I620430

(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 I620430 B**

(45)公告日： 中華民國 107 (2018) 年 04 月 01 日

(21)申請案號：104104009 (22)申請日： 中華民國 104 (2015) 年 02 月 05 日

(51)Int. Cl.： *H04L29/06 (2006.01)* *H04L9/30 (2006.01)*
G06F9/54 (2006.01) *G06F21/64 (2013.01)*

(30)優先權：2014/02/05 美國 61/935,967

(71)申請人：蘋果公司 (美國) APPLE INC. (US)
美國

(72)發明人：麥克勞林 凱文P MCLAUGHLIN, KEVIN P. (US)；柏克斯 安德魯 BURKS, ANDREW (US)；拉瑪 史瑞尼菲 RAMA, SRINIVAS (US)；那達瑟 阿納許 NADATHUR, ANUSH (IN)；阿布安 喬伊 ABUAN, JOE (US)；布萊利 包柏 BRADLEY, BOB (US)；多利 克雷格 DOOLEY, CRAIG (US)；高藍培斯基 葛瑞格 二世 GOLEMBESKI, GREGG, JR. (US)；馬席亞斯 艾隆 MATHIAS, ARUN (US)

(74)代理人：陳長文

(56)參考文獻：

TW 200937931A TW 201250481A
WO 2013/174540 WO 2014/004133A1

審查人員：林建儒

申請專利範圍項數：25 項 圖式數：39 共 250 頁

(54)名稱

用於控制器與配件之間通信的統一通信協定

UNIFORM COMMUNICATION PROTOCOLS FOR COMMUNICATION BETWEEN CONTROLLERS AND ACCESSORIES

(57)摘要

一統一協定可有助於一控制器器件與由該控制器控制之一配件器件之間的安全的經鑑認通信。一配件及一控制器可建立一配對，該配對之存在稍後可經驗證且用以建立一安全通信工作階段。該配件可提供將該配件定義為服務之一集合的一配件定義記錄，每一服務具有一或多個特性。在一安全通信工作階段內，該控制器可詢問該等特性以判定配件狀態及/或修改該等特性以指示該配件改變其狀態。

A uniform protocol can facilitate secure, authenticated communication between a controller device and an accessory device that is controlled by the controller. An accessory and a controller can establish a pairing, the existence of which can be verified at a later time and used to create a secure communication session. The accessory can provide an accessory definition record that defines the accessory as a collection of services, each service having one or more characteristics. Within a secure communication session, the controller can interrogate the characteristics to determine accessory state and/or modify the characteristics to instruct the accessory to change its state.

指定代表圖：

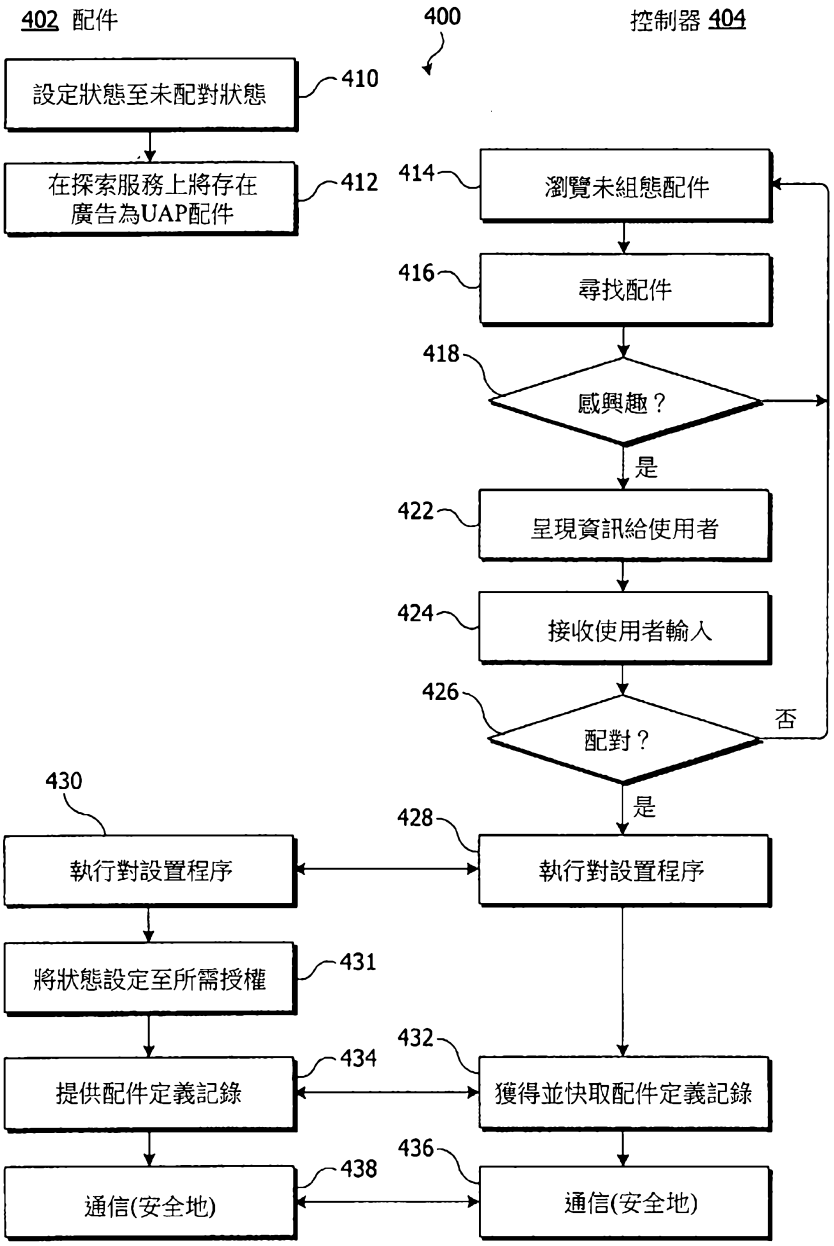


圖4

符號簡單說明：

400・・・用於藉由控制器來探索配件的程序

402・・・配件

404・・・控制器

410・・・區塊

412・・・區塊

414・・・區塊

416・・・區塊

418・・・區塊

422・・・區塊

424・・・區塊

426・・・區塊

428・・・區塊

430・・・區塊

431・・・區塊

432・・・區塊

434・・・區塊

436・・・區塊

438・・・區塊

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】

用於控制器與配件之間通信的統一通信協定

UNIFORM COMMUNICATION PROTOCOLS FOR COMMUNICATION BETWEEN CONTROLLERS AND ACCESSORIES

相關申請案之交叉參考

本申請案主張2014年2月5日申請的題為「用於配件管理系統之協定及規範(Protocols and Specifications for an Accessory Management System)」之美國臨時申請案第61/935,967號的權利，該臨時申請案的揭露內容係以全文引用方式併入本文中。

【先前技術】

本發明大體係關於電子器件之間的通信，且特定言之係關於用於控制器與配件之間的通信的統一通信協定。

電子器件在在應用範圍內變得愈來愈風行。行動電話、平板電腦、家庭娛樂系統及類似者僅為使用者有規律地互動的電子器件其中之一些。

變得更風行的另一類別之電子器件包括各種電子式可控制器件，諸如恆溫器、照明器件家用、家庭電氣設備等。

【發明內容】

目前，使用者可難以管理多個電子可控制器件或系統。舉例而言，使用者的家中可能具有恆溫器、電子可控制照明系統、家庭安全性系統等。每一此系統可由不同製造商製造，且每一製造商可提供使用者可在通用計算器件(諸如行動電話、平板或家庭電腦系統)上安裝

並執行的專用控制器器件(例如，基於IR之遙控器件)或控制器應用程式。每一控制器器件或應用程式通常係針對特定製造商之系統定製且不可與來自其他製造商之系統或甚至與來自同一製造商之其他系統可相互操作。此逐件方法不易可擴充。使用者尋求用可中央地進行控制或管理的系統之不同陣列來建立「智慧型家庭」環境或其類似者面臨累積過多控制器器件及/或控制器應用程式的需要。

本發明之某些實施例係關於用於控制器器件(或「控制器」)與待控制的任何數目之其他電子器件(在本文中被稱作「配件器件」或簡言之「配件」)之間的通信的「統一」協定。控制器可藉由為通用計算器件提供適當可執行程式碼而實施於(例如)通用計算器件(諸如桌上型電腦、膝上型電腦、平板電腦、行動電話、其他手持型或可穿戴式計算器件)上；替代地，控制器可為專用計算器件。配件可包括由控制器可控制的任何器件。配件之實例包括燈具、恆溫器、門鎖、自動開門器(例如，車庫開門器)、靜態或視訊攝影機等。配件及控制器可使用標準傳輸協定(諸如Wi-Fi、藍芽、藍芽LE或其類似者)經由有線或無線頻道彼此通信。

在一些實施例中，統一配件協定可定義用於將配件定義為服務之集合的簡單且可延伸之架構，且每一服務經定義為一組特性，該組特性中之每一者在任何給定時間具有已定義值。該等特性可表示配件之狀態的各種基本態樣。舉例而言，就恆溫器而言，特性可包括電源(恆溫器單元是接通或關斷)、當前溫度(恆溫器所測量到的實際溫度)及目標溫度(恆溫器設法維持的可設定溫度)。該協定可進一步定義可由控制器用來將命令及控制訊息(請求)發送至配件及配件用來發送回應訊息的訊息格式。該等請求可允許控制器詢問(例如，讀取)配件特性且在一些執行個體中修改(例如，寫入至)配件特性；例如，控制器可讀取電源特性以判定配件是接通或關斷且可寫入至電源特性以接通或關

斷配件。因此，不管功能如何，任何類型之配件可藉由發送適當請求來控制。配件可將配件定義記錄提供至控制器。該配件定義記錄可包括關於配件之所有可存取特性的完整資訊。控制器可在判定如何與配件互動中使用該配件定義記錄。舉例而言，來自該配件定義記錄之資訊可由控制器使用以建構用於操作配件之使用者介面以及建構至配件之請求訊息。

在一些實施例中，該協定可進一步定義配件可使用以通知控制器何時特性改變的通知機制。實例包括：被動式通知機制，其中控制器可關於任何特性是否已改變查詢配件；以及主動式或基於事件之通知機制，其中配件可在特定特性改變時選擇性地產生訊息至一或多個控制器。可同時支援多個通知機制，且控制器可選擇待用於特定配件、服務或特性之通知機制。

在一些實施例中，該協定可定義可用以防止未授權控制器操作配件之安全性措施。舉例而言，配件可經組態以接受僅來自先前已與配件建立配對且因此藉由配件來辨識的控制器之請求。建立配對可包括以安全方式在配件與控制器之間交換長期公用金鑰，其中每一器件持久地儲存該等金鑰。該協定可規定對設置程序以便減少配對未經配件之擁有者/操作員批准而建立的風險。舉例而言，在對設置程序期間，使用者可能需要讀取藉由一個器件(例如，配件)呈現之設置碼並將該設置碼輸入至另一器件(例如，控制器)中或使該等器件彼此實體靠近地置放。一旦配對建立，該配對即可被利用以提供端對端訊息加密，以使得僅配對控制器及配件可讀取在其間交換之訊息。舉例而言，當先前建立配對的配件及控制器重新連接時，該等器件可驗證先前配對(例如，藉由正面每一者擁有另一者的長期公用金鑰)且產生工作階段特定加密金鑰。

在一些實施例中，該協定可界定供控制器用於探索及組態其附近

之相容配件的程序。此等程序可簡化將新配件新增至藉由控制器管理之自動控制系統的任務。

以下詳細描述連同附圖將提供對本發明之性質及優點的更好理解。

【圖式簡單說明】

圖1展示根據本發明之一實施例的家庭環境。

圖2A至圖2D展示根據本發明之一實施例的配件特性之實例定義。

圖2E展示根據本發明之一實施例的可針對特性定義之特性之實例。

圖2F展示根據本發明之一實施例的可定義之延伸特性之實例。

圖2G至圖2H展示根據本發明之一實施例的配件服務之實例定義。

圖2I展示根據本發明之一實施例的可定義之配件資訊服務之實例。

圖2J展示根據本發明之一實施例的用於可定義之配件資訊服務的特性之實例。

圖3A至圖3C展示根據本發明之一實施例的配件定義記錄之實例。

圖4為根據本發明之一實施例的用於藉由控制器探索配件之程序的流程圖。

圖5A至圖5K展示根據本發明之一實施例的請求訊息及回應訊息之實例。

圖6A至圖6E展示根據本發明之一實施例的請求訊息及回應訊息之額外實例。

圖7展示根據本發明之一實施例的被動式通知程序之實例。

圖8展示根據本發明之一實施例的廣告式通知程序之實例。

圖9展示根據本發明之一實施例的主動式通知程序之實例。

圖10展示根據本發明之一實施例的事件通知程序之實例。

圖11A展示根據本發明之一實施例的訂用通知之請求訊息之實例。

圖11B展示根據本發明之一實施例的事件訊息之實例。

圖12展示根據本發明之一實施例的用於配件之配對設定檔的實例特性。

圖13A至圖13C展示根據本發明之一實施例的基於設置碼之對設置程序之實例。

圖14A至圖14C展示根據本發明之一實施例的使用鑑認晶片及安全性憑證之對設置程序之實例。

圖15A至圖15F展示根據本發明之一實施例的使用設置碼及安全性憑證之對設置程序之實例。

圖16展示根據本發明之一實施例的一般化對設置程序之實例。

圖17A至圖17C展示根據本發明之一實施例的對驗證程序之實例。

圖18A至圖18B展示根據本發明之一實施例的對新增程序之實例。

圖19 (包含圖19A及圖19B)展示根據本發明之一實施例的對移除程序之實例。

圖20展示根據本發明之一實施例的用於門鎖配件之實例操作環境。

圖21展示根據本發明之一實施例的用於門鎖配件之實例服務定義。

圖22展示根據本發明之一實施例的用以配對控制器與配件之程序之實例。

圖23展示根據本發明之一實施例的用於解除鎖定門之程序之實例。

圖24展示根據本發明之一實施例的用於IP攝影機配件之操作環境。

圖25A至圖25B展示根據本發明之一實施例的用於IP攝影機配件之實例服務定義。

圖26A至圖26E展示根據本發明之一實施例的針對圖25中所示之服務之特性的實例定義。

圖27A至圖27D展示根據本發明之一實施例的用於IP攝影機配件之配件定義記錄之實例。

圖28展示根據本發明之一實施例的用於控制IP攝影機配件之程序之實例。

圖29展示根據本發明之一實施例的開始媒體工作階段請求之實例。

圖30展示根據本發明之一實施例的開始媒體工作階段回應之實例。

圖31展示根據本發明之一實施例的結束媒體工作階段請求之實例。

圖32展示根據本發明之一實施例的結束媒體工作階段回應之實例。

圖33展示根據本發明之一實施例的用於IP串流服務之實例服務定義。

圖34展示根據本發明之一實施例的用於圖33之IP串流服務之實例特性定義。

圖35展示根據本發明之一實施例的用於IP串流之程序之實例。

圖36為根據本發明之一實施例的控制器之簡化方塊圖。

圖37為根據本發明之一實施例的配件之簡化方塊圖。

圖38為根據本發明之一實施例的控制器架構之簡化方塊圖。

圖39為根據本發明之一實施例的配件架構之簡化方塊圖。

【實施方式】

本發明之某些實施例係關於用於控制器器件(或「控制器」)與待控制的任何數目之其他電子器件(在本文中被稱作「配件器件」或簡言之「配件」)之間的通信的「統一」協定。控制器可藉由為通用計算器件提供適當可執行程式碼而實施於(例如)通用計算器件(諸如桌上型電腦、膝上型電腦、平板電腦、行動電話、其他手持型或可穿戴式計算器件)上；替代地，控制器可為專用計算器件。配件可包括由控制器可控制的任何器件。配件之實例包括燈具、恆溫器、門鎖、自動開門器(例如，車庫開門器)、靜態或視訊攝影機等。配件及控制器可使用標準傳輸協定(諸如Wi-Fi、藍芽、藍芽LE或其類似者)經由有線或無線頻道彼此通信。

實例環境

圖1展示根據本發明之一實施例的家庭環境100。家庭環境100包括可與位於環境100中之各種配件器件(亦被稱作配件)通信的控制器102。控制器102可包括(例如)桌上型電腦、膝上型電腦、平板電腦、智慧型手機、可穿戴式計算器件、個人數位助理或能夠如本文中所描述地將命令及控制訊息傳達到配件且呈現使用者介面以允許使用者指示對配件之所要操作的任何其他計算器件或器件集合。在一些實施例中，控制器102可使用多個離散器件來實施。舉例而言，可存在與配件通信之基地台(其在環境100中可安裝在固定位置中)，及提供使用者介面且與該基地台通信以實現對配件之控制的一或多個行動遙控台(例如，手持型或可穿戴式器件，諸如行動電話、平板電腦、智慧型手錶、眼鏡等)。

任何類型之配件器件可受控制。配件器件之實例包括門鎖104、車庫門系統106、燈具108、安全性攝影機110及恆溫器112。在一些情況下，控制器102可直接與配件通信；舉例而言，控制器102經展示直接與門鎖104及車庫門系統106通信。在其他情況下，控制器102可經由

中間物來通信。舉例而言，控制器102經展示經由無線網路存取點114與在由存取點114提供之無線網路上的配件108、110、112通信。如上文所指出，在一些實施例中，控制器102可包括基地台，且基地台功能性可整合至存取點114中或整合至待控制之配件中之一者(例如，恆溫器112)中。

可使用各種通信傳輸及傳輸之組合，且不同傳輸可供不同器件使用。通信傳輸之一項實例可為符合藉由Bluetooth SIG, Inc.(http://www.bluetooth.com)界定並頒佈的Bluetooth®通信標準及協定的傳輸；如本文中所使用之術語「藍芽」大體上係指Bluetooth®通信標準及協定，且如本文中所使用之術語「藍芽LE」係指Bluetooth®智慧通信標準及協定。藍芽協定可在有限範圍內支援器件之間的直接點對點通信。通信傳輸之另一實例可為符合藉由Wi-Fi Alliance®(http://www.wi-fi.org)界定並頒佈的Wi-Fi®通信標準及協定的傳輸；如本文中所使用，「Wi-Fi」大體上係指Wi-Fi®標準及協定。Wi-Fi協定可定義具有中心存取點之無線網路，該中心存取點投送該網路上之不同器件之間的通信。該網路可支援包括(例如) TCP及HTTP之標準網際網路協定套件(IP)。應理解，使用藍芽及Wi-Fi作為通信傳輸及協定之實例；亦可使用其他傳輸及協定。此外，儘管展示了無線通信傳輸，但亦可針對配件中之一些或全部提供有線傳輸。舉例而言，燈泡108可藉由有線連接連接至存取點114，且控制器102可藉由以無線方式將訊息發送至存取點114來與燈泡108通信，該存取點可充當橋接器從而經由有線連接將訊息傳遞至燈泡108。有線及無線通信之其他組合亦為可能的。

此外，儘管展示了一個控制器102，但家庭環境100可具有多個控制器器件。舉例而言，生活在家中的每個人可具有可充當用於配件104至112中之一些或全部之控制器的一或多個個人器件(例如，行動電

話、平板電腦、膝上型電腦、可穿戴式器件)。不同控制器器件可經組態以與配件之不同子集通信；例如，可阻止兒童控制器修改恆溫器112上之設置，而准許父母控制器器件修改設置。此等權限可(例如)使用下文所描述之配對技術來組態及控制。

本發明之某些實施例係關於促進藉由控制器(諸如控制器102)進行的與一或多個配件(諸如配件104至112中之任一者或全部)之通信的統一配件協定。該協定可提供將配件模型化為服務之集合的簡單且可延伸之架構，其中每一服務經定義為一組特性，該等特性中之每一者在任何給定時間具有經定義值。該等特性可表示配件之狀態的各種基本態樣。舉例而言，就恆溫器112而言，特性可包括電源(恆溫器是接通或關斷)、藉由恆溫器112測量到的當前溫度及恆溫器112經設定至的目標溫度。使用服務及特性之配件模型之實例描述如下。

該協定可進一步定義可由控制器(例如，控制器102)使用以將命令及控制訊息(請求)發送至配件(例如，恆溫器112)的訊息格式及可由配件(例如，恆溫器112)使用以將回應訊息發送至控制器(例如，控制器102)的訊息格式。命令及控制訊息可允許控制器詢問(例如，讀取)配件特性之當前狀態且在一些執行個體中修改(例如，寫入至)配件特性。舉例而言，修改恆溫器112之電源特性可關斷或接通恆溫器112。因此，不管功能或製造商如何，任何類型之配件可藉由發送適當訊息來控制。該等訊息格式在控制器及配件上可統一；實例描述如下。在一些實施例中，配件可將配件定義記錄提供至控制器。該配件定義記錄可包括關於配件之所有可存取特性的完整資訊。控制器可在判定如何與配件互動中使用該配件定義記錄。舉例而言，控制器可使用來自該配件定義記錄之資訊建構用於操作配件之使用者介面以及建構至配件之請求訊息。

該協定可進一步定義允許配件112 (或其他配件)在狀態改變之情

況下選擇性地通知控制器102的通知機制。實例包括：被動式通知機制，其中控制器102可查詢配件(例如，配件112)以找出任何特性是否已改變；以及主動式、廣告式或基於事件之通知機制，其中配件112 (或其他配件)可在特定特性改變時選擇性地產生至一或多個控制器之訊息及/或廣播廣告。可同時支援多個通知機制，且控制器可選擇待用於特定配件、服務或特性之通知機制。實例描述如下。

