通常已就各種說明性組件、區塊、模組及元素之功能性對其等進行了闡述。此功能性是實施為硬體還是軟體取決於特定應用及施加於總體系統上之設計約束。所闡述功能性可針對每一特定應用以不同方式實施，但此等實施決策不應被解釋為致使背離本發明之範疇。

【0077】 結合本文中所揭示之實施例而闡述之各種說明性邏輯區塊及模組可由一機器實施或執行，諸如一電腦處理器、一數位信號處理器(DSP)、一特殊應用積體電路(ASIC)、一場可程式化閘陣列(FPGA)或其他可程式化邏輯裝置、離散閘或電晶體邏輯、離散硬體組件或其經設計以執行本文中所闡述之功能之任何組合。一電腦處理器可係一微處理器，但在替代方案中，處理器可係一控制器、微控制器或狀態機、其等之組合，或諸如此類。一處理器可包含經組態以處理電腦可執行指令之電路。在另一實施例中，一處理器包含執行邏輯操作而不處理電腦可執行指令之一FPGA或其他可程式化裝置。一處理器亦可實施為計算裝置之一組合，例如，一DSP與一微處理器之一組合、複數個微處理器之一組合、一或多個微處理器與一DSP核心之聯合或任一其他此類組態。儘管本文中主要關於數位技術進行闡述，但一處理器亦可主要包含類比組件。舉例而言，本文

中所闡述之信號處理演算法中之某些或全部可在類比電路或混合式類比與數位電路中實施。一計算環境可包含任何類型之電腦系統，包含但不限於，基於一微處理器之一電腦系統、一主機電腦、一數位信號處理器、一可攜式計算裝置、一裝置控制器，或在一器具內之一計算引擎，僅舉幾項實例。

【0078】結合本文中所揭示之實施例闡述之一方法、處理程序或演算法之元素可直接以硬體、以儲存於一或多個記憶體裝置中且由一或多個處理器執行之一軟體模組或以兩者之一組合體現。一軟體模組可駐存於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟機、一可抽換式磁碟、一CD-ROM或者本技術領域中已知之任一或若干其他形式之非暫時性電腦可讀儲存媒體或實體電腦儲存裝置。一實例儲存媒體可耦合至處理器，使得該處理器可自該儲存媒體讀取資訊並將資訊寫入至該儲存媒體。在替代方案中，儲存媒體可係處理器之組成部分。儲存媒體可係揮發性或非揮發性的。處理器及儲存媒體可駐存於一ASIC中。ASIC可駐存於一使用者終端機中。在替代方案中，處理器及儲存媒體可作為離散組件駐存於一使用者終端機中。

【0079】此外，除非另外具體陳述或另外在內容脈絡內如所使用而理解，否則本文中所使用之條件語言(尤其諸如「可(can)」、「可能(might)」、「可以(may)」、「例如(e.g.)」及諸如此類)通常意欲傳達某些實施例包含而其他實施例不包含某些特徵、元件及/或狀態。因此，此條件語言通常不意欲暗示一或多項實施例以任何方式需要特徵、元件及/或狀態或者一或多項實施例必然包含在有或沒有作者輸入或提示之情況下決定在任一特定實施例中是否包含或執行此等特徵、元件及/或狀態之邏

輯。術語「包括 (comprising)」、「包含 (including)」、「具有 (having)」及諸如此類係同義詞且係以一開放方式包含性地使用且不排除額外元件、特徵、動作、操作等等。並且，術語「或」係以其包含意義 (且不以其排除意義) 使用，使得在例如用於連接一元素清單時，術語「或」意指該清單中之元素中之一者、某些或全部。此外，如本文中所使用，術語「每一」除具有其普通含義之外亦可意指術語「每一」被應用到的一組元素之任一子集。

【0080】 除非另外具體陳述，否則諸如片語「X、Y或Z中之至少一者」之析取語言應以其他方式與內容脈絡一起理解為一般性地用於表示一項目、條目等可係X、Y或Z或者其任一組合(例如，X、Y及/或Z)。因此，此類析取語言通常不意欲且不應暗示某些實施例需要呈現X中之至少一者、Y中之至少一者，或Z中之至少一者中的每一者。

【0081】 除非另外明確陳述，否則諸如「一(a)」、「一(an)」或「該(the)」等冠詞應通常解釋為包含一或多個所闡述項目。因此，諸如「一裝置，其經組態以」等片語意欲包含一或多個所敘述裝置。此一或多個所敘述裝置亦可共同經組態以執行所陳述敘述。舉例而言，「一處理器，其經組態以執行敘述A、B及C」可包含經組態以執行敘述A之一第一處理器，其聯合經組態以執行敘述B及C之一第二處理器一起工作。