在一些實施例中，與給定配件之通信可限於授權控制器。該協定可規定用於在提供高度可信度：使用者希望控制器102能夠控制配件104的情況下建立控制器102與給定配件(例如，門鎖配件104)之間的「配對」的一或多個機制，且已與特定配件建立配對的控制器可被視為針對彼配件授權。配對可(例如)藉由使用短期金鑰及頻帶外共用秘密建立安全密碼編譯架構來建立。用於配件及控制器之長期公用金鑰可在此架構內交換，且配件及控制器可持久地儲存交換的金鑰，藉此建立配對。在配對經建立之後，配件104能夠驗證接收的通信是否來自配對控制器102或另一器件，且配件104可拒絕並非來自配對控制器102之任何通信(反之亦然)。舉例而言，當先前建立配對之配件及控制器重新連接時，該等器件可驗證先前配對(例如，藉由證明每一者擁有另一者之長期公用金鑰)且產生工作階段特定加密金鑰以用於對驗證工作階段內之通信。在一些實施例中，多個控制器可與同一配件建立配對，且配件可在拒絕或忽略來自未配對控制器之通信的同時接受並回應來自其配對控制器中之任一者之通信。配對程序之實例描述如下。

將瞭解，家庭環境100係說明性的且變化及修改係可能的。本發明之實施例可實施於使用者希望使用控制器器件來控制一或多個配件器件的任何環境中，環境包括(但不限於)家庭、汽車或其他車輛、辦公建築物、具有多個建築物之場地(例如，大學或企業場地)等。控制器可為用以控制一或多個其他器件(配件)的任何器件，且配件可為允

許其操作中之一些或全部由控制器來控制的任何器件。控制器102可實施或包括本文中描述為實施於或包括於控制器中之特徵之任一者或全部，且諸如配件104至112之配件可實施或包括本文中描述為實施於或包括於配件中之特徵之任一者或全部。

在一些實施例中，控制器102可從遠端位置(例如，世界上的任何地方)與配件(例如，配件108)通信。舉例而言，儘管位於遠端環境中，但控制器102可經由廣域網路(例如，網際網路)與具有將訊息轉送至配件108 (例如，藉由與位於環境100中之存取點114通信，該存取點可區域地與配件108通信)之能力的伺服器通信。控制器102與配件108之間的通信之內容伺服器可不瞭解；例如，控制器102及配件108可建立訊息經加密的安全通信工作階段(例如，如本文中所描述之對驗證工作階段)，且伺服器可僅傳遞加密資料而保持對加密資料之內容不可知。因此，配件可區域地(例如，藉由能夠建立至配件之直接通信路徑的控制器)或遠端地(例如，藉由經由轉送伺服器或其類似者間接地通信的控制器)操作。

實例配件模型

在一些實施例中，統一配件協定可提供用於將任何配件模型化為「服務」之集合的統一架構及語法。如本文中所使用之「服務」可指用於實現配件器件(或其某一部分)之特徵、功能或操作的資料及相關聯行為之集合。每一服務可模型化為「特性」之集合，特性中之每一者表示配件之基本資料元素或行為(亦被稱作配件狀態之元素)。如下所述，配件可藉由將配件定義記錄提供至控制器而向控制器描述其本身，配件定義記錄可為定義配件之服務及特性的結構化資料物件。結構化資料物件可以各種特定格式來表示，例如使用JSON (JavaScript物件記數法)、藍芽LE一般屬性設定檔(GATT)或用於表示及傳達結構化資料之其他技術及格式。如下所述，控制器可使用配件定義記錄來判

定如何控制配件。

舉例而言，圖1之恆溫器配件112可包括執行調節區域(例如，房間或建築物或建築物之部分)之溫度以使溫度維持接近某一目標的組件。出於模型化配件112之目的，溫度調節可經被識別為「恆溫器」服務。恆溫器服務之特性可包括：恆溫器是接通或關斷；當前設定之目標溫度；當前量測溫度；及藉由恆溫器調節之系統當前是處於加熱模式(能夠接通加熱器以朝較高目標溫度驅使量測溫度)中或處於冷卻模式(能夠接通冷卻器以朝較低目標溫度驅使量測溫度)中。在較複雜實例中，恆溫器可為可程式化的，例如視當日時間及/或星期幾而選擇不同目標溫度，且在此等情況下，特性可包括諸如一組時間範圍及針對每一時間範圍之相關聯目標溫度的程式化特徵。

在一些情況下，配件可提供多個服務。舉例而言，車庫門配件106可使用可開啟及關閉門且亦具有可控制(例如)照明車庫之內部之燈的自動車庫開門器來實施。因此，車庫門配件106之定義可包括實現開啟及關閉車庫門之功能的「開門器」服務及實現接通或關斷燈之(不同)功能的「燈泡」服務。開門器服務之特性可包括門之當前狀態(例如，開啟、關閉、在開啟中、在關閉中)、門是否被鎖定(例如，以防止開門器開啟門)及門是否受阻礙(例如，開門器系統中之阻礙感測器是否已偵測到防止門關閉之阻礙)。燈泡服務之特性可包括燈是接通或關斷及當前亮度位準(在燈具有可變亮度控制之情況下)。

應理解，任何配件可模型化為服務之集合，且同一環境中之不同配件可包括相同或類似服務之一些或全部。舉例而言，諸如家庭環境100之環境可具有在不同位置之多個燈泡(例如，每一房間中之燈)、多個門鎖(例如，每一外部門上之鎖、內部門上之鎖)等。在一些實施例中，統一配件協定藉由以下處理來明確地允許此重疊：定義名稱空間以使得每一配件及服務可唯一地經識別，從而允許不同配件上之相同

服務之執行個體或同一配件上之類似服務之多個執行個體容易區分。

在一些實施例中，統一配件協定可定義一組「核心」特性，該等特性可包括預期將頻繁使用及/或將跨不同配件類型之範圍存在之特性。該組特性可變得可延伸；例如，配件製造商可經允許而定義製造商特定特性(在本文中亦被稱作「延伸」特性)。因此，配件不限於該等核心特性。然而，在適用情況下使用核心特性可有助於系統設計及操作。舉例而言，控制器之系統軟體可包括定義該等核心特性之性質的程式碼，且僅使用核心特性之配件可藉由識別其特性及該等特性之當前值來向控制器描述其本身。

圖2A至圖2D展示根據本發明之一實施例的可定義之標準特性201至229之一些實例。每一特性201至229可具有表示提供特性之給定執行個體所屬之服務之配件(或配件之部分)之狀態之某一態樣的值(圖2A至圖2D中未示)。在此實例中，每一特性201至229經描述為具有類型、權限及格式。視格式而定，亦包括額外資訊(例如，有效值之最小值、最大值、步長、單位或列舉清單)。

特性之「類型」可為指派給彼特性之唯一名稱或識別符(例如，字元字串)。在此實例中，反相網域名稱約定用來指派類型，此可有助於配件製造商對延伸特性之定義。舉例而言，包括圖2A至圖2D中所示之特性定義之統一配件協定之發佈者係稱為「proto.com」之網際網路網域的擁有者，則所有核心特性類型可以字串「com.proto.ch.」開始，繼之以特性特定名稱，諸如「on」、「brightness」等。可使用其他命名約定。

在一些實施例中，除名稱類型之外或替代名稱類型，每一特性亦可經之品唯一數值識別符(圖2A至圖2D中未示)。舉例而言，唯一數值識別符可為由符合網際網路工程任務小組(Internet Engineering Task Force，IETF) RFC 4122之36個十六進位數字組成的UUID (本文中所參

考之所有「IETF RFC」文件可經由http://ietf.org/rfc.html存取)。統一配件協定可定義用於所有核心特性之共同「基本」UUID (例如，最後28個十六進位數字)且將唯一「短」UUID (例如，前8個十六進位數字)指派給每一特性；可使用任何編號方案。UUID之使用(特定言之與用於截短UUID之約定組合使用)可允許控制器或配件使用相對於使用字元字串相對少量的傳輸資料來規定感興趣之特性。舉例而言，在一些實施例中，截短約定可將36數字UUID減少至僅兩個或三個十六進位數字。

特性之「權限」可指示允許控制器與特性互動之方式(例如，詢問或修改特性)。在一些實施例中，權限可表示為字串之一陣列，其中每一字串對應於特定互動方式。若字串存在，則其對應互動方式經准許；若字串不存在，則互動未經准許。可定義之權限字串之一些實例展示於表1中。

權限字串	描述
「配對讀取」(「PR」)	配對控制器可讀取特性(例如，使用如下所述之HTTP GET請求)
「配對寫入」(「PW」)	配對控制器可寫入至特性(例如，使用如下所述之HTTP PUT請求)
未配對讀取(「UR」)	未配對控制器可讀取特性(例如，使用如下所述之HTTP GET請求)
未配對寫入(「UW」)	未配對控制器可寫入至特性(例如，使用如下所述之HTTP PUT請求)
管理員讀取(「AR」)	具有管理員權限(參見下文)之配對控制器可讀取特性
管理員寫入(「AW」)	具有管理員權限(參見下文)之配對控制器可寫入至特性

表1

在一些實施例中，對特性之讀取權限係在需要控制器找出配件狀態之對應態樣時授予，且寫入權限係在需要控制器能夠激起配件狀態之對應態樣之改變時授予。因此，例如，與配件能夠直接控制的條件相關之特性(例如，目標溫度特性210)可具有讀取及寫入權限，而與配件無法直接控制的條件相關之特性(例如，當前溫度特性209)可僅具有讀取權限。

每一特性201至229可具有反應配件狀態之對應屬性或態樣之

值。圖2A至圖2D規定用於每一特性201至229之值的格式。如本文中所使用，<boolean>格式指示特性採用真及假之值；<int>格式指示特性採用帶正負號之整數值；<float>指示特性採用帶正負號的浮點值)；<string>指示特性採用(例如)使用UTF-8編碼之字元字串值)；<date>指示特性採用日期值(例如，ISO 8601格式之UTF-8日期字串)；且<data>指示特性可用以儲存資料斑點(亦即，協定可關於含量不可知的資料區塊)。<enum>格式指示特性採用表示特定條件之值之經定義集合中之一者，且可能值經列出為彼特性之「有效值」。在一些實施例中，列舉值格式可藉由將不同整數指派給每一有效值來實施。<tlv>格式指示緊縮的類型-長度-值資料類型，其中第一位元組指示類型，第二位元組指示長度(N個位元組)，且剩餘N個位元組含有值。在一些實施例中，可使用其他格式；實例包括在此表示為<object>之資料物件格式(資料物件可使用金鑰-值格式進一步定義)及陣列格式(其可為其他格式中之任一者之值的固定長度或可變長度陣列)。在一些實施例中，統一配件協定可規定用於特性之允許格式的封閉宇宙，以使得所有特性(包括延伸特性)之值係以允許格式中之一者來表示。

特性之值可指示配件狀態之屬性或態樣。值可在適於所表示之資訊之格式中規定。在一些情況下，特性定義可規定值之範圍。舉例而言，「最大」(或「最大值」)可表示上限，「最小」(或「最小值」)可表示下限，且「步進」(或「步長」)可表示用於採用離散值之特性的最小增量。「單位」可經定義以指示藉以量測值之特定單位；此資訊可有助於控制器對值之解譯。

舉例而言，「接通」特性201可在配件通電之情況下具有布林值「真」且在配件斷電之情況下具有布林值「假」。此特性可(例如)結合燈泡、燈開關或具有接通及關斷狀態(且可在處於關斷狀態下與控制器通信)的其他配件來使用。作為另一實例，「使用中插座」特性202可供

具有電源插座之配件使用，且布林值可指示電源插頭是否連接至電源插座。在此情況下，假定配件無法實體上插入或移除電源插頭，且因此，該特性具有唯讀權限。

作為使用配件模型之配件控制之簡單實例，假設電源插座配件具有可開始或停止電力至插座之流動的控制開關。電源插座配件可模型化為具有「接通」特性201及「使用中插座」特性202之服務。控制器可讀取「使用中插座」特性202以判定電源插頭是否連接至插座，接著寫入至「接通」特性201以視電源插頭是否已連接而啟用或停用至插座之電力。

亮度特性203、色調特性204及飽和度特性205可(例如)結合提供光源之配件來使用。亮度特性203可具有在0至100範圍內之整數值(如圖2A中之「最小，最大，步進」欄位中所指示)以將亮度位準指示為配件所支援之最大亮度的百分比。如同以百分比單位所規定之所有特性，應理解，不需要配件精確地支援器件狀態之對應態樣(在此情況下，亮度)的一百個相異設定；實情為，配件可將給定百分比值映射至可用之設定。色調特性204可具有在0度至360度範圍中的規定色調之浮點值；度之值至實體色調之轉譯可遵循標準色彩模型化作法。飽和度特性205可具有在0至100範圍中之浮點值以將所要色彩飽和定義為最大值之百分比。控制器可讀取此等特性以判定當前設定及寫入至該等特性以改變設定。

可使用音訊回饋特性206，其中配件具有回應於在配件處偵測到之使用者輸入或其他事件的選用之音訊回饋(例如，嗶嗶聲)。可藉由將布林值寫入至此特性來啟用或停用音訊回饋。輸出音量特性207可用以讀取或設定產生聲音之配件上之輸出音量；值可指示配件能夠產生之最大音量之百分比。

可使用記錄檔特性208，其中配件維持活動之具時間戳記之記錄

檔。記錄檔之結構可由配件製造商定義，或針對特定類型之配件由統一配件協定之發佈者規定。在此實例中，控制器可藉由讀取特性208來獲得配件之記錄檔，但不寫入至特性208，此係因為控制器之作用並非更新記錄檔。應理解，作為配件之例行操作之部分，配件可將控制器互動之記錄新增至記錄檔中，且控制器可將任何此等記錄與記錄檔之其餘部分一起接收。

圖2B展示關於恆溫器配件之特性之實例，恆溫器配件可包括可監控環境(例如，房子或房間)內之當前溫度且控制加熱及/或冷卻系統以朝目標溫度調整溫度的任何配件。當前溫度特性209可由控制器讀取以判定藉由配件量測之當前溫度。目標溫度特性210可由控制器讀取以判定恆溫器配件之目標溫度設定且亦可由控制器寫入以改變目標溫度設定。在此實例中，溫度係以攝氏度規定；其他標度(例如，華式溫度、開爾文)可取代。不管協定規定了何種標度，控制器或配件始終可轉換至不同標度以供內部使用及/或向使用者顯示。舉例而言，溫度單位特性211可由控制器讀取或寫入以指示當向使用者顯示溫度時配件應使用什麼單位。此外，儘管溫度特性209及210規定允許值之範圍，但可使用其他範圍，或範圍可保持未規定。

一些恆溫器可能可操作以控制加熱及冷卻兩者。因此，當前熱/冷狀態特性212可經讀取以判定恆溫器當前係加熱(主動地朝目標溫度加熱)、冷卻(主動地朝目標溫度冷卻)或關斷。由於控制器未決定何時加熱或冷卻，故不提供寫入權限。恆溫器之操作模式可藉由寫入至目標熱/冷模式特性213來控制。在此實例中，模式特性213之有效值包括加熱模式(其中恆溫器朝目標溫度使環境升溫)、冷卻模式(其中恆溫器朝目標溫度使環境變冷)、自動模式(其中恆溫器可視環境條件而動態地選擇加熱模式或冷卻模式)及關斷。當選擇自動模式時，可能需要規定用於將恆溫器切換成加熱或冷卻模式之溫度臨限值。舉例而言，冷

卻臨限溫度特性214可由控制器寫入以設定冷卻臨限溫度，以使得恆溫器在當前溫度超過冷卻臨限溫度的情況下將啟用冷卻模式，且加熱臨限溫度特性215可由控制器寫入以設定加熱臨限溫度，以使得恆溫器在當前溫度降低到加熱臨限溫度以下的情況下將啟用加熱模式。如圖2B中所示，冷卻溫度臨限值特性214及加熱溫度臨限值特性215可以而不必具有彼此不同及不同於目標溫度特性210之上限及下限。

圖2C展示關於開門器(例如車庫開門器或開啟及/或關閉門之其他自動化機構)及門鎖之特性之實例。當前門狀態特性216可由控制器讀取以判定門當前是開啟、關閉、在開啟或關閉中或停止(例如，未完全開啟或未完全關閉，但不移動)。目標門狀態特性217可由控制器寫入以指示門是否應開啟或關閉。若控制器將不匹配當前門狀態特性216之值寫入至目標門狀態特性217，則配件可藉由致動開門器機構來回應以便改變當前狀態以匹配目標。舉例而言，若門開啟(當前門狀態特性216具有「開啟」值)且控制器將值「關閉」寫入至目標門狀態特性217，則配件可致動開門器以關閉門。在致動開門器後，配件隨即可將當前門狀態特性216更新為「關閉中」，且一旦門完全關閉，配件可進一步將當前門狀態特性216更新為匹配目標狀態之「關閉」。控制器可藉由讀取目標門狀態特性217來瞭解門在任何時間之當前狀態。

在一些實施例中，開門器配件可將額外資訊提供至控制器。舉例而言，運動偵測特性218可用以指示配件是否已偵測到門周圍之運動(例如，敲門)。障礙物偵測特性219可用以指示配件是否已偵測到可防止門移動之障礙物。控制器可藉由讀取此等特性來獲得此資訊。在一些實施例中，配件可在偵測到此等特性之改變的情況下(例如，在門變得受阻礙的情況下或在偵測到運動的情況下)將通知發送至控制器。

鎖定門可與開啟或關閉門分開地對待。舉例而言，「鎖機構」配件可針對控制死栓(deadbolt)、磁鎖或可參與防止門被開啟之任何其他

實體機構之任何器件而實施。鎖機構當前狀態特性220可由控制器讀取以判定鎖機構當前未扣緊(解除鎖定)、已扣緊(鎖定)、已卡住(不能鎖定或解除鎖定)或未知。鎖機構目標狀態特性221可由控制器寫入以請求門之鎖定或解除鎖定。鎖機構最後動作特性222可由控制器讀取以判定對鎖執行之最後已知動作。可支援變化之細節位準。舉例而言，在一項實施例中，有效值可包括：(1)使用實體移動自內部扣緊(例如，使用者實體地移動死栓槓桿)；(2)使用實體移動自外部扣緊；(3)使用小鍵盤扣緊；(4)遠端扣緊(例如，基於來自控制器之請求)；(5)基於逾時條件之扣緊；(6)使用實體移動自內部未扣緊；(7)使用實體移動自外部未扣緊；(8)使用小鍵盤未扣緊；及(9)遠端未扣緊。亦可視所要的資訊粒度來定義有效值之其他組合。

額外特性可與管理鎖機構相關聯。舉例而言，鎖管理自動逾時特性223可用以設定逾時週期，配件在該逾時週期之後自動地重新鎖定鎖。逾時週期可(例如)在鎖變得解除鎖定時開始。在一些實施例中，逾時週期之持續時間可為該特性之數值(例如，以秒計)，且值0可用以指示不存在逾時期間(亦即，鎖可保持解除鎖定，直至進行特定動作以鎖定該鎖)。鎖管理控制點特性224可用以調用與鎖相關之特定功能，例如藉由將值寫入至識別該功能之特性224。可調用之功能之實例包括讀取鎖定活動之記錄檔(其可導致配件傳回用於記錄檔特性208之值)、清除記錄檔、設定鎖上之時間等。作為另一實例，供應商可能想要允許使用者設定關於鎖之使用的各種政策，諸如僅允許在一天中的特定時間之間遠端開啟鎖。在一些實施例中，控制器可藉由寫入至鎖管理控制點特性224而將此等政策提供至鎖配件。在一些實施例中，統一配件協定並不規定寫入至鎖管理控制點特性224之資料之內容，而可能規定資料應以TLV格式或其他格式提供，以使得資料可使用統一配件協定可靠地自控制器傳達至配件，且資料可由配件以供應商特定方

式解譯。

圖2D展示核心特性之額外實例。旋轉方向特性225可用以控制風扇(或具有旋轉元件之任何其他配件)在順時針方向或逆時針方向上旋轉。旋轉速度特性226可用以控制風扇(或其他旋轉元件)之旋轉速度，其中速度經指示為最大速度之百分比。

名稱特性227可用以將人可讀名稱指派給配件或服務。名稱可表示為字元字串(例如，以UTF-8格式)。

僅管理員存取特性228可用以將對配件或服務之存取限於已建立以作為配件之管理員(亦即，具有管理員權限)之控制器。用於將控制器建立為管理員之技術之實例描述如下。在一些實施例中，僅已建立以作為配件之管理員之控制器可寫入至特性228。

版本特性229可用以提供關於配件或服務之版本資訊。

應理解，圖2A至圖2D中所示之該等特性係作為實例而提供。可定義任何數目之核心特性。舉例而言，可定義關於室內環境之其他可控制態樣之特性(例如，相對濕度)。被定義為統一配件協定之部分的特性之特定組合可視需要變化。在一些實施例中，未被定義為核心特性之特性可由第三方(例如，配件製造商)使用此處所描述之技術定義為延伸特性。

在一些實施例中，該組特性係可延伸的。配件可藉由提供特性之一組性質(或描述符)來定義新特性(亦被稱作「延伸」特性)。圖2E展示根據本發明之一實施例的特性之一組可定義性質。對於核心特性，此等可由協定來定義(例如，如圖2A至圖2D中所示)。在一些實施例中，配件可重新定義核心特性之性質中之一些且藉此覆寫針對彼特性所定義之預設性質。在一些實施例中，延伸特性可藉由在配件定義記錄內提供此等性質來定義。實例描述如下。

「類型」230可為(例如)使用如上所述之反向網域名稱約定的識別

特性之類型的字串。在一些實施例中，除字串之外或替代字串，數字識別符(例如，如上所述之UUID)亦可用作類型識別符。

「權限」231可為用於控制器的識別所准許之存取類型的字串之陣列(例如，上文之表1中之權限之任一者或全部)。

「通知模式」232可為用以指示應如何通知控制器特性之改變的字串之陣列。在一些實施例中，控制器可寫入至此性質以訂用特定通知模式。表2列出可支援之通知模式之一些實例。每一此等通知模式之操作描述如下。

通知模式	描述
被動	配件藉由更新其內部狀態計數器(例如，如下所述之「被動」通知)來指示特性之改變。
廣告	配件藉由經由器件探索服務(例如，如下所述之「廣告」通知)廣告經更新資訊來指示此特性之改變。
事件	配件將在特性改變時將通知發送至已連接且已訂用之控制器(例如，使用如下所述之未經請求的HTTP EVENT回應)
主動式連接	配件藉由起始至已訂用控制器之連接(例如，如下所述之「主動式」通知)來指示此特性之改變

表2

在一些實施例中，對於所有特性，被動式通知藉由所有配件來支援而不管由控制器進行之任何訂用；可訂用由控制器進行之訂用請求來選擇性地啟用其他所支援之通知模式。在一些實施例中，具有「配對讀取」權限之所有核心特性亦至少支援「事件」通知模式。

「格式」233可為識別用於特性之值之格式(例如，布林值、字串、整數、浮點數、TLV等)的字串。在一些實施例中，協定可定義一組已辨識格式，且格式233可選自該經定義集合。

「值」234可為特性之當前值。

「最小值」235及「最大值」236可用以設定特性之下限及上限，若極限係所要的。類似地，「步長」237可用以規定用於改變特性之值的最小增量，若最小增量係所要的。在最小值、最大值及步進值經規

定的情況下，期待配件辨識並回應在範圍內之任何有效值。然而，如上文所指出，此並不暗示配件上可用之設定之數目必須等於有效值之數目。舉例而言，若燈泡配件具有亮度特性203，則該配件可控制亮度(例如，藉由調節供應至燈泡之電流)以使得亮度在該亮度特性經設定成100時最大且在該亮度特性經設定成0時為零。吾人預期(雖然未必絕對需要)亮度特性經定義之燈泡可具有在零與最大亮度之間的至少一個中間等級；若該配件支援大於或小於100個中間等級，則該配件可定義亮度特性值至其亮度等級之映射。

在一些實施例中，可支援列舉值格式，且「有效值」性質238可用以列出格式233經規定為「列舉」之情況下的有效值。

「單位」性質239可指示用於特性之單位(例如，百分比、特定溫度標度等)。在一些實施例中，協定可規定較佳單位系統，且用於給定特性之單位性質239可在此系統內選擇。

「使用者描述符」性質240可以人可讀方式提供描述特性或其功能之字串。舉例而言，用於當前熱/冷狀態特性212之使用者描述符可表達「指示加熱/冷卻系統當前加熱、冷卻或關斷」。

「擁有者」性質241可識別定義或重新定義特性之組織單位。在一些實施例中，此性質可幫助使用者或開發者理解各種特性之定義之來源。

可針對特性定義圖2E中之性質(及視情況之其他性質)中之任一者或全部。如上文所指出，針對核心特性，協定可規定預設定義，且在使用核心特性之情況下，未必將特性之所有性質包括於(例如，如下所述之)配件定義記錄中。在一些實施例中，配件可藉由將待重新定義之彼等性質包括於配件定義記錄中來重新定義核心特性。延伸特性可藉由將其定義性質全部包括於配件定義記錄中來定義。

在一些實施例中，特性之性質可由控制器來讀取且用以判定如何

顯現用於控制特性及/或呈現當前值之圖形使用者介面。舉例而言，就表示為百分比之亮度特性203 (圖2A)或任何其他特性而言，控制器可將控制件顯現為0至100%之滑桿且以1%之步進移動該滑桿。在表示為布林值之接通特性201 (圖2A)或任何其他特性之情況下，控制器可顯現接通/關斷開關。在溫度相關特性之情況下，控制器可基於具有「攝氏」(或其他溫度單位)之特性而顯現溫度計量錶或類似者，或控制器可僅顯示數字值。在針對特性定義使用者描述符240之情況下，控制器可結合用於該特性之使用者介面控制元件顯現文字，且此可有助於使用者理解控制元件。因此，配件可自我描述，以使得給定配件定義記錄，控制器可動態地產生用於控制任何配件而不用針對彼配件特定地程式設計之介面。

將瞭解，圖2A至圖2D中所示之特性及圖2E中所示之性質(或描述符)為說明性的且變化及修改係可能的。統一配件協定可定義任何數目及組合之特性，且特性可使用來自所示之性質及值的不同組之性質及值來定義。舉例而言，最大字串長度性質可用以規定字串之長度之上限，且最大資料長度性質可用以規定含資料特性之上限(例如，用於資料物件或資料斑點)。

此外，如所指出，協定可允許配件製造商定義用於其配件的定製或製造商特定之延伸特性。以實例說明，假設製造商(其擁有網際網路網域「discoball.com」)產生包括可受控制而在不同方向上且以不同速度旋轉之鏡面球的迪斯可球(disco ball)系統，及可朝該球之表面定向之光源。該光源可使用來自圖2A至圖2D之核心特性(例如，「接通」特性201及亮度特性203)來模型化及控制。製造商可能想要定義用於光源及/或鏡面球之進一步控制的延伸特性。圖2F展示用於此情形之延伸特性之實例。

閃光特性242為用於控制閃光效應之實例特性。當為真時，燈係

以閃光模式操作；當為假時，燈係以穩定模式操作。

方向特性243為用於控制鏡面球之旋轉方向之實例特性。該球可不旋轉(停止)、順時針旋轉或逆時針旋轉。在核心特性包括旋轉方向特性225之實施例中，製造商可選擇使用該核心特性抑或定義延伸特性。

速度特性244為用於控制鏡面球之旋轉速度之實例特性。此實例中之速度具有兩個設定(用於緩慢旋轉之0，用於快速旋轉之1)。在核心特性包括旋轉速度特性226之實施例中，製造商可選擇使用該核心特性抑或定義延伸特性。

如上文所指出，統一配件協定可將配件模型化為一或多個服務，其中每一服務經模型化為特性之集合。因此，服務可藉由識別其構成特性來定義，構成特性可包括核心特性及/或延伸特性之任何組合。在一些實施例中，統一配件協定可定義一組核心服務，該等核心服務可包括預期將頻繁使用及/或將跨配件類型之範圍有用的服務。該組服務可變得可延伸；例如，配件製造商可經允許將製造商特定特性新增至核心服務或定義額外「延伸」服務。然而，在適用情況下使用核心服務可藉由允許系統設計者充分利用預定義之服務及特性而有助於系統設計及操作。

圖2G至圖2H展示根據本發明之一實施例的可定義之核心服務251至258之實例。每一服務251至258可經指派「類型」，其可為識別服務之唯一名稱。在此實例中，類似於特性類型，使用反向網域名稱約定來定義類型以便有助於配件製造商對新服務之定義。因此，圖2G至圖2H中之核心服務類型以「com.proto.svc」(其中「svc」可用以指示類型係針對服務而非特性)開始。

在一些實施例中，除類型之外或替代類型，每一服務可經指派唯一數值服務識別符(圖2G至圖2H中未示)。舉例而言，如IETF RFC 4122

所定義之UUID (由36個十六進位數字組成之識別符)可指派給每一服務。統一配件協定可針對所有服務定義共同「基本」UUID (例如，最後28個十六進位數字) (視需要，其可相同於或不同於指派給所有特性之基本UUID)且將唯一「短」UUID (例如，前8個十六進位數字)指派給每一服務；可使用任何編號方案。UUID之使用(特定言之與用於基於「短」UUID截短UUID之約定組合使用)可允許控制器或配件使用相對於使用字元字串相對少量的傳輸資料來規定感興趣之服務。

每一服務251至258表示配件可實施之功能及藉由參考一組必需特性(圖2G至圖2H中「必需特性」)及一組選用之特性(圖2G至圖2H中之「選用之特性」)來定義。在本文中之實例中，每一服務具有至少一個選用之特性(名稱)；在其他實施例中，該組選用之特性對於至少一些服務可為空。

在此實例中，針對給定核心服務，在期待自稱提供彼核心服務之任何相容配件辨識「必要」特性且使用其來控制配件之執行個體中，將該特性經定義為「必要」的。舉例而言，燈泡服務251包括必需特性「com.proto.ch.on」(圖2A之特性201)；此意謂若配件自稱提供「com.proto.svc.lightbulb」服務，則預期配件藉由接通(真)或關斷(假)燈來回應對特性「com.proto.on」之寫入請求且藉由傳回指示燈接通(真)抑或關斷(假)之布林值來回應對特性「com.proto.on」之讀取請求。在一些實施例中，配件可僅回應來自授權(或配對)控制器之請求；授權描述如下。

在此實例中，在不需要配件將特性包括於其服務定義但可包括該特性之執行個體中，針對給定核心服務，將該特性定義為「選用」。舉例而言，燈泡服務251包括選用之特性「com.proto.ch.brightness」(圖2A之特性203)。僅具有接通或關斷設定之燈泡配件(諸如許多習知螢光燈具)可不具有用於亮度控制之任何用途，且此配件不必支援

「com.proto.ch.brightness」特性。具有亮度控制之燈泡配件(例如，可調光燈)可包括「com.proto.ch.brightness」特性以允許控制器操作調光器。類似地，色調及飽和度可為用於燈泡服務251之選用之特性。

其他服務252至258可類似地定義，從而規定必需特性及選用之特性之組合。該等特性係按類型在圖2G至圖2H中識別且可如如上文所述的圖2A至圖2D中所示地定義。應注意，特性在一個核心服務中可為必要的且在另一核心服務中可為選用的。舉例而言，鎖機構當前狀態及目標狀態對於車庫開門器服務253係選用之特性，但對於鎖機構服務254係必需特性。

應理解，圖2G至圖2H中之核心服務實例係出於說明目的而提供。可定義任何數目之核心服務，且可視需要改變與給定核心服務相關聯之特定必需特性及/或選用之特性。此外，在延伸特性得到支援之實施例中，製造商可經允許藉由新增延伸特性來擴增核心服務。另外或實情為，在一些實施例中，製造商可使用核心特性及/或延伸特性之任何組合來定義延伸服務。

配件本身可使用「配件資訊」服務來描述，該服務可為由協定規定之核心服務。在一些實施例中，協定可規定所有協定相容配件將配件資訊服務之執行個體包括於其配件定義記錄中。圖2I展示根據本發明之一實施例的配件資訊服務261之定義(格式與圖2G至圖2H相同)，且圖2J展示配件資訊服務261之額外特性271至276之定義(格式與圖2A至圖2D相同)。

身分識別特性271可由控制器寫入以調用配件之自識別常式。此自識別常式可包括配件起始使用者可觀擦動作。舉例而言，配件可使光閃爍、發出聲音、振動、移動可移動組件(例如，開啟及關閉門)、顯示特定訊息(例如，「Here I am」)，或執行使用者可觀察之某一其他實體動作。自控制器調用配件之自識別常式可有用，例如，結合確認

控制器正與使用者想要控制之配件通信。在一些實施例中，控制器可藉由將「真」寫入至身分識別特性271來調用配件之自識別常式。

製造商名稱特性272、模型名稱特性273及序號特性274可由控制器讀取以獲得關於配件之識別資訊。在一些實施例中，該等值可為人可讀字元字串。

韌體修訂特性275、硬體修訂特性276及/或軟體修訂特性277可由控制器讀取以獲得關於配件之代資訊，代資訊可由控制器用以判定如何與配件互動。在一些實施例中，修訂資訊可以標準格式(例如，<x>.<y>.<z>;<w>)來表示，其中<x>為主要版本數目，<y>為次要版本數目，<z>為修訂版本數目，且<w>可含有額外資訊。

將瞭解，特性及服務的前述實例係說明性的且變化及修改係可能的。統一配件協定可規定任何數目及組合之核心特性及核心服務，且給定服務可用來自所示之彼等核心特性及核心服務的不同組特性來定義。如所指出，核心服務可經擴增具有延伸特性及/或延伸服務(例如，如配件製造商如所定義)，從而將大程度之靈活性及適應性提供至統一通信及控制架構內之變化需要。

在一些實施例中，核心服務定義之不同版本可共存。為了促進不同代之產品之間的相容性，可將核心服務定義之稍後版本限於新增新選用之特性；維持一致組之必需特性可有助於互操作性。

如上文所指出，在一些實施例中，配件製造商可將延伸特性新增至服務。舉例而言，若配件為具有閃光選項之燈，則製造商可將閃光特性(例如，圖2F之閃光特性242)新增至核心燈泡服務251。製造商亦可定義延伸服務。舉例而言，就上文所述之迪斯可球而言，製造商可定義延伸服務「com.discoball.svc.discoball」以控制鏡面球及燈。此服務可包括以下特性：

com.proto.ch.on (特性201，圖2A)；

com.proto.ch.brightness (特性203，圖2A)；

com.proto.ch.hue (特性204，圖2A)；

com.discoball.ch.strobe-on (特性242，圖2F)；

com.discoball.ch.rotate-direction (特性243，圖2F)；及

com.discoball.ch.rotate-speed (特性244，圖2F)。

將配件表示為具有特性之服務之集合的配件模型可作為配件物件傳達至控制器。配件物件可使用用於表示結構化資料物件(例如，使用巢套金鑰值對)之JSON或其他記數法來傳達。圖3A至圖3C展示根據本發明之一實施例的配件物件300之實例。配件物件300係使用JSON表示；其他表示可取代。具有附著燈之車庫開門器係用於說明目的，儘管配件模型不限於任何特定配件。

配件物件300可表示為服務執行個體310、320、330之陣列，該等服務執行個體中之每一者可表示為特性執行個體之陣列。因此，服務執行個體310可包括特性執行個體311至315；服務執行個體320可包括特性執行個體321至325；且服務執行個體330可包括特性執行個體331至332。在此實例中，服務執行個體310為圖2I之配件資訊服務261之執行個體，服務執行個體320為圖2G之車庫開門器服務253之執行個體，且服務執行個體330為圖2G之燈泡服務251之執行個體。(術語「服務」及「服務執行個體」在本文中可互換使用，術語「特性」及「特性執行個體」亦可如此)。

每一服務執行個體310、320、330及每一特性執行個體311至315、321至325、331至332可包括服務或特性類型，從而識別哪個服務或特性係執行個體。在此實例中，使用類型字串。在一些實施例中，可使用UUID或截短UUID，從而允許服務及特性類型以數字方式而非用字串來識別。此可減小配件物件300之大小。每一服務執行個體及每一特性執行個體亦經指派執行個體識別符。在此實例中，配件之每一服務

執行個體及特性執行個體具有唯一執行個體識別符，其可連續地或以任何其他所要方式來指派。此可允許配件內之任何服務執行個體或特性執行個體藉由參考其執行個體識別符來定址，如下所述。在一些實施例中，可實施不同唯一性規則。舉例而言，每一服務執行個體可具有唯一服務執行個體識別符，且每一特性執行個體可具有在服務執行個體內之特性執行個體中唯一的特性執行個體識別符。此可允許服務執行個體藉由參考其執行個體識別符來定址且允許特性執行個體藉由其執行個體識別符與其所屬之服務執行個體之執行個體識別符一起來定址。可以使用其他方案。

在圖3A中，服務執行個體310為圖2I之配件資訊服務261之執行個體。在一些實施例中，協定可規定每一配件具有配件資訊服務之單一執行個體且配件資訊服務執行個體具有執行個體ID 1；可視需要規定不同規則。特性執行個體311至315可為服務261之必需特性之執行個體。在圖3B中，服務執行個體320可為圖2G之車庫開門器服務253之執行個體。特性執行個體321至323可為服務253之必需特性之執行個體。在此實例中，服務執行個體320亦包括選用之特性執行個體324、325以控制車庫開門器之鎖機構。在圖3C中，服務執行個體320可為圖2G之燈泡服務251之執行個體。特性執行個體331可為服務251之必需特性之執行個體，且特性執行個體332可為選用之亮度特性之執行個體。

對於除配件資訊服務外之服務，同一服務之多個執行個體可共存於配件物件內。舉例而言，操作多個獨立可控制燈泡之配件可具有用於每一燈泡之燈泡服務251之不同執行個體，從而允許每一燈泡之狀態獨立地受控制。

配件物件300亦可提供具有讀取權限之每一特性執行個體之當前值。舉例而言，車庫門當前封閉(當前門狀態特性執行個體321具有值2，其映射至「關閉」)，且燈關斷(接通特性執行個體331具有值假)。

識別特性執行個體315具有空值，此係因為對此特性之存取係唯寫的。

針對每一特性執行個體之權限可指示為「perms」字串之陣列。在此實例中，該陣列可包括「Events」字串以指示配件支援關於此特性之事件通知。舉例而言，如下所述，控制器可訂用權限包括「Events」字串之任何特性執行個體之事件通知。事件通知機制之實例描述如下。

圖3C展示部分地重新定義核心特性之配件之實例。亮度特性執行個體332經重新定義(相對於核心特性203)以藉由規定新的最小值、最大值及步進值來減小亮度增量之數目。重新定義僅應用於執行個體332且可不影響配件物件300內所定義之任何其他服務執行個體或任何其他配件(給定控制器與之相互操作)的亮度特性。

應瞭解，圖3A至圖3C之配件物件係說明性的且變化及修改係可能的。配件可包括任何數目及組合之服務執行個體，且配件內之服務執行個體可包括任何數目及組合之特性執行個體。可在配件物件內規定給定特性執行個體之更多或更少性質；例如，可規定圖2E中所示之各種性質中之任一者或全部。在配件包括多個服務執行個體之情況下，該等服務執行個體中之一者(例如，配件物件中所列出的除配件資訊服務執行個體外的第一服務執行個體)可指定為主服務。

另外，儘管圖3A至圖3C展示使用JSON之實施，但任何特定記數法或語法之使用並非必需的。舉例而言，可利用本發明之熟悉此項技術者應理解，可藉由充分利用藍芽LE一般屬性設定檔(Generic Attribute Profile，GATT)來表示配件服務及特性，藉此促進控制器與配件之間使用藍芽LE的通信。舉例而言，服務及特性可藉由UUID來識別，以使得每一服務及每一特性具有唯一UUID。

此外，在一些實施例中，控制器可與單一端點(亦被稱作配件伺服器)通信以與一或多個配件互動。為了支援此情形，配件定義記錄可包括一或多個配件物件之陣列，其中每一配件物件可以圖3A至圖3C中所

示之方式來表示。每一配件物件可經指派在配件物件之陣列內唯一之配件執行個體ID。應理解，給定配件伺服器可服務全部表示於用於彼配件伺服器之單一配件定義記錄中的一或多個配件物件。控制器可與任何數目之配件伺服器通信。在一些實施例中，控制多個配件(或將訊息轉送至另一配件)之單一端點可被稱作「橋接器」，且用於此存取點之配件定義記錄可包括用於橋接器之配件物件以及用於由橋接器控制之每一配件之配件物件。用於橋接器之配件物件可僅包括配件資訊服務之單一執行個體，且用於橋接器之配件物件之存在可向控制器指示橋接器存在。

在操作中，每一配件(或配件伺服器)可將其配件定義記錄儲存於持久性儲存器中。配件可應請求而將其配件定義記錄之全部或部分提供至控制器。如下所述，此可作為器件探索程序之部分或在其他時間(例如，在來自配對控制器之請求後)發生。在一些實施例中，控制器可使用來自配件定義記錄之資訊來判定是與配件配對抑或以其他方式連接至配件。若建立配對或連接，則控制器可使用配件定義記錄來判定如何控制配件。

配件定義記錄可為自含的，意味控制器不需要關於配件之任何其他資訊以與配件互動。舉例而言，配件定義記錄可包括製造商特定特性(例如，「com.discoball.ch.rotate-direction」)及/或製造商特定服務(例如，「com.discoball.svc.discoball」)之完整定義，且該定義可包括特性及服務之人可讀描述符。控制器可經程式設計以產生呈現人可讀描述符及用於各種特性之使用者可操作控制元件(例如，基於特性之「單位」性質來選擇)之使用者介面，且使用者可操作控制元件以視需要控制配件。控制器可基於使用者輸入(例如，將新值寫入至特性)來發送控制訊息，因此允許控制配件而控制器不需要配件特定軟體或其他配件特定定製。

實例配件探索程序

在控制配件之前，控制器首先建立與待控制之配件之通信。如本文中所使用之「配件探索」大體上係指控制器可藉以定位將與之通信之配件的任何程序。在一些情況下之探索可包括控制器與配件之間的通信應發生的使用者驗證。在一些實施例中，配件探索可充分利用有助於定位無線或其他網路上之器件及/或服務的現有服務探索協定，諸如簡單服務探索協定(Simple Service Discovery Protocol，SSDP)、由UPnP論壇(http://www.upnp.org)開發之協定或由Apple Inc.開發之Bonjour®網路連接技術(公開為IETF RFC 6762及IETF RFC 6763且在本文中被稱作「Bonjour」)。在器件探索服務中，一個器件(例如，配件)可廣告指示其存在之資訊、位址及視情況關於其能力之額外資訊。其他器件(例如，控制器)可瀏覽廣告且基於廣播資訊來識別感興趣之器件。使用該位址，瀏覽器件可起始與廣告主之通信。

視網路及探索服務而定，廣告可(但不必)包括資訊之即時廣播(例如，經由多播或信標信號)及/或將廣告資訊提供至中央儲存庫(例如，處於網路存取點)，其他器件可自該儲存庫擷取資訊。廣告瀏覽可包括偵測廣播廣告及/或自該中央儲存庫擷取廣告資訊。