【0082】 雖然以上詳細說明已展示、闡述且指出適用於各種實施例之新穎特徵，但將理解，可在不背離本發明之精神之情況下在所圖解說明之裝置或演算法之形式及細節方面作出各種省略、替代及改變。如將認識到，本文中所闡述之某些實施例可在不提供本文中所陳述之所有特徵及益處之一形式內實施，此乃因某些特徵可與其他特徵分開使用或實踐。所有

此等修改及變化形式皆意欲包含於本文中在本發明之範疇內。此外，藉由組合本文中所闡述之一或多項實施例之任兩個或更多個特徵或技術而形成之額外實施例亦意欲包含於本文中在本發明之範疇內。

【符號說明】

【0083】

100: 裝置管理系統

102: 分享管理器

104: 授權管理器

106: 資料儲存區

110: 裝置

110a-110n: 裝置

112: 組件/處理器組件/記憶體組件/長期儲存組件/原始組件/初始組的組件

112a-112n: 組件

114: 識別符

114a-114n: 識別符

120: 資料儲存區

120a-120n: 資料儲存區

122: 作業系統

124: 分享資料

124a-124n: 分享資料

126: 驗證密鑰資料

130: 簽章管理器

150: 通信網路/網路

300: 說明性處理程序/處理程序

302: 方塊

304: 方塊

306: 方塊

308: 方塊

310: 方塊

312: 方塊

314: 方塊

316: 方塊

318: 方塊

320: 方塊

322: 方塊

402a-402n: 權重資料

500: 應用程式伺服器

502a-502n: 識別符

504: 驗證密鑰資料

504a-504n: 秘密分享

602a-602n: 安全模組

604a-604n: 權重

606: 驗證密鑰資料

[1]: 操作

[2]: 操作

[3]: 操作

- [4]: 操作
- [5]: 操作
- [6]: 操作
- [7]: 操作
- [A]: 操作
- [B]: 操作
- [C]: 操作
- [D]: 操作
- [E]: 操作
- [a]: 操作
- [b]: 操作
- [c]: 操作
- [d]: 操作
- [e]: 操作
- [f]: 操作
- [g]: 操作
- [h]: 操作
- [i]: 操作
- [ii]: 操作
- [iii]: 操作
- [iv]: 操作
- [v]: 操作
- [vi]: 操作

[vii]: 操作

[viii]: 操作

【發明申請專利範圍】

【請求項1】

一種輸注泵，其包括：

一安全監測器；

一馬達控制單元，其經組態以控制藥物之輸注，其中該馬達控制單元與一第一組件識別符相關聯；

一電池，其經組態以給該輸注泵供電，其中該電池與一第二組件識別符相關聯；

一電腦處理器，其係用可執行指令程式化，其中該電腦處理器與一第三組件識別符相關聯；及

一資料儲存區，其儲存：

驗證密鑰資料，其表示一驗證密鑰；

分享資料，其表示用於產生一數位簽章之複數個秘密分享，其中該複數個秘密分享中之一第一秘密分享與該第一組件識別符相關聯，其中該複數個秘密分享中之一第二秘密分享與該第二組件識別符相關聯，且其中該複數個秘密分享中之一第三秘密分享與該第三組件識別符相關聯；及