圖4為根據本發明之一實施例的用於藉由控制器404探索配件402之程序400的流程圖。配件402可為(例如)圖1中之配件中之任一者，且控制器404可為(例如)圖1之控制器102。

在區塊410，配件402可設定狀態位元以指示配件當前未配對(或在尋找與之配對之控制器)。此可為(例如)下文所描述之狀態旗標指示符「sf#」中之位元。

在區塊412，配件402可在器件探索服務上將配件之存在廣告為支援配件協定之配件。舉例而言，使用Bonjour，配件可自身對名稱及服務類型做廣告。名稱可為用於配件之使用者可讀名稱(例如，「恆溫

器」)；在一些情況下，所廣告之名稱可為配件定義記錄之配件資訊服務執行個體中所規定之名稱。服務類型可針對統一配件協定來定義(例如，服務類型「_uap._tcp」。廣告亦可包括額外資訊。舉例而言，配件可提供具有表3中所示之金鑰之Bonjour TXT記錄。

金鑰	描述
「c#」	當前組態號碼。 在配件定義記錄經修改時(例如，在配件、服務或特性經新增或移除時)更新；跨重新啟動、功率循環等持續。可由配對控制器使用以偵測配件組態改變。
「ff」	特徵旗標 可為可用以指示選定特徵之存在或不存在的位元遮罩。
「id」	配件之全域唯一ID (例如，主MAC位址)
「md」	配件模型名稱
「ps」	配件之主服務類型(例如，「com.proto.svc.lightbulb」) 若存在，則可提供關於配件功能(名稱除外)之控制器額外資訊。
「pv」	協定版本字串(例如，以格式<major>.<minor>) 可用以檢查相容性。在一些實施例中，若配件指示之主要版本大於控制器之軟體之主要版本，則控制器可將配件自可用組排除。
「s#」	當前狀態號碼 每當特性之值改變時遞增；跨重新啟動、功率循環等持續。
「sf#」	探索狀態旗標。 可為指示當前狀態之態樣(例如，未配對、在配件上偵測到之問題、存取配件所需之授權、未組態以加入無線網路之配件)的位元遮罩。

表3

熟習此項技術者將瞭解，類似資訊可使用其他服務探索協定及技術來分散。舉例而言，使用SSDP，配件可使用多播HTTP NOTIFY訊息來廣告名稱及服務類型URI，且URI可由控制器使用以經由對配件之單播請求來擷取額外資訊。

在區塊414，控制器404可瀏覽未組態配件。無特定時序係必需的，儘管一般而言，控制器將僅在配件之廣告在控制器瀏覽時可偵測之情況下探索配件。

在區塊416，控制器404可(例如)藉由偵測來自區塊412之廣告來尋找配件402。在區塊418，控制器404可基於廣告來判定配件402係「感興趣」的抑或用於相互操作之潛在候選者。舉例而言，控制器404可檢

查表3中之探索狀態旗標「sf#」以判定配件是否已經組態或與控制器配對。作為另一實例，控制器404可檢查表3中之協定版本「pv」以判定配件之協定版本是否與控制器之協定版本相容。此外，在一些情況下，控制器可瀏覽特定內容脈絡(例如，執行特定應用程式)中之配件且可基於所廣告之名稱、主服務識別符、配件模型名稱、特徵旗標或可自配件之廣告得到的任何其他資訊來限制感興趣之配件。若控制器404判定配件並非感興趣的，則控制器404可返回區塊414並繼續瀏覽。(在一些實施例中，瀏覽操作可在未找到感興趣之配件的情況下逾時)。

在區塊422，控制器404可呈現關於配件之資訊給使用者，且在區塊424，使用者可提供指示控制器是否應與該配件建立一配對之輸入。舉例而言，控制器404可呈現自配件之廣告獲得之資訊之任一者或全部給使用者且提示使用者指示控制器404是否應連接至配件402。儘管非必要，但請求使用者確認可幫助避免控制器與配件之間的混充或非所需配對。

在區塊426，控制器404可解譯區塊424處所接收之使用者輸入且判定控制器是否應與配件402配對。若不配對，則控制器404可返回區塊414以尋找其他配件。若控制器404及配件402應配對，則在區塊428及430，控制器404及配件402可執行對設置程序。在一些實施例中，對設置程序可用以建立加密金鑰以促進控制器404與配件402之間的安全通信；區塊428及430處可實施之對設置程序之實例描述如下。在一些實施例中，使用者確認可併入至對設置程序中，且在起始對設置之前的單獨使用者確認並非必需的。

假定對設置製程成功地完成，則在區塊431，配件402可更新其狀態以指示現在需要授權以與配件通信及/或配件現與至少一個控制器配對，例如，藉由更新上文所述之狀態旗標指示符「sf#」。

在區塊432，控制器404可自配件402獲得配件定義記錄且快取該

配件定義記錄，在區塊434，該配件可在請求後提供該記錄。在控制器404快取配件定義記錄之情況下，資訊可用以促進偵測配件402中之狀態改變。在一些實施例中，控制器404亦可自配件之廣告快取資訊(例如，來自上表3之資訊之任一者或全部)，且此資訊亦可用以(例如)使用如下所述之狀態計數器「s#」來偵測配件中之狀態改變。

在區塊436及438，控制器404及配件402可開始交換命令及控制訊息，從而允許控制器404控制配件402。在一些實施例中，此等訊息可使用在對設置程序中或在如下所述之後續對驗證程序中所產生之金鑰來加密。

應瞭解，本文中所描述之探索程序係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。此外，儘管使用Bonjour服務作為器件探索服務之實例，但其他器件探索服務之內容脈絡中可應用類似概念。

在一些實施例中，在判定是否與特定配件配對之前，控制器404可向配件402請求配件定義記錄(或其一部分)。舉例而言，控制器404可將訊息(例如，HTTP GET請求)發送至配件以請求配件之配件定義記錄。至用於HTTP GET請求之URL可由統一配件協定之約定或在配件之廣告內(例如，在TXT記錄中)規定。視組態而定，配件402可回應於來自未配對控制器之請求而提供其配件定義記錄之全部、一些或不提供任一者。在一些實施例中，配件402可提供部分配件定義記錄。舉例而言，如上所述，一些特性可具有規定該等特性僅可由配對控制器讀取及/或寫入的性質，且將關於此等特性之資訊提供至未配對控制器可能非所要的。因此，配件402可識別「公用」特性(亦即，准許未配對控制器讀取及/或寫入之特性)，且提供至未配對控制器之部分配件定義可僅包括具有至少一個公用特性的服務執行個體且可僅包括具有公用及非公用特性兩者之服務執行個體的公用特性執行個體。在一些實施

例中，配件定義記錄在配對建立之前根本不可存取；在彼情況下，是否配對之決策可基於配件之廣告、控制器之內容脈絡及/或使用者輸入。

在一些實施例中，探索程序400或類似程序可用以偵測狀態改變。舉例而言，如表2中所指出，狀態數目「s#」可在狀態改變時遞增。配件可(例如)藉由廣播已更新TXT記錄來廣告狀態改變，且先前已快取該TXT記錄(例如，在程序400之區塊432)之配對控制器可藉由比較「s#」之廣播值與其快取值來偵測該改變。

圖4之程序可在控制器及配件使用TCP/IP通信的情況下使用。在一些實施例中，除TCP/IP之外或替代TCP/IP，統一配件協定亦可支援諸如藍芽LE之其他傳輸。在情況如此的情況下，配件可使用藍芽LE來廣告其服務。舉例而言，配件可在一或多個藍芽LE廣告頻道上做廣告。廣告資料可包括(例如)以下各者中之任一者或全部：配件之本機名稱；唯一配件識別符；指示配件可探索之旗標；用於服務中之至少一些(包括如下所述之配對服務)的UUID；配件狀態之指示符(類似於表2中之當前狀態號碼)；及配件是否已執行與至少一個控制器之對設置的指示。此資訊可用於類似於上文所述之程序400的探索程序中。

實例通信

在一控制器已與配件建立配對之後，該控制器可將命令及控制訊息(請求)發送至該配件。此等請求可用以獲得關於該配件之狀態的資訊及/或改變該配件之狀態的態樣。在一些實施例中，該命令及控制訊息可為定址至反映用於特定服務或特性之路徑之URL的HTTP請求，如配件定義記錄中所定義。在此等實施例中，該配件可充當一伺服器(接收及回應對資源之請求)，而該控制器可充當一HTTP用戶端(產生對伺服器/配件之請求及接收回應)。應注意，一些配件可實施(例如)用於管理不同介面或網域上之通信的多個HTTP伺服器。在一些實施例中，配

件及控制器可經由單一TCP連接及/或HTTP管線來支援多個HTTP請求(例如，在接收回應之前發送多個HTTP請求)。

舉例而言，給定圖3A至圖3C中所示之配件物件300，控制器可建構圖5A之URL 500以表示資源(在此情況下，圖3B中所定義之開門器服務執行個體320之門狀態特性執行個體321)。URL 500包括協定識別首碼502 (「http://」)、用於配件之主機名稱504 (其可經由上文所述的圖4之探索程序獲得)及本機路徑506。本機路徑506可包括用以指示對經由統一配件協定暴露之服務之引用的協定關鍵字508 (「proto/」)、用以識別特定服務執行個體的服務執行個體識別符510 (「service/<serviceID>」)及用以識別服務執行個體內之特性執行個體的特性執行個體識別符512 (「characteristic/<characteristicID>」)。在圖5A中，<serviceID>及<characteristicID>用配件物件中所定義之執行個體識別符來替換。因此，參看圖3A至圖3C，具有instanceID 7的服務執行個體為車庫開門器服務執行個體320，且具有instanceID 8的特性執行個體可為當前狀態特性執行個體321。因此，URL 500可理解為參考車庫開門器之當前門狀態。以類似方式，其他URL可使用用於服務及特性之instanceID根據配件定義記錄產生。任何服務執行個體之任何特性執行個體可以此方式來識別。

控制器可產生對以此方式建構之URL的HTTP GET(PUT)請求以讀取(寫入)特性。此外，URL 500之階層結構可經利用以允許控制器在單一異動中讀取多個特性或多個服務或寫入至多個特性或多個服務。舉例而言，發送讀取特定服務之所有特性的GET請求可藉由省略特性識別符來實現。回應可為含有特性之JSON物件，格式類似於圖3A至圖3C。

為了判定配件資源之當前狀態，控制器可基於圖5A之URL 500發送HTTP GET請求。圖5B展示自圖5A之URL 500建構之GET請求520之

實例。GET請求520經定址至URL 500之主機504且將本機路徑526 (類似於URL 500之本機路徑506)規定為待擷取之資源。在此實例中，本機路徑526未規定單一特性；此可解譯為讀取所規定服務執行個體之所有特性的請求。

回應於HTTP GET請求520，配件可發送提供所請求資源(狀態資訊)之HTTP回應。圖5C展示可回應於圖5B之請求提供的實例HTTP回應530之一部分。該回應包括HTTP回應標頭532，其識別回應及狀態(「200 OK」)及指示內容534如統一配件協定所定義地格式化為JSON物件。內容534包括所請求資源之狀態資訊，在此實例中，該狀態資訊為圖3B之開門器服務執行個體320。服務執行個體320包括五個特性執行個體，且所有五個特性之當前狀態經報告，此係因為該請求用以讀取所有特性。(僅兩個特性展示於圖5C中；應理解，其餘特性可以類似方式呈現)。其他粒度層級處的讀取請求及反應可藉由修改路徑526以反映所要粒度層級來建構(例如，單一特性執行個體或所有服務執行個體)。

類似地，控制器可藉由將HTTP PUT請求發送至適當URL來改變配件之狀態資訊。圖5D展示自圖5A之URL 500建構之PUT請求540之實例。PUT請求540經定址至URL 500之主機504且將本機路徑546 (類似於URL 500之本機路徑506)規定為內容542待寫入至的資源。在此實例中，PUT請求540寫入至一個特性執行個體，因此路徑546包括所要特性執行個體之instanceID (其對應於圖3B之開門器目標狀態特性執行個體322)。內容542規定待寫入之值。在圖3B之實例中，特性執行個體322係類型「com.proto.ch.door-state.target」，且如上所述，此特性類型之值1可映射至「開啟」狀態。因此，PUT請求540可由配件解譯為用以開啟車庫門之指令。

配件可回應以空HTTP「204 No Content」回應，可(例如)藉由開啟門來實施狀態更新。(雖然門係主動地開啟，但配件可將當前門狀態

特性執行個體321更新至指示門在開啟中的值，接著在門完全開啟後即更新至指示「開啟」的值。在一些實施例中，配件回應可包括例如如下參看圖5F所述之內容。舉例而言，若錯誤產生，則配件可回應以HTTP錯誤回應。舉例而言，HTTP錯誤碼400可指示不良請求(例如，語法錯誤或無效特性)，錯誤碼403可指示禁止動作(例如，試圖寫入至一資源，控制器並不具有針對該資源之寫入權限)，且錯誤碼500可指示配件處之內部錯誤。在一些情況下，錯誤回應之內容可包括具有關於該錯誤之資訊的「回應」物件。回應物件之實例描述如下。

在一些實施例中，多個特性可使用單一PUT請求來寫入。圖5E展示自圖5A之URL 500建構之PUT請求550之實例。PUT請求550可類似於PUT請求540，惟以下除外：本機路徑556處在服務粒度層級，其允許寫入多個特性。參考圖3之配件定義300及圖2A中之特性定義，PUT請求550可解譯為用以解除鎖定並開啟車庫門之請求。如此實例展示，有可能使用PUT請求寫入至服務之特性之一子集。該請求可包括待寫入之特性；類型及instanceID金鑰存在於每一特性資料物件內可防止語意模糊。此外，待寫入之特性可以任何次序列出。

配件可回應以包括每一特性之當前狀態的訊息。圖5F展示根據本發明之一實施例的實例回應560。回應560係非空HTTP回應，其內容562包括每一已更新特性563、564之當前值。對於每一特性，將包括「回應」物件565、566。如所示，回應物件可包括「developerMessage」。若錯誤發生，則developerMessage可提供錯誤的一般語言解釋且視情況提供用於校正問題之建議。「errorCode」可為數值碼(其可用以(例如)選擇作為回應的待採取之控制器動作)。「moreInfo」字串可提供額外資訊，諸如識別協定規範之區段或應參考以用於對錯誤有幫助之其他文件。在圖5F中所示之實例中，無錯誤發生，且每一特性之狀態係圖5E中所請求之狀態。若錯誤發生，則狀態可不匹配所請求之狀態。

以類似方式，類似於圖5E之請求550的PUT請求可用以寫入至服務或寫入至多個服務，且類似於圖5F之請求506的回應可產生。

如所描述，控制器可藉由發送PUT請求來請求配件中之狀態改變。在一些情況下，狀態改變可涉及調用可需要某一時間來完成對配件功能(例如，命令或操作之執行)。為了允許回應中之配件靈活性，一些實施例支援關於一些特性或服務之延遲回應行為。

當控制器使用HTTP PUT寫入至特性時，配件可評估請求且選擇一回應選項(例如，基於被寫入之特定特性)。在一些實施例中，提供兩個回應選項：「內嵌結果(inline result)」及「查詢結果(query result)」。對於內嵌結果，配件執行所請求之操作，接著在HTTP回應中傳回結果(例如，如上參看圖5E及圖5F所描述)。該回應可視需要儘量延遲以完成操作。對於查詢結果，配件在執行操作之前傳回HTTP回應。在此情況下，預操作HTTP回應可包括「transactionID」(由配件指派)，控制器稍後可使用其發送HTTP GET請求以獲得結果。預操作HTTP回應亦可包括「異動持續時間」(亦由配件指派)，其指示控制器在發送GET請求之前應等待的最少時間。配件可基於每個請求來選擇回應選項。

以說明方式，考慮實施用以開啟組態埠之功能性的配件。該埠可模型化為具有各種特性之服務。圖5G展示特性執行個體571，控制器可將布林值真寫入至該特性執行個體以請求開啟埠。圖5H展示根據本發明之一實施例的PUT請求572，其可由控制器使用以請求開啟埠。(應理解，特性執行個體571係定義於具有instanceID 22之服務執行個體內)。配件可滿足或拒絕該請求，例如，視控制器權限或配件之當前狀態而定。配件可選擇首先作用於請求、接著回應(內嵌結果)或回應、接著作用(查詢結果)。

若配件選擇首先作用於請求，則配件可發送指示結果之內嵌回應。舉例而言，滿足請求可包括建立通訊端及開始在埠上收聽。配件

可在其HTTP回應中傳遞關於組態埠之資訊。圖5I展示圖5H之請求572的內嵌HTTP回應573之實例。內容574可包括用於該請求之埠識別符及狀態指示符。

若配件選擇首先回應，則配件可發送含有控制器稍後可用以查詢結果之資訊的異動回應。圖5J展示根據本發明之一實施例的異動回應575之實例。異動回應575包括異動ID 576 (其可為UUID或由配件產生以識別異動之其他識別符)及異動持續時間577 (例如，以秒計)。回應575指示：控制器應等待5秒，接著查詢配件以擷取回應。在彼時間期間，配件可執行動作且連同異動ID一起儲存結果。

在異動持續時間已過去之後，控制器可(例如)藉由使用與第一請求相同之URL發送HTTP GET請求 來查詢配件。圖5K展示根據本發明之一實施例的可用於異動狀態查詢之HTTP GET請求578之實例。GET 578可包括來自異動回應575之異動ID。此向配件指示：查詢係針對配件已儲存之特定異動結果。配件可回應以包括異動之結果的HTTP回應；此回應可類似或等同於圖5I之內嵌回應573。

可實施用於存取資源之其他技術。一個替代實施可使用非階層式URL且利用配件之每一服務執行個體及特性執行個體的唯一執行個體ID，此可減小HTTP訊息之長度。

舉例而言，圖6A展示可建構以允許存取配件之特性及服務的簡化URL 600。URL 600包括協定識別首碼602 (「http://」)、主機名稱604 (其可經由上文所述的圖4之探索程序提供)及本機URL 606 (在此實例中為「/characteristics」)。本機URL 606可選自由配件支援之一組URL。表4列出統一配件協定可根據本發明之一實施例定義之URL。

本機URL	支援請求
/accessories	GET：獲得配件定義記錄
/characteristics	GET：詢問特性 PUT：修改特性

/identify	POST：調用配件自識別常式(可被具有至少一個已建立對之配件忽略或拒絕)
/pair-setup	POST：對設置請求
/pair-verify	POST：對驗證請求
/pairings	POST：新增、移除或列出配對之請求

表4

在此實例中，控制器可藉由發送對以圖6A中所示之方式建構、具有基於待調用之功能選自表4之本機URL的URL之請求來調用配件功能。/pair-setup、/pair-verify及/pairings URL可結合建立及驗證控制器與配件之間的配對來使用；實例描述如下。配對控制器可發送對配件之/accessories URL的GET請求以獲得其配件定義記錄。/特性URL可用於涉及讀取或寫入配件特性之所有互動。

/identify URL可允許未配對控制器調用配件之自識別常式，例如在配件已與任何控制器建立配對之前。若配件未與任何控制器配對，則配件可回應以HTTP 204「No Content」回應且進行至調用該自識別常式。若配件已與控制器建立配對，則配件可拒絕該請求(例如，以HTTP 400「Bad Request」回應)，指示該URL無效。在一些實施例中，配對控制器可藉由寫入至身分識別特性271 (其可包括於如圖2I及圖3A中所示之配件識別服務中)來調用配件之自識別常式。

圖6B展示可使用URL 600發送以讀取由圖3A至圖3C之配件物件300定義的配件之特性的HTTP GET請求610之實例。GET請求610經定址至URL 600之主機604且規定本機URL 606。字串612係規定待讀取之特性執行個體的URL參數。所使用之格式為<accessoryIID>.<characteristicIID(s)>，其中<accessoryIID>係配件之執行個體識別符，且<characteristicIID(s)>係用於待讀取之特性之執行個體識別符的逗號分隔之清單。參考圖3B之執行個體ID，GET請求610可理解為用以讀取當前門狀態及目標門狀態之請求。可使用其他格式，諸如特性執行個體識別符之範圍(例如，URL參數「?1.8-12」)。

在此實例中，指定服務執行個體識別符並非必需的，此係因為配件之每一特性經指派唯一執行個體識別符。在其他實施例中，可視需要包括服務執行個體識別符。

圖6C展示可回應於GET請求610發送之HTTP回應620之實例。回應620可包括HTTP回應標頭622，其識別回應及狀態(「200 OK」)且指示內容624係針對統一配件協定格式化為JSON物件。內容624可包括每一請求特性執行個體之狀態資訊(值)。在此實例中，針對每一特性所傳輸之資料僅包括該值及執行個體ID。只要配件之每一特性執行個體具有唯一執行個體ID，此資訊足以回應該請求。

配件之任何數目個特性(包括不同服務執行個體之特性)可使用單一GET請求及回應以此方式讀取。此外，若控制器正與服務多個配件物件之配件伺服器通信，則控制器可發送單一GET請求以讀取該伺服器上的多個配件之特性，例如藉由將該等特性規定為<accessoryIID>.<characteristicIID(s)>的逗號分隔之清單。舉例而言，URL參數(「?1.8.9,2.6,7」)可由配件伺服器理解為自具有執行個體ID 1之配件讀取特性執行個體8及9及自具有執行個體ID 2之配件讀取特性執行個體6及7。

特性可使用HTTP PUT請求寫入至配件之/characteristics URL。圖6D展示可用以寫入至配件之任何數目個特性的PUT請求630之實例。對於待寫入之每一特性，內容634可規定配件執行個體ID、特性執行個體ID及新值。在此實例中，寫入兩個特性，但陣列可包括任何數目個(一或多個)特性，包括同一配件伺服器上之不同配件之特性。

若無錯誤發生，則配件可回應以空HTTP「204 No Content」回應且可藉由起始適當動作(例如，觸發車庫開門器中之馬達以移動門)來實施狀態更新。若錯誤發生，則配件可回應以一錯誤訊息。圖6E展示可回應於PUT請求630發送之錯誤訊息640之實例。在此實例中，內容

644識別每一特性執行個體，針對每一特性執行個體之嘗試寫入(再次使用配件執行個體ID及特性執行個體ID)。未指示新值。狀態碼646、648係用以傳達哪些寫入失敗。在此實例中，狀態碼646 (值0)指示：關於具有執行個體ID 8之特性，無錯誤發生。狀態碼648 (值-12345)指示：關於具有執行個體ID 9之特性，錯誤發生。狀態碼648之值可指示錯誤之類型。舉例而言，狀態碼可經定義以視需要指示不足特殊權限(例如，控制器未經授權而寫入至特性)、不能存取資源(例如，配件斷電)、資源忙碌、請求不被支援(例如，嘗試寫入至唯讀特性)、值無效(例如，超出具有最小值及最大值之特性之範圍)及其他錯誤條件。

應瞭解，圖5A至圖5K及圖6A至圖6E之此等命令及控制訊息格式及序列係說明性的且變化及修改係可能的。HTTP允許任何資源在任何時間被請求；因此，控制器可以任何次序發送HTTP請求，且配件可以接收之次序來回應HTTP請求。配件可回應以標準HTTP反應(包括錯誤訊息)，且控制器可將HTTP反應視為應答(或，在錯誤的情況下，否定應答)訊息。在一些實施例中，配件服務及特性至HTTP資源之映射可允許控制器如何擷取資訊的很大靈活性。在一些實施例中，使用具有較短URL之執行個體識別符可導致較短請求及反應，此可減小頻寬要求。

此外，儘管所示實施例使用HTTP，但本發明不限於任何特定框架協定；其他協定可取代。舉例而言，在控制器及配件使用藍芽LE通信之實施例中，控制器可藉由充分利用藍芽LE GATT層及指派給每一服務及特性之UUID來讀取及寫入至特性。

在上文之實例中，控制器可藉由(例如)使用HTTP請求將命令及控制訊息(請求)發送至配件來起始配件中之狀態改變。在其他情況下，可藉由除控制器外之源來起始配件狀態改變，且控制器在此改變發生時可能或可不連接至配件。舉例而言，不同控制器可在不同時間與同

一配件互動，或使用者可人工地操作配件(例如，推動車庫中之開啟/關閉按鈕以啟動車庫開門器)。因此，配件狀態可在控制器不知道的情況下改變。因此，統一配件協定之一些實施可提供用於通知控制器狀態改變之機制。可同時支援多個通知機制，且控制器可例如基於每個特性或每個服務來判定其首選哪個機制。

通知機制之實例在上文之表2中列出。在一些情況下，配件可維持每當配件之狀態改變時可遞增的內部狀態計數器。單一狀態計數器可維持在配件層級，或不同狀態計數器可視需要針對不同服務或特性維持。各種實施例可支援描述如下之通知機制中之任一者或全部。

圖7展示根據本發明之一實施例的「被動式」通知程序700之實例。程序700涉及控制器讀取配件之內部狀態計數器以判定狀態改變是否已發生。因此，改變在控制器與配件斷接時已發生的事實可由控制器在其隨後重新連接時偵測。在一些實施例中，被動式通知係預設啟用(例如，每一配件維持內部狀態計數器)，不需要特定動作(例如，訂用)來啟用被動通知。

在區塊706及708，控制器702及配件704可建立連接。在各種實施例中，建立連接可包括執行程序400及/或描述如下之其他程序(例如，對驗證)。

在區塊712，配件704可將其當前內部狀態計數器值提供至控制器702，在區塊714，該控制器可獲得並儲存該值。在一些實施例中，控制器702可發送對適當資源(例如，可定義於配件資訊服務中之可讀狀態計數器特性)之HTTP GET請求。配件704在區塊712處之回應可含有該計數器值。控制器702可儲存此值。在此後的某一點，控制器702可與配件704斷接(區塊716)。

在區塊718，在控制器702已斷接之後，狀態改變可出現在配件704中。作為回應，在區塊720，配件704可更新其狀態計數器。

此後，控制器702可重新連接至配件704 (區塊722)。在區塊724，配件704可將當前內部狀態計數器值提供至控制器702，在區塊726，該控制器獲得該值。在一些實施例中，此操作可經由控制器702對適當資源的HTTP GET請求來進行；配件704之回應可含有該計數器值。在區塊728，控制器702可(例如)藉由比較在區塊726所獲得之計數器值與先前在區塊714所獲得並儲存之計數器值來偵測狀態改變。在一些實施例中，控制器702可用新值覆寫舊的儲存計數器值。此後，在區塊730，配件704可將已更新狀態資訊提供至控制器702，在區塊732，該控制器獲得該資訊。在一些實施例中，此操作可使用控制器702之HTTP GET請求及配件704之回應來進行。該控制器可選擇請求配件定義記錄或僅請求特定特性(針對該等特性之狀態改變係控制器所關心的)。

圖8展示根據本發明之一實施例的「廣告式」通知程序800之實例。在程序800中，配件可使用器件探索服務(例如，如上所述)來廣告狀態改變已發生。偵測廣告之控制器可連接至配件並獲得已更新狀態資訊。

在區塊806及808，控制器802及配件804可建立連接。在各種實施例中，建立連接可包括執行程序400及/或描述如下之配對程序。在區塊810，控制器802可指示訂用廣告式通知之需要。舉例而言，如上所述，參看圖2E，每一特性可具有notificationMode性質，且控制器可藉由寫入至notificationMode性質來規定通知模式。在一些實施例中，配件804不廣告狀態改變，除非至少一個控制器已訂用廣告式通知；此可減少網路訊務。

在區塊812，配件804可將當前內部狀態計數器值提供至控制器802，在區塊814，該控制器獲得並儲存該值。在一些實施例中，此操作可經由控制器802對適當資源的HTTP GET請求來進行；配件804之回應可含有該計數器值。控制器802可儲存此值。在此後的某一點，控制

器802可與配件804斷接(區塊816)。

在區塊818，在控制器802已斷接之後，狀態改變可出現在配件804中。作為回應，在區塊820，配件804可更新其內部狀態計數器。在區塊822，配件804亦可廣告已更新狀態計數器。舉例而言，如上文之表3中所示，配件可(例如)在Bonjour TXT記錄或類似者中廣告包括狀態數目「s#」之資訊。配件可藉由更新該欄位及廣播新TXT記錄來廣告狀態改變。

在區塊824，假定控制器802正在收聽廣播，則控制器802可偵測改變。舉例而言，控制器802可自廣播提取當前狀態計數器、比較該廣播狀態計數器與儲存之狀態計數器且偵測不一致，其指示配件之狀態已改變。在區塊826，控制器802可重新連接至配件804。在區塊828，配件804可將已更新狀態資訊提供至控制器802，在區塊830，該控制器獲得該資訊。在一些實施例中，此操作可經由控制器802之HTTP GET請求及配件804之回應來進行。

圖9展示根據本發明之一實施例的「主動式」通知程序900之實例。在程序900中，配件可起始至控制器之連接以在狀態資訊經更新時警示控制器。舉例而言，控制器可登記具有專用於接收狀態更新之器件探索服務(例如，Bonjour服務)的服務記錄，且配件可使用控制器之服務記錄來起始至控制器之連接。

在區塊906及908，控制器902及配件904可建立連接。在各種實施例中，建立連接可包括執行程序400及/或描述如下之配對程序。在區塊910，控制器902可指示訂用主動式通知之需要。舉例而言，如上所述，每一特性可具有notificationMode性質，且控制器可藉由寫入至notificationMode性質來規定通知模式。在一些實施例中，配件904僅當至少一個控制器已訂用主動式通知時才執行與主動式通知相關之操作；此可減少網路訊務。

在區塊912，控制器902可設置一埠以收聽主動式通知。在區塊914，控制器902可登記具有器件探索服務之服務記錄。舉例而言，若使用Bonjour服務，則控制器902可登記唯一DNS SRV記錄。若SRV記錄係唯一的，則控制器可避免諸如探查、廣告或提供TXT記錄之操作，藉此減少網路訊務。在一項實施例中，DNS SRV記錄可具有如下格式：

<ID>._guid._tcp.local. <TTL> IN SRV <priority> <weight> <port> <target>,

其中<ID>為控制器之唯一識別符(例如，小寫且破折號經移除之GUID、UUID或其他識別符)；「._guid._tcp」為DNS服務類型；「local」為網域名稱；<TTL>為SRV記錄之存留時間(其可為例如120秒)；<priority>為目標主機之優先權(其可為例如在服務中辨識之最高優先權)，<weight>為用於具有相同優先權之記錄的相對權重(其可為例如0)；<port>為在控制器902上執行的一統一配件協定伺服器之TCP埠數目(例如，在區塊912設置之埠)；且<target>為可用以獲得IP位址以連接至該統一配件協定伺服器的DNS名稱。

在區塊916，控制器902可斷接。

在區塊918，在控制器902已斷接之後，狀態改變可出現在配件904中。作為回應，在區塊920，配件904可查詢器件探索服務以定位已登記服務，例如藉由發送針對服務類型「._guid._tcp」之多播DNS SRV查詢。(在一些實施例中，配件904在區塊920執行該查詢且僅當至少一個控制器已訂用主動式通知時才執行隨後動作)。在區塊922，控制器904可以在區塊912及914建立之DNS名稱及埠識別符來回應該查詢。在區塊924，配件904可發送對該埠之單播查詢以解析DNS名稱。在一些實施例中，支援IPv4及IPv6定址版本兩者之配件可使用IPv4及IPv6定址兩者來發送查詢(例如，用於IPv4之DNS A查詢及用於IPv6之DNS AAAA查詢)；若配件僅支援一個IP位址版本，則配件可發送一個查詢。

在區塊926，控制器902可發送具有其解析位址之單播回應。若配件發生兩個查詢，則控制器可視其支援哪個(哪些) IP位址版本來回應任一者或兩者。

在區塊928，配件904可使用解析位址來起始至控制器902之新連接。在一些實施例中，若控制器提供IPv4及IPv6位址兩者，則IPv6可為較佳的。在區塊930，控制器902可接受該連接。若連接嘗試失敗，則配件可重試；在一些實施例中，重試頻率可(例如)限於每60秒一次。

在區塊932，配件904可發送已更新狀態資訊，且在區塊934，控制器902可接收已更新狀態資訊。在一些實施例中，在發送已更新狀態資訊之前可需要(例如，使用描述如下之對驗證程序)驗證先前建立之配對。此可提供配件將狀態資訊報告至訂用通知之同一控制器的保障。

圖10展示根據本發明之一實施例的「事件通知」程序1000之實例。在程序1000中，配件可將非請求型HTTP回應(在本文中亦被稱作EVENT訊息)發送至控制器，其當前經訂用以接收針對已改變之特性之事件通知。在此實例中，控制器可在其連接至配件時在任何時間訂用通知且在與配件斷接後自動地變得不訂用。

在區塊1006及1008，控制器1002及配件1004可建立連接。在各種實施例中，建立連接可包括執行程序400及/或描述如下之其他配對程序。在區塊1010，控制器1002可指示訂用事件通知之需要。舉例而言，如上所述，每一特性可具有通知模式性質，且控制器可藉由寫入至此性質來規定通知模式。

圖11A展示用以訂用針對特性之事件通知的HTTP PUT請求1100之實例。內容1102識別特性(按配件執行個體ID及特性執行個體ID)且包括用於notificationMode性質之值「ev」。多個特性可在單一訂用請求中列出，且在一些實施例中，訂用請求可與寫入值至一或多個特性之請求組合。配件可將請求1100理解為訂用針對規定特性之事件通知的

請求且可回應以確認(例如，HTTP 204「No Content」)或錯誤回應(例如，在針對該特性不支援事件通知的情況下)。類似訊息可由控制器使用以藉由規定所要通知方法來訂用其他類型之事件通知(例如，如上所述的主動式或廣告式通知)。

在訂用之後，在區塊1014，控制器1002可取消訂用基於事件之通知。在一些實施例中，控制器1002在其與配件1004斷接的情況下自動取消訂用。另外或實情為，控制器1002可藉由在不與配件1004斷接之情況下將新值寫入至通知模式性質來明確地取消訂用。若控制器1002取消訂用(自動地或明確地)，則任何後續事件通知將不再發送至控制器1002，且程序1000可在區塊1016結束。(未取消訂用之控制器1002當然可執行程序1000以再次訂用)。自動地或明確地取消訂用控制器1002可幫助減少配件1004之電力消耗，此係因為配件1004可避免產生事件訊息或嘗試將事件訊息發送至無興趣(或未連接)之控制器。

在區塊1018，狀態改變可出現在配件1004中，且在區塊1020，配件1004可更新其內部狀態計數器；更新內部狀態計數器可對與例如如上所述之被動式及/或廣告式通知之連接有用。另外，若控制器1002經訂用基於事件之通知，則配件1004可產生至控制器1002之通知。

舉例而言，在區塊1024，配件1004可判定任何控制器(例如，控制器1002)當前是否訂用針對受影響特性之狀態改變的基於事件之通知。

若當前無控制器訂用，則不採取進一步動作，且程序1000可在區塊1026結束。若至少一個控制器(例如，控制器1002)當前經訂用，則在區塊1028，配件1004可產生含有已更新狀態資訊之事件訊息。

圖11B展示根據本發明之一實施例的事件訊息1120之實例。事件訊息1120在結構上可類似於HTTP回應；然而，不同於HTTP回應，事件訊息1120並非回應於特定HTTP請求而發送。標頭節1122可將訊息1120識別為事件訊息且可包括版本資訊及狀態碼。主體1124可包括改

變的特性之更新值；如在本文中之其他實例中，特性可藉由配件識別符及執行個體識別符來識別。應理解，若多個特性已改變，則配件可將多個特性包括於單一事件訊息1120中；亦即，事件訊息可聚結。亦可使用其他格式。

再次參看圖10，在區塊1030，配件1004可將事件訊息發送至控制器1002，且在區塊1032，控制器1002可接收事件訊息。舉例而言，控制器1002中之HTTP堆疊可經修改以辨識事件訊息1100 (例如，基於標頭1122)。控制器1002可自接收的事件訊息提取已更新狀態資訊。

將瞭解，上文所述之各種通知方法係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。此外，同一配件可同時支援該等通知程序中之任一者或全部，且相同狀態改變可導致以下各者中之任一者或全部：更新內部狀態計數器；廣告已更新狀態計數器；起始與一或多個訂用控制器之連接；及/或將事件訊息發送至訂用控制器，視在狀態改變時各種控制器已訂用哪些通知選項而定。除圖7至圖10中所示之彼等通知機制及程序之外或替代前述各者，亦可支援其他通知機制及程序。

如上所述，控制器可基於每個特性來訂用狀態改變通知，例如藉由寫入至特性之notificationMode性質。配件可基於是否任何控制器訂用關於在考慮中之特性的每一通知機制來判定執行哪個(哪些)通知機制。在一些實施例中，被動式通知為預設機制且內部狀態計數器始終在更新，不管任何控制器特定地請求了什麼。因為廣告式、事件及/或主動式通知可建立網路訊務，所以此等機制之使用可限於依賴於被動式通知可不利地影響使用者體驗的執行個體。

在一些實施例中，可強加各種策略以減少藉由宣告狀態改變(例如，經由廣告式、事件及/或主動式通知)產生之網路訊務。舉例而言，狀態改變廣告可限於至少一個控制器訂用廣告通知的執行個體，且查

詢服務記錄以起始連接可限於至少一個控制器訂用主動式通知的執行個體。此外，可需要配件聚結具有最小延遲週期(例如，1秒)之所有廣告、主動式或事件通知，以進一步減少網路訊務。作為另一實例，廣告、事件通知及/或配件起始之連接在頻率上受限(例如，限於每30秒一個)。將網路訊務減到最少之被動式通知可用作預設。此等侷限性係設計選擇之麻煩且可視需要改變或消除。在強加侷限性且配件違反該等侷限性之情況下，偵測違規之控制器可警示使用者不適當行為及/或終止控制器與配件之配對。

實例配對程序

在一些實施例中，保全配件與控制器之間的通信可有用。舉例而言，參看圖1，控制器102可用以例如藉由如上所述地發送請求訊息來對門104解除鎖定或開啟車庫106。熟習此項技術者將瞭解此等操作應限於特定授權控制器。

因此，本發明之一些實施例提供安全性措施，諸如鑑認配對及端對端加密。鑑認配對可作為建立配件與控制器之間的配對(亦被稱作對設置)之部分發生，在配對期間，配件及控制器可建立安全性架構(例如，使用密碼編譯技術)且可在彼架構內交換長期公用金鑰。在一些實施例中，對設置可併有資訊(例如，設置碼)之頻帶外交換，且頻帶外交換可併有使用者輸入(或使用者動作)以向配件驗證其應與特定控制器配對及/或向控制器驗證其應與特定配件配對。在以此方式交換公用金鑰之後，控制器及配件可儲存該等金鑰且稍後使用該等金鑰來驗證配對經建立。端對端加密可包括產生配件及控制器兩者內之工作階段金鑰(例如，在驗證配對之後)及使用該等工作階段金鑰在每一訊息離開發送器件之前將每一訊息加密，以使得若訊息被攔截，則攔截器將不能夠利用該訊息。因此，在鏈路層或輸送層處保全通信網路並非必需的。舉例而言，新的工作階段金鑰可在每當配件及控制器重新連接

(例如，使用如下所述之對驗證程序)時產生。此外，可提供用於移除已建立配對之機制(例如，藉由移除儲存之長期公用金鑰)，以使得從前經授權以控制特定配件之控制器變為未授權的。

在一些實施例中，密碼編譯金鑰(包括描述如下之金鑰中之任一者或全部)可排他性地儲存於「安全元件」(諸如可安全地儲存器件之資料的專用積體電路晶片)(亦被稱作「安全儲存元件」)內。安全元件可用以提供接收的長期公用金鑰及/或識別其他器件(與該等器件的配對關係已建立)之其他資訊的持久性安全儲存。此可幫助防止攻擊者在不經過適當設置程序而新增配對(其可導致控制器之非法使用)或防止在未授權的情況下移除配對(其可阻止控制器之合法使用)。此外，在一些實施例中，安全元件亦可包括允許安全元件充當配件之主要處理器或控制器之共處理器(或「安全計算元件」)的邏輯電路。安全元件可接收各種輸入及用以對該等輸入執行密碼編譯操作的指令。安全元件可執行該等操作且提供輸出。本文中所描述之密碼編譯操作中之任一者或全部(例如，產生金鑰、用秘密金鑰簽署及涉及金鑰之其他操作)可委派給安全計算元件。如本文中所使用，「安全元件」可提供安全儲存及/或安全計算之任何組合。

在一些實施例中，支援配對之配件可具有作為其配件模型化之部分的配對設定檔。類似於本文中所描述之其他服務，配對設定檔可經定義為特性之集合。在一些實施例中，統一配件協定可規定具有配對設定檔之所有配件。在其他實施例中，配對設定檔可為選用之特徵，但協定可規定，若配件具有配對設定檔，則可需要控制器在交換任何命令及控制訊息之前與配件配對。配對要求之進一步訂製亦係可能的。舉例而言，配件之配對設定檔可識別需要配對之特定服務執行個體，從而允許在未配對的情況下存取配件之服務中的一些服務。

圖12展示根據本發明之一實施例的用於配對設定檔的實例特性

1201至1205。格式大體上類似於圖2A。如同本文中所描述之其他特性，特性1201至1205可由控制器(例如)使用HTTP GET請求或類似者來讀取；寫入(在准許情況下)可(例如)使用HTTP PUT或HTTP POST請求或類似者來執行。

配對狀態請求特性1201可由控制器寫入至以請求配對程序之狀態的改變(例如，在描述如下之對設置、對驗證、對新增及/或對移除程序期間發送各種請求)。在一些實施例中，控制器可藉由將HTTP POST請求發送至配對URL (例如，如上文之表4中所示)而非寫入至特性1201來請求配對程序之狀態的改變。配對程序狀態及請求之實例關於特定配對程序描述如下。

特徵旗標特性1202可為定義由配件支援之配對特徵的位元遮罩。舉例而言，如下所述，各種配件可支援基於設置碼之配對(其可需要使用者鍵入諸如PIN之設置碼以確認配對應發生)、基於憑證之配對(其可使用可使用器件中之任一者或兩者中之鑑認晶片來提供的憑證基礎結構，如下所述)及/或委派配對(其可允許已配對控制器驗證另一控制器應配對)。在一些實施例中，特徵旗標特性1202亦可包括指示配件當前是否處於使用對設置可藉以建立新配對之模式中的位元。特性1202可由控制器讀取但不寫入，且控制器可在判定如何及是否執行對設置中使用該資訊。

配對當前狀態特性1203可指示配對程序之當前狀態，例如錯誤是否已發生或描述如下之各種其他狀態。該狀態可由控制器讀取但不寫入。

配對清單特性1204可儲存器已與配件建立之所有配對之清單。舉例而言，可針對每一配對產生TLV項目，其指示配對控制器之公用金鑰(用於基於設置碼之配對)及/或憑證(用於基於憑證之配對)以及每一控制器具有的權限。此等TLV項目可(利用分離符)緊縮在一起以作為單