複數個權重，其中該複數個權重中之個別權重與該複數個秘密分享中之個別秘密分享相關聯；

其中該電腦處理器係藉由該等可執行指令程式化以至少：

判定已發佈用於執行控制該輸注泵之一功能之軟體之一命令；

判定複數個組件識別符，其中該複數個組件識別符中之個別組件識別符對應於在發佈該命令時存在的該輸注泵之個別組件；

至少部分地基於該複數個組件識別符而載入該複數個秘密分享之至少一子集；

使用該複數個秘密分享之該子集產生複數個簽章分享，其中需要門檻數目個經加權分享以便產生門檻數目個簽章分享；

使用該複數個簽章分享產生該數位簽章；

使用該驗證密鑰驗證該數位簽章；及

授權執行該軟體；及

其中該安全監測器經組態以至少：

偵測一安全事件之發生；及

至少部分地基於該安全事件修改一權重之一值，其中該權重與該輸注泵之一組件相關聯，且其中該安全監測器與該輸注泵之該組件相關聯。

【請求項2】

如請求項1之輸注泵，其中該安全事件包括以下各項中之一者：一失敗的登入嘗試、一藥物警報、一安全更動嘗試、一重複試通、網路掃描活動、一拒絕服務事件，或一錯誤。

【請求項3】

一種用於授權執行輸注系統命令之電腦實施之方法，該電腦實施之方法包括由經組態以執行特定指令之一或多個計算裝置執行之以下操作：

判定複數個組件識別符，其中每一組件識別符包括一輸注系統之一對應組件之一識別符；

針對該複數個組件識別符中之每一組件識別符判定用於產生一數位簽章之一對應秘密分享；

儲存該複數個組件識別符及該等對應秘密分享；

儲存與該等秘密分享相關聯之一驗證密鑰；

接收用於執行之一系統命令；及

起始一預執行授權程序，該預執行授權程序包括：

判定該複數個組件識別符之至少一組件識別符子集，其中該組件識別符子集對應於在該預執行授權程序期間存在的該輸注系統之組件；

針對每一秘密分享，判定一對應加權因子，其中需要門檻量的經加權秘密分享以便產生該數位簽章；

載入至少一秘密分享子集，其中該秘密分享子集中之每一秘密分享對應於該組件識別符子集中之一組件識別符；

使用該秘密分享子集產生該數位簽章，其中需要門檻量的秘密分享以便產生該數位簽章；

使用該驗證密鑰驗證該數位簽章；及

授權執行該系統命令；

偵測一安全事件之發生；及

至少部分地基於該安全事件，修改一加權因子之一值。

【請求項4】

如請求項3之電腦實施之方法，其中偵測該安全事件之發生包括偵測以下各項中之一者：一失敗的登入嘗試、一藥物警報、一安全更動嘗試、一重複試通、網路掃描活動、一拒絕服務事件，或一錯誤。

【請求項5】

如請求項3之電腦實施之方法，其進一步包括回應於授權執行該系統

命令而執行該系統命令，其中執行該系統命令包括以下各項中之一者：執行特許軟體、施配藥物，或與一網路伺服器通信。

【請求項6】

如請求項3之電腦實施之方法，其中儲存一秘密分享包括將該秘密分享儲存於與該輸注系統之一對應組件相關聯之一安全儲存位置中。

【請求項7】

如請求項3之電腦實施之方法，其中儲存一秘密分享包括儲存該秘密分享之一混淆版本。

【請求項8】

一種基於門檻簽章之醫療裝置管理之系統，該系統包括：
複數個醫療裝置；
一授權管理器；及
一應用程式伺服器，其包括一或多個計算裝置，其中該應用程式伺服器經組態以至少：

自該複數個醫療裝置中之一第一醫療裝置接收關於該第一醫療裝置之操作之一通信；

在對該通信作出回應之前判定起始用以對該第一醫療裝置授權之一授權處理程序；

將一符記發送至該授權管理器；

自該授權管理器接收一數位簽章；

使用一驗證密鑰及該符記驗證該數位簽章；

基於驗證該數位簽章判定該第一醫療裝置被授權操作；及

對該通信作出回應；且

其中該授權管理器包括一或多個計算裝置且經組態以至少：

自該應用程式伺服器接收該符記；

至少部分地基於該複數個醫療裝置之至少一子集與該授權管理器通信而識別該複數個醫療裝置之該子集；

存取與該複數個醫療裝置之至少該子集相關聯之秘密分享資料，其中與該子集中之一第一醫療裝置相關聯之秘密分享資料表示用於產生一數位簽章之一秘密分享，且其中需要門檻數目個秘密分享以便產生該數位簽章；