一頂層TLV之子TLV。在一些實施例中，配件在將頂級TLV發送至請求控制器之前將其加密。

配對ID特性1205可為用於配件之全域唯一識別符，諸如MAC位址、配件之公用金鑰之一部分、配件「使用者名稱」(例如，如下所述)或類似者。

在一些實施例中，特性1201至1205可藉由定義未配對控制器可見之配件配對服務執行個體而暴露於控制器，至少直至配件已與至少一個控制器建立配對的時間為止。舉例而言，在配件使用藍芽LE作為通信傳輸之執行個體中，配件可經由藍芽LE來廣告其配對服務。

除配對服務之外或替代配對服務，配件可定義控制器可參考以存取配對功能性的一或多個URL。舉例而言，參考上文之表4，控制器可發送對URL/對設置之HTTP POST請求，以作出請求且在對設置程序期間提供相關聯資訊。控制器可發送對URL/對驗證之HTTP POST請求，以作出請求且在對驗證程序期間提供相關聯資訊。控制器可發送對URL/配對之POST請求，以管理配對(例如，起始對新增及對移除程序或擷取用配件之已建立配對之清單)；POST請求可包括指示特定請求之資料物件。

現將描述用於建立配件與控制器之間的配對之程序(被稱作「對設置」)之實例。此等或其他程序中之任一者可(例如)在圖4之程序400之區塊428及430實施。因此，在下文中，假定配件及控制器已執行探索並開啟可能非安全之通信頻道。進一步假定使用者已經向控制器證實控制器應與特定配件配對。

在一些實施例中，僅當配件處於配對模式中時才准許對設置。使配件處配對模式中可涉及藉由使用者進行的與配件之實體接觸。舉例而言，可能需要使用者將實體物件(例如，鑰匙)插入至配件上之插座、將配件上之開關移動至「配對」位置或類似操作。在一些實施例中，

僅當配件不具有與任何控制器之建立配對時才准許對設置。一旦配件具有一個建立配對，即可使用如下所述之對新增程序(或其他委派配對程序)來建立額外配對。

圖13A至圖13C展示根據本發明之一實施例的用於控制器1302及配件1304的基於設置碼之對設置程序1300。在基於設置碼之對設置中，可需要使用者在控制器處鍵入配件之設置碼(其可為例如特定於彼配件且不容易猜測的八位數識別號碼)以提供雙向鑑認。出於安全性，配件之設置碼可由展示於顯示器上或由使用者手動地提供至配件(例如，藉由設定配件上之實體撥號盤或在小鍵盤中鍵入數字)，或設置碼印刷在配件外殼或包裝上或內的某處(例如，在不顯眼表面上之標籤上)。配件製造商可藉由不自公開可存取資訊(例如，序號、MAC位址、製造商名稱、生產日期等)衍生設置碼來增強安全性。在本文中之實例中，對設置充分利用安全遠端密碼(「SRP」)協定(記錄在http://srp.standford.edu)；然而，可使用其他協定。

首先參看圖13A，在區塊1306，控制器1302可查找相關聯使用者名稱(「userC」)。使用者名稱可包括控制器1302及/或控制器1302之授權使用者之任何識別符，其可由配件使用以幫助區分一個控制器與另一控制器。在區塊1308，控制器1302可發送對設置開始請求，例如對適當URL之HTTP POST請求。該對設置開始請求可包括用以指示對設置開始請求已發送的狀態指示符(在一些實施例中，此及後續狀態指標可由控制器寫入至圖12之配對狀態請求特性1201)、用以指示基於設置碼之配對方法在使用中的方法指示符及控制器使用者名稱userC。

在區塊1310，配件1304可判定是否節流該對設置開始請求。舉例而言，為了阻止基於隨機猜測之攻擊，配件1304可實施指數式節流，其中等待下一開始請求的時間在每一不成功對設置嘗試之後加倍(例如，若前面n次嘗試不成功，則第(n+1)次嘗試必須等待至少2^{n-1}秒)。該

節流可全域地而非每個工作階段或每個連接應用。節流時間可在成功對設置嘗試之後重置。因此，在區塊1310，若節流起作用且節流時間自上次嘗試起尚未過去，則在區塊1312，配件1304可發送一節流訊息。該節流訊息可指示控制器在重試之前需要等待多久。在區塊1314，若接收到節流訊息，則控制器1302可判定是否重試(在等待適當時間之後)。若控制器1302判定重試，則程序1300可返回至區塊1308以在適當等待時間之後發送新的對設置開始請求。

若在區塊1310，配件1304不節流該請求，則程序1300可進行至區塊1316，其中配件1304可建立SRP工作階段(例如，藉由調用適當SRP協定函數，諸如SRP_new(SRP6a_server_method()))；將控制器之使用者名稱設定為接收值userC（利用SRP_set_username或SRP_set_user_raw)；產生隨機salt（例如，至少16位元組)，其可用SRP_set_params來設定；選擇並設定其自身的設置碼(例如，使用SRP_set_auth_password或SRP_set_auth_password_raw)；且產生公用金鑰(「pkA」)(例如，使用SRP_gen_pub)。公用金鑰pkA可為在程序1300之持續時間中使用且接著被捨棄之短期金鑰對之部分(連同秘密金鑰「skA」)。

配件可使用各種技術來選擇設置碼。舉例而言，設置碼可預先程式化在EEPROM中(並印刷在配件上或標籤或類似者(使用者可在其中找到設置碼)上)。或者，在程序1300之前(或在該程序期間)，使用者選擇的設置碼可由使用者使用提供於配件上或中之機械或電子輸入器件鍵入至配件中。作為又一選項，配件可在執行對設置程序1300之每一執行個體期間產生隨機設置碼，限制條件為配件具有向使用者告知該設置碼(例如，藉由顯示該設置碼或以其他方式將該設置碼發信至使用者)的能力。亦可使用其他技術。

在區塊1318，配件1304可將隨機salt及公用金鑰pkA發送至控制器

1302，在區塊1320，該控制器可接收該隨機salt及該公用金鑰。在區塊1318發送隨機salt及公用金鑰後，配件1304隨即可更新配對狀態以指示配件之公用金鑰已發送。

在區塊1322，控制器1302可自使用者獲取配件之設置碼。舉例而言，控制器1302可呈現提示使用者鍵入配件之設置碼的使用者介面畫面。可使用其他技術，只要設置碼係在頻帶外(亦即，經由獨立於用以執行對設置程序之通信頻道的通信頻道)傳遞至控制器1302即可。舉例而言，在一些實施例中，使用者可操作控制器1302之機上攝影機以在設置碼出現在配件上時擷取設置碼之影像(該影像可包括人可讀表示或機器可讀表示，諸如條碼或快速回應(QR)碼或類似者)，且控制器1302可執行影像處理以提取該設置碼。可用以將設置碼自配件1304提供至控制器1302之技術的其他實例包括：當控制器1302實體接近配件1304置放或保持時，自配件1304至控制器1302之近場通信(NFC)傳輸；藉由可由控制器1302偵測到之配件1304進行的音波或超音波傳輸；高速光學發信(例如，由在控制器1302之攝影機或光偵測器之視野中的配件1304產生之光脈衝之序列)；或將配件1304或儲存設置碼之相關聯器件實體連接至控制器1302之連接器介面。

在區塊1324，控制器1302可建立SRP工作階段(例如，藉由調用適當SRP協定函數，諸如SRP_new(SRP6a_server_method()))；設定控制器之使用者名稱(利用SRP_set_username或SRP_set_user_raw)；設定自配件接收之salt (利用SRP_set_params)；產生其自身的公用金鑰(「pkC」)(例如，使用SRP_gen_pub)；使用使用者鍵入之設置碼來設定SRP密碼(例如，使用SRP_set_auth_password或SRP_set_auth_password_raw)；及計算共用秘密(「inputKey」) (例如，使用SRP_compute_key)。如同配件公用金鑰pkA，公用金鑰pkC可為在程序1300之持續時間中使用且接著被捨棄之短期金鑰對之部分(連同秘密金鑰「skC」)。

在區塊1326，控制器1302可產生控制器證明(「proofC」)以證明其自身身分識別(例如，使用SRP_respond)。在區塊1328，控制器1302可將驗證請求(包括公用金鑰pkC及證明proofC)發送至配件，例如作為對適當URL之HTTP POST請求。在區塊1328發送該請求後，控制器1302隨即可更新配對狀態以指示控制器之證明已發送。

在區塊1330，配件1304可驗證控制器證明proofC。舉例而言，配件1304可計算共用秘密(「inputKey」) (例如，使用SRP_compute_key)且使用該共用秘密來驗證proofC (例如，使用SRP_verify)。

如圖13B中所示，若在區塊1332，區塊1330處之驗證失敗，則在區塊1334，配件1304可將一錯誤訊息發送至控制器1302。若在區塊1336，控制器1302接收該錯誤訊息，則程序1300可在區塊1338結束。在一些實施例中，控制器可向使用者報告該錯誤。

若在區塊1332，驗證成功，則在區塊1340，配件1304可產生配件證明(「proofA」)以證明其自身身分識別(例如，使用SRP_respond)。在區塊1342，配件1304可將配件證明發送至控制器1302，在區塊1344，該控制器可接收proofA。在區塊1342發送proofA後，配件1304隨即可更新配對狀態以指示配件之證明已發送。

在區塊1346，控制器1302可驗證proofA (例如，使用SRP_verify)。若在區塊1348，驗證失敗，則程序1300可退出(區塊1350)。若在區塊1348，驗證成功，則配件及控制器現各自擁有經鑑認的共用秘密。

因此，在區塊1352，控制器1302可自該共用秘密inputKey產生新的加密金鑰(「Key」)。舉例而言，控制器1302可使用基於HMAC之金鑰衍生函數，其使用inputKey、隨機salt及額外資訊項目(其可預先程式化至控制器1302中)作為輸入來實施用於512位元雜湊(HMAC-SHA-512，定義於IETF RFC 2104中)的安全雜湊演算法版本2。在區塊1354，控制器1302可使用Key來加密其長期公用金鑰

(LTPKC)。該長期公用金鑰可為持久地儲存(例如，在如上所述之安全元件中)在控制器上的金鑰且與程序1300中較早所產生之短期公用金鑰無關。該加密可使用加密及鑑認演算法(諸如ChaCha20-Poly1305 (描述於可在https://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-03獲得之IETF Internet Draft draft-agl-tls-chacha20poly1305-03中)，其中Key作為金鑰、LTPKC作為訊息，及臨時亂數)，以產生加密資料edataC及鑑認標記authTagC。

在區塊1356，控制器1304可將edataC及authTagC發送至配件1304；控制器1302亦可更新配對狀態以指示LTPKC已發送至配件。

在區塊1358，在接收edataC及authTagC後，配件1302隨即可使用控制器1302在區塊1352處所使用的相同方法來產生加密金鑰(「Key」)。若全部已正確地進行至此點，則該加密金鑰應為同一Key。在區塊1360，配件1302可驗證接收的authTagC。

如圖13C中所示，若在區塊1362，區塊1360處之驗證失敗，則在區塊1364，配件1304可將一錯誤訊息發送至控制器1302。若在區塊1366，控制器1302接收該錯誤訊息，則程序1300可在區塊1368結束。在一些實施例中，控制器可向使用者報告錯誤。

若區塊1362導致成功，則在區塊1370，配件1304可解密LTPKC，且在區塊1372，配件1304可持久地儲存LTPKC及控制器之使用者名稱userC以作為配對控制器記錄。此儲存可在如上所述之安全元件中。

在區塊1374，配件1304可建置包括配件之長期公用金鑰(LTPKA)及與配件相關聯之使用者名稱的資料物件。配件之長期公用金鑰可為持久地儲存(例如，在配件1304之安全元件中)之金鑰且與在程序1300中較早所產生之短期公用金鑰pkA無關。如同控制器使用者名稱userC，配件使用者名稱userA可包括配件1304或配件1304之授權使用者之任何識別符，其可由控制器使用以幫助區分一個配件與另一配

件。在區塊1376，配件1304可加密在區塊1374所產生之資料物件以產生edataA及authTagA。可使用由控制器1302在區塊1354所使用之相同加密演算法。在區塊1378，配件1304可將edataA及authTagA發送至控制器1302;配件1304亦可更新配對狀態以指示LTPKA已發送至控制器。

在區塊1380，在接收edataA及authTagA後，控制器1302隨即可驗證接收的authTagA。

若在區塊1382，區塊1380處之驗證失敗，則在區塊1384，程序1300可結束，且控制器1304可向使用者報告該錯誤。若驗證成功，則在區塊1386，控制器1304可解密LTPKA且持久地儲存LTPKA及配件之使用者名稱userA以作為配對配件記錄。此儲存可在如上所述之安全元件中。在區塊1388，對設置完成，且配對狀態可經更新以指示該完成。

將瞭解，程序1300係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1300可結束，且控制器可通知使用者該錯誤。此外，對SRP及特定加密及/或鑑認演算法之參考係出於說明目的，且用於資料在非安全通信頻道上之安全交換的其他協定及演算法可取代。

在一些實施例中，配對程序可充分利用鑑認基礎結構。舉例而言，鑑認晶片(積體電路器件或IC)可併入至配件及/或控制器器件中。鑑認晶片可安全地儲存器件之加密金鑰、器件之安全性憑證及關於可由其他器件呈現之有效或無效安全性憑證的資訊。在一些實施例中，鑑認晶片可實施上文所述之安全元件(或其一部分)。在給定配件包括鑑認晶片的情況下，鑑認晶片可用於對設置程序中。

圖14A至圖14C展示根據本發明之一實施例的使用鑑認晶片的用

於控制器1402及配件1404之對設置程序1400之實例。假定在起始程序1400之前，控制器1402已確認配件1404具有鑑認晶片。舉例而言，上文所述之特徵旗標特性1202可包括指示配件是否支援基於憑證之配對的旗標。此可針對具有鑑認晶片之配件來設定。作為另一實例，指示配件是否支援基於憑證之配對的旗標可包括於配件之服務探索記錄之特徵旗標欄位(例如，表3中之Bonjour TXT記錄之特徵旗標「ff」欄位)中，此可使該旗標可更容易存取未配對控制器。(若缺少鑑認晶片之配件仍然設定此旗標，則控制器可在執行程序1400之正常過程中偵測鑑認晶片之不存在並報告錯誤)。

參看圖14A，在區塊1406，控制器1402可(例如)使用基於橢圓曲線Diffie-Hellman金鑰合約協定之Curve25519演算法(記錄於http://cr.yp.to/ecdh.html)來產生公用/秘密金鑰對(pkC, skC)。此金鑰對可為在程序1400之持續時間中使用且接著被捨棄之短期金鑰對。在區塊1408，控制器1402可將對設置開始請求發送至配件1404 (例如，作為對適當URL之HTTP POST請求)；該請求可包括公用金鑰pkC。該對設置開始請求可包括用以指示對設置開始請求已發送的狀態指示符(在一些實施例中，此及後續狀態指標可寫入至圖12之配對控制點特性1201)。

在區塊1410，回應於該對設置開始請求，配件1404可(例如)使用Curve25519演算法產生公用/秘密金鑰對(pkA, skA)。如同(pkC, skC)，此金鑰對可為在程序1400之持續時間中使用且接著被捨棄之短期金鑰對。儘管未圖示，但可併入上文參考程序1300所述之節流行，且若在不成功嘗試之後不久即接收對設置開始請求，則配件1404可拒絕該對設置開始請求。

在區塊1412，配件1404可使用skA及pkC產生共用秘密(「inputKey」)。在區塊1414，配件1404可藉由串連公用金鑰pkA及pkC

來建構一訊息，且在區塊1416，配件1404可使用其鑑認晶片來簽署該訊息以產生訊息「smsg」。該鑑認晶片可具有其自身的持久性金鑰對(獨立於pkA及skA)且可實施所要之任何演算法，諸如SHA-1或SHA-2 (由美國國家安全局(U.S. National Security Agency)設計之密碼編譯雜湊函數，記錄在聯邦資訊處理標準公開案180-4中)。

在區塊1418，配件1404可產生對稱金鑰(「Key」)。舉例而言，配件1404可使用將inputKey、salt (例如，預定義字串)及額外資訊用作輸入的HMAC-SHA-512。

在區塊1420，配件1404可使用在區塊1418所產生之金鑰Key來加密來自區塊1416之已簽署訊息smsg以產生證明「proofA」。可使用任何對稱加密演算法。

在區塊1422，配件1404可將回應發送至控制器1402。該回應可包括公用金鑰pkA、配件證明proofA及由鑑認晶片供給之配件憑證。在區塊1422發送該回應後，配件1404隨即可更新配對狀態以指示配件之證明已發送。

在區塊1424，控制器1402可驗證配件憑證。舉例而言，控制器1402可具有其自身的鑑認晶片或儲存識別有效配件憑證之資訊的其他安全資料儲存器；該資訊可提供至控制器1402且在一些情況下由受信任憑證授權單位來更新。控制器1402可使用此資訊來確認接收的配件憑證有效。在一些實施例中，某些憑證可能僅針對某些類別之配件有效，且控制器1402可使用先前自配件接收之資訊(例如，配件定義記錄或在如上所述之器件探索期間提供之其他資訊)來判定配件之類別及接收的配件憑證針對配件之類別是否有效。

參看圖14B，在區塊1426，若配件憑證無效，則程序1400可終止(區塊1428)，且控制器1402可向使用者告知該錯誤。若配件憑證有效，則在區塊1430，控制器1402可使用skC及pkA產生共用秘密

(「inputKey」)。在區塊1432，控制器1402可產生對稱金鑰(「Key」)。舉例而言，配件1404可使用將inputKey、salt (例如，預定義字串)及額外資訊用作輸入的HMAC-SHA-512。在區塊1434，控制器1404可使用對稱金鑰Key以使用由配件1404用以加密proofA之相同演算法來解密自配件接收之proofA。控制器1402因此獲得已簽署訊息smsg。在區塊1436，控制器1402可使用配件憑證來驗證smsg上之簽章。在區塊1438，若簽章無效，則程序1400可終止(區塊1440)，且控制器1402可向使用者告知該錯誤。

參看圖14C，若簽章有效，則在區塊1442，控制器1402可用控制器使用者名稱「userC」及控制器之長期公用金鑰LTPKC來建置資料物件(其可與上文所述之程序1300中相同)。在區塊1444，控制器1402可加密該資料物件以產生edataC及authTagC。類似於上文所述之程序1300，區塊1442處之加密可使用加密及鑑認演算法(諸如ChaCha20-Poly1305，其中Key作為金鑰、LTPKC作為該訊息，及臨時亂數)。在區塊1446，控制器1402可將包括edataC及authTagC之交換請求訊息發送至配件1404；控制器1402亦可更新配對狀態以指示LTPKC已發送至配件。

在區塊1448，配件1404可使用其對稱金鑰Key來驗證接收的authTagC。若在區塊1450，區塊1448處之驗證失敗，則在區塊1452，配件1404可將一錯誤訊息發送至控制器1402。若在區塊1454，控制器1402接收該錯誤訊息，則程序1400可在區塊1456結束。在一些實施例中，控制器可向使用者報告該錯誤。

若區塊1450導致成功，則在區塊1458，配件1404可解密LTPKC，且在區塊1460，配件1404可持久地儲存LTPKC及控制器之使用者名稱userC以作為配對控制器記錄。此儲存可在上文所述之安全元件中。

在區塊1462，配件1404可建置一資料物件，該資料物件包括配件

之長期公用金鑰(LTPKA)及與配件相關聯之使用者名稱(userA)，該兩者可與上文所述之程序1300中的相同。配件之長期公用/秘密金鑰對可不同於配件之鑑認晶片中的金鑰對。在區塊1464，配件1404可加密在區塊1462所產生之資料物件以產生edataA及authTagA。可使用由控制器1402在區塊1444所使用之相同加密演算法。在區塊1466，配件1404可將edataA及authTagA發送至控制器1402；配件1404亦可更新配對狀態以指示LTPKA已發送至控制器。

在區塊1468，在接收edataA及authTagA後，控制器1402隨即可使用先前所產生之金鑰Key來驗證接收的authTagA。

若在區塊1470，區塊1468處之驗證失敗，則在區塊1472，程序1400可結束，且控制器1402可向使用者報告該錯誤。若驗證成功，則在區塊1474，控制器1402可解密LTPKA並持久地儲存LTPKA及配件之使用者名稱userA以作為配對配件記錄(此儲存可在上文所述之安全元件中)。在區塊1476，對設置完成，且配對狀態可經更新以指示該完成。

應瞭解，程序1400係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1400可結束，且控制器可通知使用者該錯誤。此外，對特定加密及/或鑑認演算法之參考係出於說明目的，且用於資料在非安全通信頻道上之安全交換的其他協定及演算法可取代。

如所描述之程序1400係不對稱的，此係因為配件將憑證發送至控制器以用於驗證，但控制器並不將對應憑證發送至配件。在一些實施例中，可實施雙向憑證驗證。舉例而言，具有憑證之控制器可實施類似於區塊1412至1416之處理以產生控制器證明(「proofC」)，該控制器

證明可與控制器憑證一起發送至配件。配件可實施類似於區塊1424至1436之處理以驗證控制器之證明。

在一些實施例中，鑑認晶片可特定於特定器件，且每一器件可具有唯一憑證。在其他實施例中，同一類別中之配件(或控制器)可具有相同鑑認晶片且因此具有相同憑證。在如此情況下，防止設置期間的中間人攻擊(man-in-the-middle attack)可減少；然而，一旦長期公用金鑰經交換，此等金鑰即可可靠地用於後續對驗證期間的雙向鑑認。

其他技術可用以進一步減少中間人攻擊或其他惡意探索之風險。舉例而言，若對設置程序中之兩種器件中之一者(或兩者)具有可偵測另一器件有多接近之接近性感測器(例如，使用藍芽LE或NFC)，則具有該感測器之器件可在另一器件不緊密附近或不保持緊密附近(例如，在幾吋內)的情況下中止該對設置程序。此可減少中間人攻擊之可能性，此係因為進攻器件將需要實體上接近該程序中之意欲參與者—使用者將可能要注意的情形。