使用該秘密分享資料及該符記產生該數位簽章；及

將該數位簽章發送至該應用程式伺服器。

【請求項9】

如請求項8之系統，其中該應用程式伺服器經組態以驗證該數位簽章包括：該應用程式伺服器經組態以至少：

使用該數位簽章及該驗證密鑰產生一經解密訊息，其中該驗證密鑰包括用於一解密函數之一解密密鑰；及

判定該經解密訊息包括表示該符記之資料。

【請求項10】

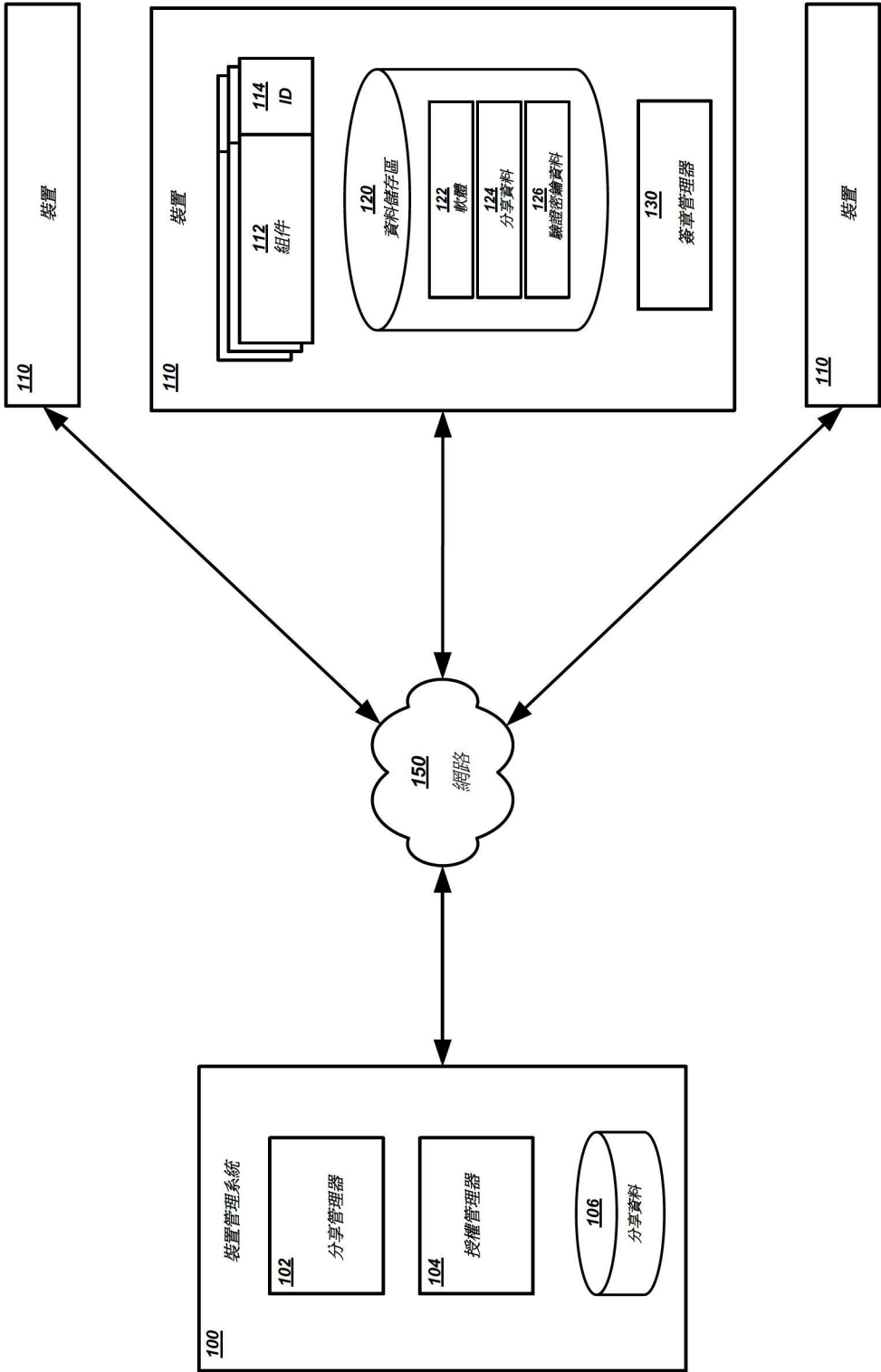
如請求項8之系統，其中該授權管理器經組態以產生該數位簽章包括：該授權管理器經組態以使用一秘密分享作為用於一加密函數之一加密密鑰來將該符記加密。

【請求項11】

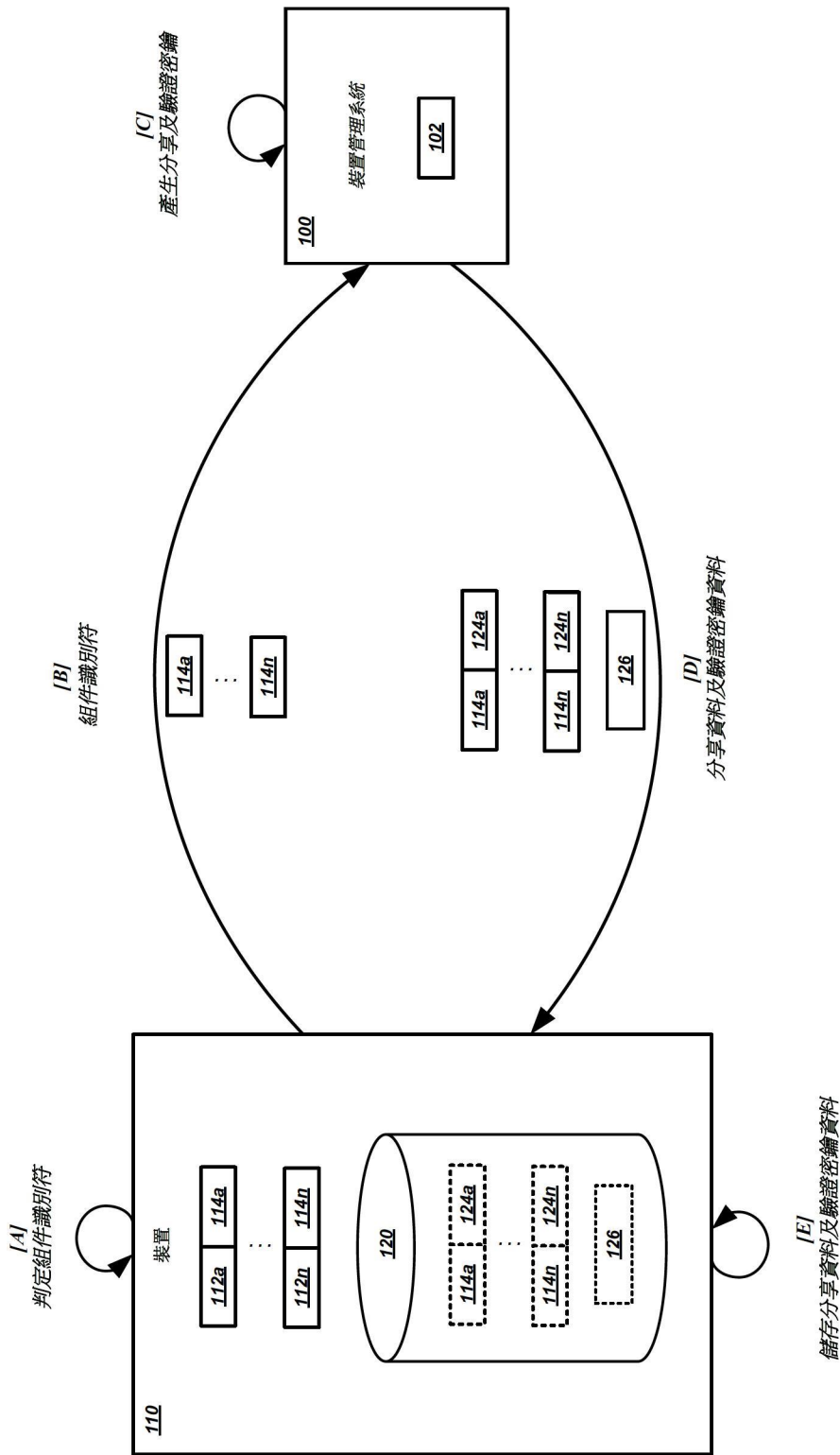
如請求項8之系統，其中該授權管理器經組態以產生該數位簽章包括：該授權管理器經組態以至少：