一些實施例可將安全性憑證及基於設置碼之配對兩者併入至對設置程序中。圖15A至圖15F展示根據本發明之一實施例的使用安全性憑證及設置碼的用於控制器1502及配件1504的對設置程序1500之實例。程序1500可併有上文所述之程序1300及1400之特徵。

首先參看圖15A，在區塊1506，控制器1502可將啟動請求發送至配件1504以開始對設置程序。舉例而言，控制器1502可發送對配件1504之/pair-setup URL之HTTP POST請求。該POST請求可包括指示所要配對狀態(例如，「start pair setup」)的TLV資料物件及指示是否將使用設置碼及/或憑證的方法識別符。在區塊1508，配件1504可接收該啟動請求且可相應地設定當前配對狀態。在區塊1510，配件1504可阻斷可能存在之任何其他控制器起始對設置。舉例而言，若開始對設置之請求係在區塊1510之後接收，則配件可傳回錯誤回應(例如，HTTP 429「Too

Many Requests」訊息)。配件1504可繼續以此方式阻斷對設置請求，直至程序1500完成(或由於錯誤而終止)。

在一些實施例中，配件1504可全域地或基於每個控制器而將不成功對設置嘗試之數目限於最大嘗試數目。舉例而言，配件1504可定義一極限(例如，5次嘗試、10次嘗試，或某一其他極限)且維持不成功嘗試之計數器。若該計數器達到或超過該極限，則在區塊1512，配件可拒絕該請求，且程序1500可在區塊1514退出。在一些實施例中，配件1504可將指示錯誤之原因(例如，太多次嘗試)之錯誤回應發送至控制器1502。或者，可使用節流技術(例如，參看圖13A如上所述)或其他技術來防止藉由未授權控制器來執行對設置之蠻力嘗試。

假定尚未超過嘗試之最大數目，則在區塊1516，配件1504可開始對設置。舉例而言，配件1504可建立SRP工作階段(例如，藉由調用適當協定函數，諸如SRP_new(SRP6a_server_method()))；設定該工作階段之SRP使用者名稱(例如，利用SRP_set_username、使用可為一般之固定字串作為使用者名稱)；產生隨機salt (例如，至少16位元組)，其可用SRP_set_params來設定；且選擇(例如，擷取)待設定之設置碼作為SRP密碼(例如，使用SRP_set_auth_password或SRP_set_auth_password_raw)。

類似於程序1300，配件1504可使用各種技術來選擇設置碼，包括自EEPROM讀取碼、自使用者接收碼、產生隨機碼(例如，在程序1500之執行期間)或類似者。在區塊1518，配件1504可呈現設置碼給使用者。舉例而言，視配件及設置碼而定，該碼可印刷在附接至配件1504之標籤或其包裝上、呈現在配件1504之顯示器上或類似者。在一些情況下，並非呈現設置碼給使用者，配件1504可使用獨立於用於對設置程序1500之頻道的通信頻道(諸如NFC頻道或具有極短程射程(例如，小於50 cm)之其他發信頻道)將該碼傳遞至控制器1502。

在區塊1520，配件1504可產生公用金鑰(「pkA」) (例如，使用SRP_gen_pub)。公用金鑰pkA可為在程序1500之持續時間中使用且接著被捨棄之短期金鑰對之部分(連同秘密金鑰「skA」)。

在區塊1522，配件1504可(例如)使用HTTP回應訊息發送對啟動請求之回應。該回應可包括公用金鑰pkA及隨機salt。在區塊1522發送回應後，配件104隨即可更新當前配對狀態以指示配件之公用金鑰已發送。

在區塊1524，控制器1502可接收對該啟動請求之回應。在區塊1526，控制器1502可自使用者獲取設置碼。舉例而言，控制器1502可呈現提示使用者鍵入配件之設置碼的使用者介面畫面。如同上文所述之程序1300之區塊1322，可使用其他技術，只要設置碼係在頻帶外(亦即，經由獨立於用以執行對設置程序之通信頻道的通信頻道)傳遞至控制器1502即可。視所使用之特定技術而定，由控制器獲取設置碼可併入某一形式之使用者活動(例如，鍵入該碼、使控制器保持接近配件、操作控制器之攝影機等)，且除提供器件之身分識別的頻帶外確認之外，此活動亦可充當使用者意欲建立控制器1502與配件1504之間的配對的確認。

參看圖15B，在區塊1528，控制器1502可建立SRP工作階段(例如，藉由調用適當SRP協定函數，諸如SRP_new(SRP6a_server_method()))；設定SRP使用者名稱(例如，利用SRP_set_username、使用可為一般之固定字串作為使用者名稱)；將salt設定為自配件接收之salt (利用SRP_set_params)；產生控制器自身之公用金鑰(「pkC」) (例如，使用SRP_gen_pub)；及使用在區塊1526所獲取之設置碼來設定SRP密碼(例如，使用SRP_set_auth_password或SRP_set_auth_password_raw)。如同配件公用金鑰pkA，公用金鑰pkC可為在程序1500之持續時間中使用且接著被捨棄之短期金鑰對之部分(連同秘密金鑰「skC」)。在區塊1530，

控制器1502可計算共用秘密(「inputKey」)(例如，使用SRP_compute_key)。在區塊1532，控制器1502可產生其具有共用秘密inputKey的證明(「proofC」)(例如，使用SRP_Respond)。。

在區塊1534，控制器1502可將驗證請求發送至配件1504。舉例而言，控制器1502可發送對配件1504之/pair-setup URL之HTTP POST請求。該POST請求可包括指示所要配對狀態(例如，「驗證對設置」)的TLV資料物件、控制器之公用金鑰pkC及控制器證明proofC。

在區塊1536，配件1504可接收驗證請求。在區塊1538，配件1504可計算共用秘密(「inputKey」)(例如，使用SRP_compute_key)；此應匹配由控制器1502在區塊1530所計算之共用秘密。

在區塊1540，配件1504可使用在區塊1538所計算之共用秘密來驗證控制器證明proofC (例如，使用SRP_verify)。儘管圖15B中未圖示，但若驗證失敗，則配件1504可終止程序1500且將一錯誤訊息發送至控制器1502。(如在本文中所描述之其他配對程序中，控制器1502可向使用者報告該錯誤)。

假定proofC經驗證，則在區塊1542，配件1504可產生配件證明(「proofA」)以證明該配件擁有共用秘密(例如，使用SRP_respond)。在區塊1544，配件1504可自共用秘密衍生工作階段加密金鑰(eKey)。舉例而言，配件1504可使用基於HKDF之金鑰衍生功能，其使用inputKey、salt及額外資訊作為輸入來實施用於512位元雜湊(HKDF-SHA-512，定義於IETF RFC 6234中)的安全雜湊演算法版本2。

參看圖15C，在此實例中假定配件1504具有由受信任憑證授權單位頒佈之安全性憑證。在一些實施例中，憑證可併入至如上參看圖14A至圖14C所述之鑑認晶片中。在情況如此的情況下，配件1504可使用其憑證向控制器1502進一步鑑認其身分識別。在一些實施例中，由控制器1502在區塊1506所發送之啟動請求或由控制器1502在區塊1534所

發送之驗證請求可包括配件是否應用憑證來鑑認的指示。

在配件1504用憑證進行鑑認的情況下，在區塊1546，配件1504可自在區塊1538所計算之共用秘密(inputKey)產生待簽署之查問(challenge)。舉例而言，該查問可藉由應用使用inputKey、salt及額外資訊項目作為輸入的金鑰衍生函數(諸如HKDF-SHA-512)而產生。salt及額外資訊項目可具有可作為其作業系統或韌體之部分程式化至配件1504中之預定義值。在區塊1548，配件1504可使用其憑證來簽署該查問。舉例而言，若配件1504包括鑑認晶片，則該鑑認晶片可簽署該查問。如上所述，鑑認晶片可具有其自身的持久性金鑰對(獨立於pkA及skA或LTPKA及LTSKA)且可實施所要的任何簽章演算法，諸如SHA-1。

在區塊1550，配件1504可建置包括可自鑑認晶片擷取之已簽署查問及配件憑證的資料結構。在區塊1552，配件1504可使用在區塊1544所產生之加密金鑰(eKey)來加密在區塊1550所建置之資料結構。可使用任何對稱加密演算法，諸如ChaCha20-Poly1305 AEAD演算法。加密演算法可產生加密資料結構及標記(authTagA)。

在區塊1554，配件1504可將驗證回應發送至控制器1502。驗證回應可包括在區塊1542所產生之配件證明proofA以及在區塊1550所產生之加密資料結構及authTagA。如上文所指出，在一些實施例中，可選擇性地執行或不執行基於憑證之鑑認(例如，視控制器1502是否請求基於憑證之鑑認而定)。在不執行基於憑證之鑑認的情況下，驗證回應可省略加密資料結構及authTagA。

在區塊1556，控制器1502可自配件1504接收驗證回應。在區塊1558，控制器1502可驗證配件證明proofA (例如，使用SRP_verify)。若驗證失敗，則程序1500可以錯誤終止。假定驗證成功，則在區塊1560，控制器1502可自在區塊1530所計算之共用秘密(inputKey)衍生加密金鑰(eKey)。控制器1502可使用配件1504在區塊1544所使用之相同金鑰

衍生演算法及輸入，在區塊1560所衍生之eKey預期匹配由配件在區塊1544所產生之eKey。

在區塊1562，控制器1502可驗證接收的authTagA，且在區塊1564，控制器1502可解密接收的資料結構。

現參看圖15D，在區塊1566，控制器1502可驗證自經解密資料結構提取之配件憑證。舉例而言，如上所述，控制器1502可具有其自身的鑑認晶片或儲存識別有效配件憑證之資訊的其他安全資料儲存器；該資訊可提供且在一些情況下由受信任憑證授權單位來更新。或者，控制器1502可能能夠即時地與受信任憑證授權單位通信以驗證接收的憑證。控制器1502可使用來自憑證授權單位之資訊(區域地快取的抑或即時地獲得的)來確認配件憑證係有效的。在一些實施例中，某些憑證可能僅針對某些類別之配件有效，且控制器1502可使用先前自配件接收之資訊(例如，如上所述在器件探索期間提供之資訊)來判定配件之類別及配件憑證針對該配件之類別是否有效。若憑證無效，則程序1500可以錯誤終止。

假定憑證有效，則在區塊1568，控制器1502可自共用秘密inputKey產生查問。控制器1502可使用配件1504在區塊1546所使用之相同演算法及輸入(例如，inputKey及預定義salt及額外資訊項目)，結果為控制器1502及配件1504兩者應產生相同查問。利用此技術，控制器1502未必需要將查問無阻礙地(in the clear)發送至配件1504。此外，在查問併有共用秘密inputKey之情況下，冒名頂替者可難以猜測該查問。在區塊1570，控制器1502可使用來自配件憑證之公用金鑰來驗證已簽署查問。若驗證失敗，則程序1500可以錯誤終止。

假定驗證成功，則控制器現準備與配件交換長期公用金鑰。在區塊1572，控制器1502可產生一LTPKC訊息，其串連共用秘密之表示(例如，具有salt及額外資訊項目之共用秘密的HDKF-SHA-512，其可具有

可程式化至控制器1502中以作為其作業系統或韌體之部分的預定義值)、控制器之長期公用金鑰(LTPKC)及控制器之識別符。在一些實施例中，控制器具有可在區塊1572使用之預定義(LTPKC, LTSKC)金鑰對；在其他實施例中，(LTPKC, LTSKC)金鑰對可在區塊1572產生。在區塊1574，控制器1502可使用其長期秘密金鑰(LTSKC)來簽署該LTPKC訊息，例如藉由將諸如Ed25519 (記錄在http://ed25519.cr.yp.to)之簽章演算法應用於該訊息。在區塊1576，控制器1502可建置包括來自該LTPKC訊息之簽章、LTPKC及控制器之ID的資料結構。(該LTPKC訊息本身可自此資料結構省略，此係因為配件1504將能夠重建構該訊息)。在區塊1578，控制器1502可使用在區塊1560所衍生之加密金鑰eKey來加密該資料結構及產生鑑認標記(authTagC)。

在區塊1580，控制器1502可將金鑰交換請求發送至配件。舉例而言，控制器1502可發送對配件1504之/pair-setup URL之HTTP POST請求。金鑰交換請求可包括在區塊1578所產生之加密資料結構及鑑認標記。在區塊1582，配件1504可自控制器1502接收金鑰交換請求。

現參看圖15E，在區塊1584，配件1504可驗證接收的鑑認標記。在區塊1586，配件1504可解密資料結構，且在區塊1588，配件1504可驗證含於資料結構中之簽章。若驗證中之任一者失敗，則程序1500可以錯誤終止。

假定鑑認標記及簽章經驗證，則在區塊1590，配件1504可持久地儲存自資料結構提取之LTPKC及控制器ID以作為配對控制器記錄。此儲存可在上文所述之安全元件中。

配件1504可以類似方式將其自身的長期公用金鑰(LTPKA)發送至控制器1502。舉例而言，在區塊1592，配件1504可產生一LTPKA訊息，其串連共用秘密之表示(例如，具有salt及額外資訊項目之共用秘密的HDKF-SHA-512，其可具有程式化至配件之系統軟體或韌體中的預定

義值)、配件之長期公用金鑰(LTPKA)及配件之識別符。在一些實施例中，配件具有可在區塊1592使用之預定義(LTPKA, LTSKA)金鑰對；在其他實施例中，(LTPKA, LTSKA)金鑰對可在區塊1592產生。在區塊1594，配件1504可使用其長期秘密金鑰(LTSKA)來簽署LTPKA訊息，例如藉由將諸如Ed25519之簽章演算法應用於LTPKA訊息。在區塊1596，配件1504可建置包括來自LTPKA訊息之簽章、LTPKA及配件之ID的資料結構。(該LTPKA訊息本身可自此資料結構省略，此係因為配件1502將能夠重建構該訊息)。在區塊1598，配件1504可使用在區塊1544所衍生之加密金鑰eKey來加密該資料結構及產生鑑認標記(authTagB)。

在區塊1501，配件1504可將金鑰交換回應發送至控制器1502。該金鑰回應可包括在區塊1598所產生之加密資料結構及鑑認標記。在區塊1503，控制器1502可接收金鑰交換回應。

現參看圖15F，在區塊1505，控制器1502可驗證接收的鑑認標記。在區塊1507，控制器1502可解密資料結構，且在區塊1509，控制器1502可驗證含於資料結構中之簽章。若驗證中之任一者失敗，則程序1500可以錯誤終止。

假定鑑認標記及簽章經驗證，則在區塊1511，控制器1502可持久地儲存自資料結構提取之LTPKA及配件ID以作為配對配件記錄。此儲存可在如上所述之安全元件中。

在區塊1513，對設置完成，且配對狀態可經更新以指示該完成。

將瞭解，程序1500係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1500可結束，且控制器

可通知使用者該錯誤。此外，對特定加密及/或鑑認演算法之參考係出於說明目的，且用於資料在非安全通信頻道上之安全交換的其他協定及演算法可取代。

如所描述之程序1500係不對稱的，此係因為配件將憑證發送至控制器以用於驗證，但控制器並不將對應憑證發送至配件。在一些實施例中，可實施雙向憑證驗證。舉例而言，具有憑證之控制器可實施類似於區塊1546至1552之處理以產生查問以產生查問且使用控制器憑證簽署該查問，已簽署查問可與控制器憑證一起發送至配件。配件可實施類似於區塊1566至1570之處理以驗證控制器之證明。

在一些實施例中，給定配件或控制器可支援對設置程序1300、1400、1500 (及/或未特定地描述之其他程序)中之任一者或全部，且待使用之對設置程序可基於每個配對而選擇。為了統一，控制器可支援多個對設置程序(例如，具有及不具憑證)且可基於給定配件支援哪個(哪些)程序而選擇用於該配件之程序。程序可經指派一偏好次序(例如，基於所提供之相對安全性)，且控制器可選擇給定配件支援之最佳程序。控制器可(例如)藉由將程序識別符包括於啟動請求訊息中來規定待使用之程序。

對設置之更一般視圖可參看圖16來獲得，圖16展示根據本發明之一實施例的控制器1602與配件1604之間的一般化對設置程序1600。對設置程序1600可由控制器1602在區塊1606起始。舉例而言，如上所述，控制器1602可執行程序400 (經由區塊426)以識別應對其執行對設置之配件(例如，配件1604)。控制器1602可將一訊息發送至配件1604 (例如，對適當URL之POST請求)，使得配件1604亦可在區塊1608開始對設置。

在區塊1610及1612，配件1604及控制器1602可建立共用秘密(例如，上文所述之程序1300、1400及1500中之inputKey)。建立共用秘密

可包括雙向資訊交換。舉例而言，在程序1300中，配件提供salt及短期公用金鑰，且控制器提供其短期公用金鑰。在程序1400及1500中，配件提供其短期公用金鑰及憑證，且控制器提供其短期公用金鑰。在一些實施例中，共用秘密亦可併有預先程式化至兩個器件(例如，在安全元件內或在別處)中之其他資訊。共用秘密亦可併有頻帶外資訊，其可提供控制器經授權(例如，由使用者)以與配件相互操作之證據。舉例而言，在程序1300或程序1500中，配件之設置碼係由控制器及配件使用以建構共用秘密。如上所述，配件之設置碼可在頻帶外(亦即，使用除用以發送及接收證明之頻道外的通信頻道)提供至控制器。頻帶外頻道之實例可包括使用者輸入(例如，使用者可在控制器之使用者介面處鍵入配件之設置碼、使用控制器之攝影機拍攝設置碼之照片)、近場通信頻道、光學發信頻道、有線電子發信頻道、音訊(例如，超音波)頻道等。在一些情況下，頻帶外頻道可併有使用者介入(例如，鍵入設置碼、使控制器保持近場接近配件、拍攝照片、插入連接器中)，且經由頻帶外頻道傳達設置碼之事實可充當使用者贊成建立配對之指示。

在區塊1614，控制器1602可產生一證明並將該證明發送至配件1604。該證明可為向配件1604表明控制器1602擁有共用秘密的任何資訊段(例如，加密訊息，諸如上文之標記為「proofC」的訊息)。

在區塊1616，配件1604可接收控制器之證明，且在區塊1618，配件1604可基於其區域產生的共用秘密之複本來驗證該證明。若共用秘密不匹配，則控制器之證明將未經驗證，且程序1600可以錯誤終止。應注意，在設置碼係用以產生共用秘密之情況下，區塊1618處之驗證亦可充當配件對控制器之鑑認。

假定該證明經驗證，則在區塊1620，配件1604可產生其自身證明並將該證明發送至控制器1602，以顯示配件1604亦擁有共用秘密。配件證明可為(例如)不同於控制器之證明的加密訊息，其亦併有共用秘

密(如在程序1300及1500中)。在一些實施例中，可併入配件之身分識別的其他證明；舉例而言，在程序1400及1500中，配件可使用確認配件之身分識別的至少一些態樣之憑證來簽署一訊息。

在區塊1624，控制器可驗證接收的證明。類似於區塊1618，若共用秘密不匹配，則配件之證明將未經驗證，且程序1600可以錯誤終止。應注意，在設置碼係用以產生共用秘密之情況下，區塊1624處之驗證亦可充當控制器對配件之鑑認。可提供進一步鑑認，例如在配件證明併有使用憑證簽署之訊息的情況下(如在程序1400及1500中)。

假定證明在區塊1624經驗證，則兩個器件可被視為彼此經鑑認，且共用秘密可用以交換額外資訊(諸如上文所述之長期公用金鑰)以建立(持久性)配對。舉例而言，在區塊1626，控制器1602可發送其長期公用金鑰(LTPKC)。LTPKC可以加密形式發送，例如使用自共用秘密衍生之金鑰(如在程序1300、1400及1500中)。在區塊1628，配件1604可接收並持久地儲存LTPKC (例如，在如上所述之安全元件中)。在區塊1630，配件1604可發送其長期公用金鑰(LTPKA)。LTPKA亦可以加密形式發送，例如使用自共用秘密衍生之金鑰(如在程序1300、1400及1500中)。在區塊1632，控制器1602可接收並持久地儲存LTPKA (例如，在如上所述之安全元件中)。此後，對設置完成(區塊1634)，此係因為每一器件現具有建立與另一者之配對的經鑑認、持久儲存之記錄。

將瞭解，程序1600係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，證明可以任何次序(先配件或先控制器)進行交換，且長期公用金鑰亦可以任何次序進行交換。

應注意，長期公用金鑰在本文中被稱為「公用」以指示：不同於私人(或秘密)金鑰，該等長期公用金鑰可提供至其他器件。然而，如程序1300、1400、1500、1600中所示，在共用秘密已使用其他資訊(例

如，設置碼)建立之後，對設置可允許該等器件交換加密形式之長期公用金鑰。在一些實施例中，長期公用金鑰之解密及儲存可在接收器件中之安全計算元件內發生，且此可進一步防止長期公用金鑰暴露於未授權器件。此可使未授權器件偽造對設置記錄變得相當更加困難。此安全性等級允許對設置記錄在器件重新連接時用於更簡單的對驗證程序，如下所述。

經由上文所述之對設置程序中之任一者建立的配對可為持久狀態，此係因為配件及控制器可將其接收的長期公用金鑰儲存在持久性儲存器(例如，非揮發性記憶體、磁碟或類似者)中；持久性儲存器可在安全元件中。在一些實施例中，一旦配件已執行與一個控制器之對設置，該配件即可防止任何其他控制器執行對設置，例如藉由對任何接收的起始對設置之請求回應以一錯誤訊息。已與配件執行對設置之控制器可經指定為彼配件之「管理員」且可允許指示該配件(例如)使用如下所述之對新增程序與其他控制器建立配對。