使用該門檻數目個秘密分享產生門檻數目個簽章分享；及
使用該門檻數目個簽章分享產生該數位簽章。

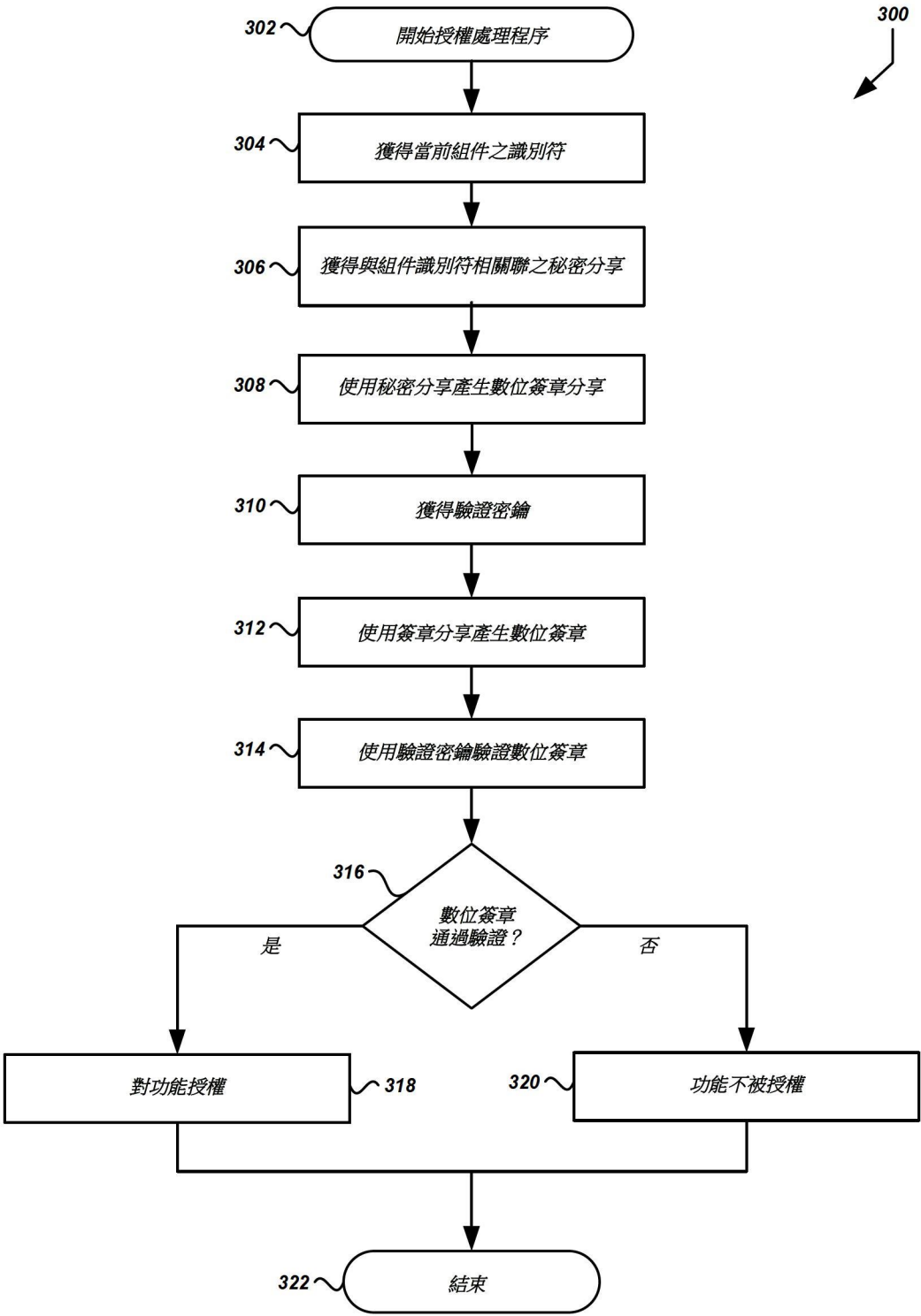
【發明圖式】



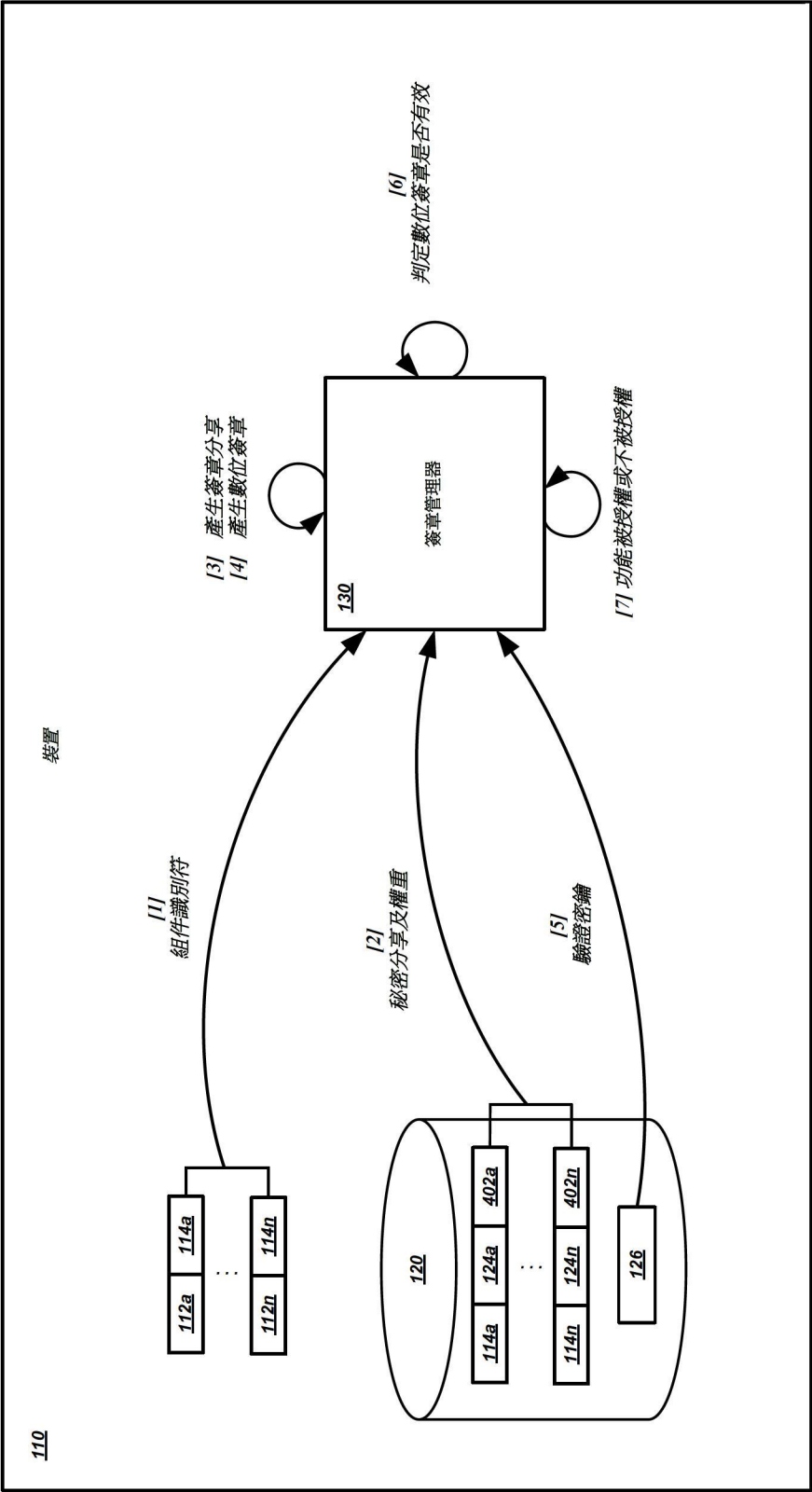
【圖1】



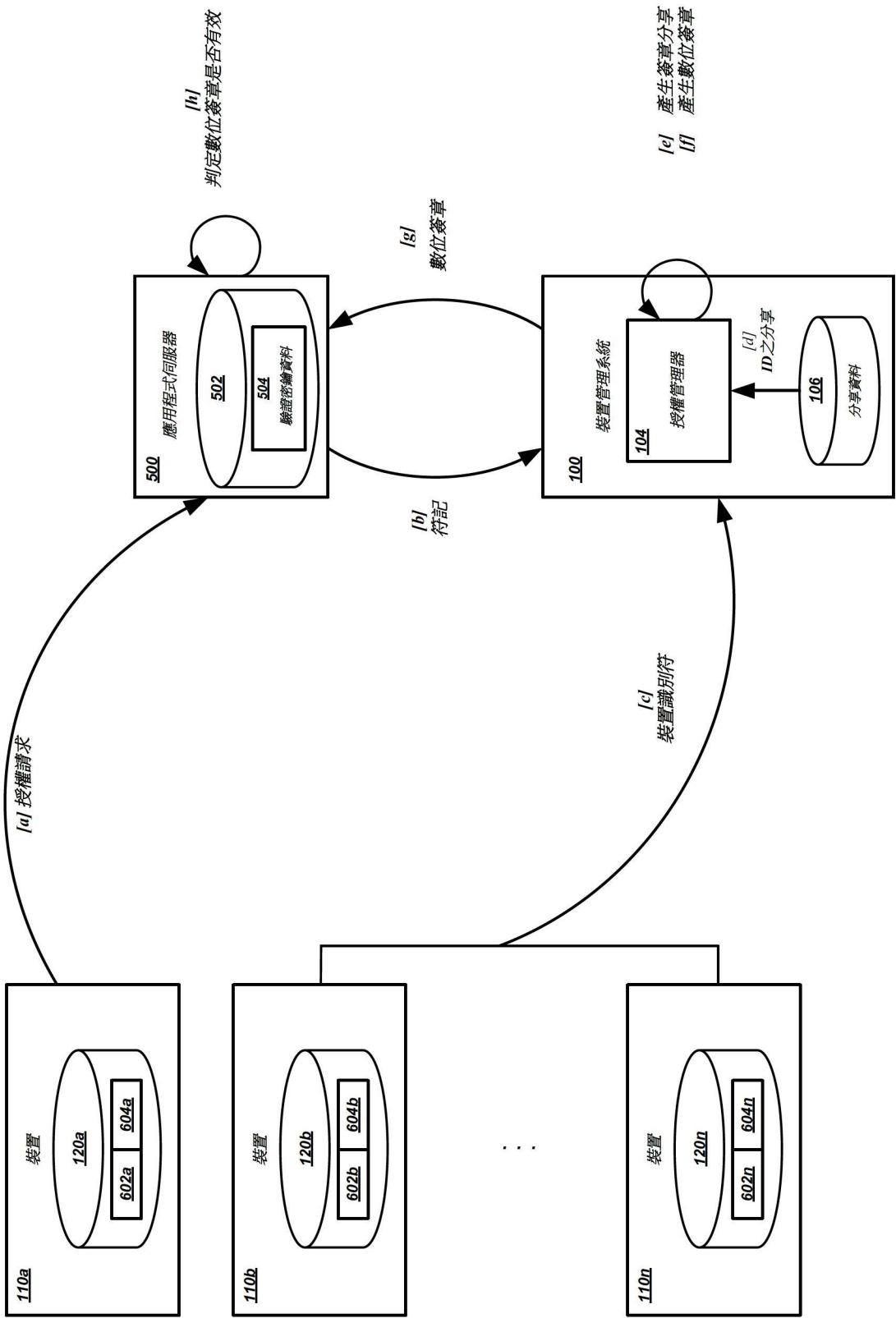
【圖2】



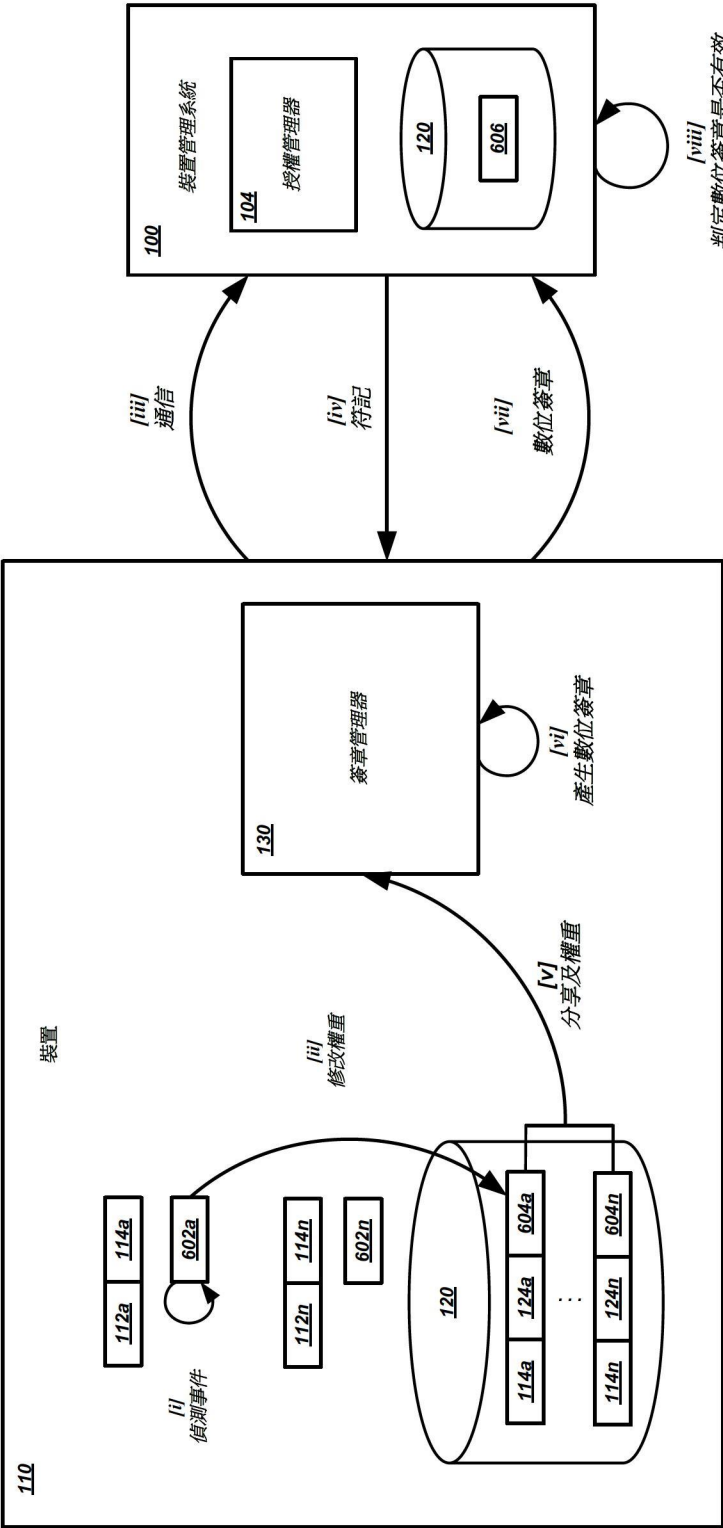
【圖3】



【圖4】



【圖5】



【圖6】