在一些實施例中，配件可同時已與多個控制器建立配對；每一配對可使用對設置、對新增(描述如下)或類似者來建立。舉例而言，配件可持久地儲存包括已建立配對之每一控制器之識別符及相關聯LTPKC的查找表或其他資料結構。資料結構亦可包括關於控制器之其他資訊。舉例而言，不同控制器可被授予對配件的不同程度控制(被稱作權限)，且由配件維持之資料結構可包括規定每一控制器具有哪些權限之指示符(例如，旗標)。可定義各種權限。可定義之一個權限為「管理員」權限，且且在一些實施例中，僅具有管理員權限之控制器才可將其他控制器之配對記錄新增至配件(例如，使用如下所述之對新增程序)。在一些實施例中，成功地執行對設置之控制器可被自動授予管理員權限。其他控制器可在對新增(例如，如下所述)期間選擇性地被授予管理員權限。

類似地，控制器可同時已與多個配件建立配對。舉例而言，控制器可執行關於多個配件之對設置，或在一些情況下，控制器可經由如下所述之對程序程序來新增與配件之配對。控制器可持久地儲存包括每一配件(控制器已與每一配件建立配對)之識別符及相關聯LTPKA的查找表或其他資料結構。資料結構亦可包括諸如控制器針對彼配件具有哪些權限之資訊。

預期已建立配對之控制器及配件在此後可不保持彼此之恆定通信。舉例而言，配件或控制器可斷電，或一個器件可移動到另一器件之範圍外。當已彼此建立配對之控制器及配件返回至通信狀態而非再次執行對設置時，該等器件可使用不同程序(在本文中被稱作對驗證)來驗證先前建立之配對的存在。對驗證可使用先前所建立並儲存(例如，在對設置或對新增期間)之長期公用金鑰。對驗證程序亦可產生可用以加密後續訊息之新的共用秘密及/或工作階段金鑰，只要該等器件保持在對驗證狀態中即可。對驗證狀態(在本文中亦被稱作對驗證工作階段)可藉由任一器件來終止，例如藉由刪除器件自身的工作階段金鑰之複本，此將使器件不能解密來自另一器件之其他訊息。在一些實施例中，對驗證可在每當控制器嘗試開啟一頻道以用於與一配件(控制器具有與該配件之已建立配對)之統一配件協定通信時執行。

圖17A至圖17C展示根據本發明之一實施例的控制器1702與配件1704之間的對驗證程序1700之實例。程序1700可在控制器1702判定對驗證係適當動作時(例如，當控制器1702接收用以控制配件1704上之某一操作的使用者指令且對驗證工作階段當前不存在於控制器1702與配件1704之間時，或當控制器1702與配件1704重新連接時)開始。

參看圖17A，在區塊1706，控制器1704可(例如)使用如上所述之Curve25519演算法產生新的短期金鑰對(pkC, skC)。在區塊1708，控制器1704可將對驗證開始請求發送至配件1704；該請求可包括短期公用

金鑰pkC (且視情況包括額外資訊，諸如在配對建立時提供至配件1704之控制器ID或控制器使用者名稱userC)。在一些實施例中，該對驗證開始請求可作為對配件之/pair-verify URL之HTTP POST請求而發送。在一些實施例中，狀態指示符可寫入至圖12之配對狀態請求特性1201以指示控制器1704已請求對驗證開始狀態。

在區塊1710，配件1704可接收該對驗證開始請求且可在配對控制器之清單中查找長期公用金鑰(LTPKC)。在一些實施例中，該查找可在安全元件內執行，且配件1704之其他邏輯組件可僅知道該查找是否成功。如上所述，關聯控制器ID (或使用者名稱userC)與LTPKC之配對記錄可在配對建立時持久地儲存，因此區塊1710可允許配件1704判定是否已經與控制器1702建立配對。

在區塊1712，若與控制器1702之配對尚未建立，則配件1704可在區塊1714發送一錯誤訊息。若在區塊1716，控制器1702接收該錯誤訊息，則程序1700可在區塊1718結束，且控制器1702可向使用者報告該錯誤。

若配件1704判定其具有與控制器1702之已建立配對，則在區塊1720，配件1704可(例如)使用Curve25519演算法產生短期公用/秘密金鑰對(pkA, skA)。在區塊1722，配件1704可使用skA及pkC產生共用秘密(「inputKey」)。在區塊1724，配件1704可衍生對稱金鑰(「Key」)。舉例而言，配件1704可使用HDKF-SHA-512，其使用inputKey、salt (例如，預定義字串，其可不同於對設置中所使用之salt)及額外資訊作為輸入。

在區塊1726，配件1704可產生並簽署一配件資訊訊息。舉例而言，配件1704可串連pkA及pkC，且用配件之長期秘密金鑰(LTSKA)來簽署該串連。亦可串連額外資訊，諸如配件ID。在區塊1728，配件1704可使用對稱金鑰Key來加密已簽署訊息以產生配件證明(proofA)及鑑

認標記(authTagA)。在區塊1730，配件1704可將一對驗證開始回應發送至控制器1702。該回應可包括proofA、鑑認標記及短期公用金鑰pkA。亦可包括其他資訊，諸如配件識別符或使用者名稱(「userA」，其可為在配對建立時給予控制器之配件名稱)。在區塊1730發送該回應後，配件1704隨即可更新配對狀態以指示配件之證明已發送。

在區塊1732，在接收該回應之後，控制器1702可(例如)基於配件ID或配件使用者名稱而在其配對配件之清單中查找長期公用金鑰(LTPKA)。在一些實施例中，該查找可在安全元件內執行，且控制器1702之其他邏輯組件可僅知道該查找是否成功。如上所述，關聯配件ID (或使用者名稱userA)與LTPKA之配對記錄可在配對建立時持久地儲存，因此區塊1732可允許控制器1702判定是否已經與配件1704建立配對。

參看圖17B，在區塊1734，若與配件1704之配對尚未建立，則程序1700可在區塊1736結束，且控制器1702可向使用者報告該錯誤。在一些實施例中，控制器1702可在開始程序1700之前判定控制器是否具有指示與配件1704之已建立配對之儲存記錄，且可省略區塊1734處之額外檢查。

若控制器1702判定其具有與配件1704之已建立配對，則在區塊1738，控制器1702可使用skC及pkA產生共用秘密(「inputKey」)。在區塊1740，控制器1702可衍生對稱金鑰(「Key」)。舉例而言，控制器1702可使用HDKF-SHA-512，其使用inputKey、salt及額外資訊項目作為輸入。在一些實施例中，salt及額外資訊項目可具有不同於在對設置期間所使用之預定義值的預定義值。若無錯誤已發生，則區塊1740處所衍生之Key應匹配由配件1704在區塊1724所衍生之Key。

在區塊1742，控制器1702可使用對稱金鑰Key來解密接收的proofA且亦可驗證authTagA。在區塊1744，控制器1702可驗證已簽署

配件上的配件之簽章-自proofA提取之資訊訊息。此驗證可使用來自與配件1704之已建立配對的儲存LTPKA。若成功，則此驗證確認配件1704係先前提供LTPKA之同一配件(假定沒有其他配件可具有相同的長期金鑰對)。在區塊1746，若authTagA或該簽章未經驗證(或若解密失敗)，則程序1700可在區塊1748結束，且控制器1702可向使用者報告該錯誤。

參看圖17C，若區塊1746處之驗證成功，則在區塊1750，控制器1702可產生並簽署一控制器資訊訊息。舉例而言，控制器1702可串連pkC及pkA (在此實例中之次序與區塊1724處之串連相反)並用控制器之長期秘密金鑰簽署該串連。亦可串連額外資訊，諸如控制器ID。在區塊1752，控制器1702可使用對稱金鑰Key來加密該已簽署訊息以產生控制器證明(proofC)及鑑認標記(authTagC)。在區塊1754，控制器1702可將一驗證完成請求發送至配件1704。該請求可包括proofC及authTagC。在區塊1754發送該請求後，控制器1702隨即可更新配對狀態以指示控制器之證明已發送。

在區塊1756，配件1704可接收該驗證完成請求且可使用對稱金鑰Key來解密接收的proofC並驗證authTagC。在區塊1758，配件1704可驗證已簽署控制器上之控制器之簽章-自proofC提取之資訊訊息。此驗證可使用來自與控制器1702之已建立配對的儲存LTPKC。若成功，則此驗證確認控制器1702係先前提供LTPKC之同一控制器(假定沒有其他控制器可具有相同的長期金鑰對)。在區塊1760，若authTagC或該簽章未經驗證(或若解密失敗)，則在區塊1762，配件1704可將一錯誤回應發送至控制器1702。若該等成功，則在區塊1764，配件1704可將一成功回應發送至控制器1702。在任一情況下，在發送該回應後，配件1704隨即可更新配對狀態以指示適當回應。

在區塊1766，控制器1702可判定哪些回應被接收。若接收到錯誤訊息1762，則程序1700可在區塊1768結束，且控制器1702可向使用者

報告該錯誤。若接收到成功訊息1764，則對驗證在區塊1770完成，且配對狀態可經更新以指示該完成。

將瞭解，程序1700係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1700可結束，且控制器可通知使用者該錯誤。此外，參考特定加密及/或鑑認演算法係出於說明目的，且用於資料之安全交換的其他協定及演算法可取代。

亦應注意，程序1700與藉以在配對建立時交換長期公用金鑰的方式(例如，使用哪個對設置或對新增程序)無關。配件及控制器可進行對驗證，只要每一器件具有另一者之長期公用金鑰即可，該金鑰始終保持儲存(例如，在每一器件之安全元件中)。

此外，與配件及控制器相關聯之使用者名稱(「userA」及「userC」)可包括允許另一器件在對驗證期間查找長期公用金鑰之任何資訊。此可(但不必)包括實際使用者之名稱或其他識別符。在一些實施例中，使用者名稱可併有(或為)特定長期公用金鑰所屬於之器件之器件識別符。

如同上文所述之各種對設置程序，對驗證程序1700可包括產生新的加密金鑰(Key)。在一些實施例中，此金鑰可用作用以加密在對驗證程序1700完成之後所發送的任何或全部訊息(例如，如上所述之請求及回應)的工作階段金鑰。該工作階段金鑰可持續，直至任一器件刪除其該工作階段金鑰之複本或使該複本失效。因此，任一器件可藉由刪除其自身的該工作階段金鑰之複本或使該複本失效而在任何時間單方面地切斷與另一器件之通信。舉例而言，在以下情況下，配件可刪除工作階段金鑰：控制器移動到附近臨限外或丟失與配件之連接性，或無

通信在逾時週期內發生，或在工作階段持續時間之固定上限(其可與配件製造商或程式設計師選擇的一樣短或長)之後。此允許配件按需要限制控制器之存取。

在一些實施例中，在對驗證程序1700期間所衍生之加密金鑰僅在程序1700期間使用。對於對驗證工作階段內的後續通信，控制器1702及配件1704可各自計算一或多個新的工作階段金鑰。舉例而言，配件至控制器工作階段金鑰(「AC工作階段金鑰」)可藉由將HKDF-SHA-512(或類似演算法)應用於在對驗證期間(例如，在程序1700之區塊1722及1738)所產生之共用秘密(inputKey)來衍生，具有控制salt及額外資訊項目(其可具有預定義恆定值)。控制器至配件工作階段金鑰(「CA工作階段金鑰」)可藉由將HKDF-SHA-512 (或類似演算法)應用於在對驗證期間所產生之共用秘密(inputKey)來衍生，具有另一控制salt及額外資訊項目(其亦可具有預定義恆定值)。在一些實施例中，不同控制salt及/或不同額外資訊項目可用以產生該AC工作階段金鑰及該CA工作階段金鑰，因此該兩個工作階段金鑰不必相同。控制器及配件可各自產生AC及CA工作階段金鑰兩者。在對驗證工作階段內的後續通信期間，AC工作階段金鑰可由配件用來加密配件發送至控制器之訊息及由控制器用來解密控制器自配件接收之訊息，而CA工作階段金鑰可使用由控制器用來加密控制器發送至配件之訊息及由配件用來解密配件自控制器接收之訊息。任一器件可藉由使其工作階段金鑰失效(例如，刪除工作階段金鑰或以錯誤回應使用該等工作階段金鑰加密之任何接收訊息)來結束工作階段。

另外，在一些實施例中，單一控制器可定義並使用多個長期金鑰對(LTPKC, LTSKC)。舉例而言，具有多個授權使用者之控制器(例如，共用電腦)可具有用於每一授權使用者之不同長期金鑰對，使得不同使用者可與配件之不同子集互動。只要控制器具有用於每一金鑰對之單

獨使用者名稱，配件即不必知道控制器具有一個或一個以上金鑰對。作為另一實例，控制器可將不同長期金鑰對用於與不同配件建立配對。使用多個長期金鑰對之控制器可記住哪個(LTPKC, LTSKC)對被用於每一配件(與其之配對已建立)。類似地，配件可具有多個長期金鑰對(LTPKA, LTSKA)且可記住哪個對被用於每一控制器(與其之配對已建立)。在一些實施例中，器件可將其他器件之數目限於該器件給定特定長期公用金鑰之數目，且具有多個長期公用金鑰可允許該器件不時地切換至不同金鑰。

在一些實施例中，在可被稱作「對新增」之程序或新增配對中，長期公用金鑰(或在一些情況下，憑證)可在對設置或對驗證之後在任何時間在器件之間交換。舉例而言，如上文所指出，配件可將本身限於關於一個控制器(其可被稱作配件之「管理員」或「admin」)執行對設置且可在第一成功對設置之後可拒絕所有後續對設置請求(至少直至該配對經移除，例如如下所述)。為了允許其他控制器與配件互動，admin控制器可執行對新增程序以建立配件與不同控制器之間(或在一些情況下，配件與同一控制器之不同長期公用金鑰之間)的配對。

圖18A至圖18B展示根據本發明之一實施例的控制器1802 (例如，具有管理員權限之控制器)與配件1804之間的對新增程序1800之實例。在此程序中，假定控制器1802先前已執行關於配件1804之對設置(且藉此獲得管理員權限)或已經由執行對新增程序1800之先前執行個體而新增為管理員。

首先參看圖18A，在區塊1806及1808，控制器1802及配件1804可完成對驗證程序(例如，程序1700)以建立共用秘密及工作階段金鑰(例如，如上所述之AC金鑰及CA金鑰)。

在區塊1810，控制器1802可識別一長期公用金鑰(LTPKN)以與配件1804交換。此可為(例如)屬於待與之建立配對的控制器(在本文中亦

被稱作「新」控制器)之長期公用金鑰；此可為除控制器1802外之控制器。在一些情況下，安全性憑證(其可含有長期公用金鑰)可針對該新控制器獲得。在區塊1812，控制器1802可產生一資料區塊，其含有該資料區塊係關於新增配對之請求之指示、長期公用金鑰LTPKN、新控制器之控制器識別符及指示待授予至新控制器之權限之權限資訊(例如，旗標)。舉例而言，如上文所指出，用以執行關於配件之對設置的第一控制器可被自動地指定為彼配件之管理員。對於經由對新增程序1800新增之每一新控制器，權限資訊可規定新控制器是否亦應被指定為管理員。在一些實施例中，准許一配件之管理員執行彼配件之對新增，而不准許並非管理員之控制器執行對新增。

在區塊1814，控制器1802可將對新增開始請求發送至配件1804；該請求可包括在區塊1812所產生之資料區塊。如同對驗證工作階段內之所有通信，該請求可使用適當工作階段金鑰來加密。在一些實施例中，該對新增開始請求可包括識別該對新增開始請求之狀態指示符(此及後續狀態指標可寫入至圖12之配對狀態請求特性1201)。在一些實施例中，該對新增開始請求可作為對配件1804之/pairings URL (或其他適當URL)之HTTP POST請求而發送。

在區塊1816，配件1804可接收該對新增開始請求。如同對驗證工作階段中的來自控制器之任何接收請求，配件1804可藉由使用適當工作階段金鑰解密該請求而開始；若解密失敗，則配件1804可傳回一錯誤回應(或根本不回應)。在區塊1818，配件1804可判定是否准許控制器1802執行對新增。舉例而言，如上所述，控制器可被選擇性地授予管理員權限，且對新增可限於具有管理員權限之控制器。作為另一實例，具有使用者介面之配件可提示使用者以指示是否准許該對新增請求。作為再一實例，如上所述，在一些情況下，使用者可經由機械操作而使配件處於配對模式中，且一些配件可經組態以僅在處於配對模

式中時准許對新增請求。作為另一實例，在一些實施例中，配件1804可具有可同時儲存之配對之數目的上限(例如，16個配對、32個配對或某一其他極限)，且配件1804可在對新增請求將導致超過此極限之情況下將該對新增請求處理為不准許。其他技術亦可用以判定配件1804是否應准許特定對新增請求。若該請求不被准許，則在區塊1820，配件1804可發送一錯誤訊息。

參看圖18B，若對新增請求被准許，則在區塊1832，配件1804可持久地儲存基於接收訊息之新配對(例如，在配件之安全元件中)。舉例而言，配件1804可儲存與針對新控制器之接收控制器識別符及權限有關聯的接收之長期公用金鑰LTPKN。

在一些實施例中，配件1804未必要在程序1800期間將長期公用金鑰(LTPKA)提供至控制器1802，此係因為控制器1802可在起始程序1800之前已接收該長期公用金鑰。然而，在其他實施例中，可能希望配件1804關於不同控制器使用不同長期公用金鑰。在情況如此的情況下，配件1804可準備含有應由該控制器使用之長期公用金鑰之資料區塊。舉例而言，在區塊1834，配件1804可識別待由新控制器使用之長期公用金鑰；此長期公用金鑰可與先前提供至控制器1802之長期公用金鑰(LTPKA)相同或不同。在區塊1836，配件1804可產生含有在區塊1834所識別之長期公用金鑰之資料區塊及待由新控制器使用之配件識別符(其可與先前提供至控制器1802之配件識別符相同或不同)。

在區塊1838，配件1804可將對新增回應發送至控制器1802。若資料區塊係在區塊1836產生，則該資料區塊可包括於該對新增回應中。如同對驗證工作階段內之所有通信，該回應可使用適當工作階段金鑰來加密。該對新增回應可包括更新狀態指示符以指示該對新增回應已發送。

在區塊1840，控制器1802可接收該對新增回應。如同對驗證工作

階段中的來自配件之任何接收回應，控制器1802可藉由使用適當工作階段金鑰解密該回應而開始；若解密失敗，則該回應可忽略且程序1800可以錯誤終止。

在區塊1844，控制器1802可判定該回應是否指示成功。若不指示成功，則程序1800可在區塊1846結束，且控制器1802可通知使用者該錯誤。若該回應指示成功，則在區塊1848，控制器1802可向新控制器通知配對。舉例而言，控制器1802可將用於配件1804之配件識別符及長期公用金鑰LTPKA傳達至新控制器。在一些實施例中，控制器1802可為新控制器提供用於配件1804的先前儲存之LTPKA及配件識別符；在其他實施例中，控制器1802可為新控制器提供由配件1804在該對新增回應中提供之資訊。新控制器可持久地儲存接收的LTPKA及配件識別符作為配對記錄。此後，新控制器可執行關於配件1804之對驗證程序(例如，程序1700) (未進一步涉及控制器1802)且可與配件1804互動。

應瞭解，程序1800係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1800可結束，且控制器可通知使用者該錯誤。此外，參考特定加密及/或鑑認演算法係出於說明目的，且用於資料之安全交換的其他協定及演算法可取代。在一些實施例中，對新增程序1800可用作委派配對之模式，如下所述。

如上所述，對設置及對新增可允許配件與控制器之間的配對藉由交換可由接收器件持久地並安全地儲存之長期公用金鑰來建立。在一些情況下，可能希望移除已建立配對，例如藉由自持久性儲存器移除長期公用金鑰。因此，本發明之某些實施例提供對移除程序。

圖19A至圖19B展示根據本發明之一實施例的控制器1902 (例如，

具有管理員權限之控制器)與配件1904之間的對移除程序1900之實例。程序1900可大體上類似於程序1800，惟以下除外：程序1900導致移除現有配對而建立新配對。在此程序中，假定控制器1902先前已執行關於配件1904之對設置(且藉此獲得管理員權限)或已(例如)經由執行對新增程序1800而新增為管理員。

參看圖19A，在區塊1906及1908，控制器1902及配件1904可完成對驗證程序(例如，程序1700)以建立共用秘密及工作階段金鑰(例如，如上所述之AC金鑰及CA金鑰)。

在區塊1910，控制器1902可獲得待移除之控制器之識別符。此可為由配件1804儲存於配對記錄中之識別符。在一些情況下，此可為控制器1902自身之識別符(控制器可移除其自身配對)；在其他情況下，該識別符可為另一控制器之識別符。在一些情況下，區塊1910可包括得到除該識別符之外的經移除之控制器之長期公用金鑰。在區塊1912，控制器1902可產生資料區塊，其含有該資料區塊係關於移除配對之請求之指示及配對待移除之控制器之識別符。在一些實施例中，該資料區塊可包括其他資訊，諸如經移除之控制器之長期公用金鑰。

在區塊1914，控制器1902可將對移除開始請求發送至配件1904；該請求可包括在區塊1912所產生之資料區塊。如同對驗證工作階段內之所有通信，該請求可使用適當工作階段金鑰來加密。在一些實施例中，該對移除開始請求可包括用以指示對移除開始請求已發送的狀態指示符(此及後續狀態指標可寫入至圖12之配對狀態請求特性1201)。在一些實施例中，該對移除開始請求可作為對配件1904之/pairings URL (或其他適當URL)之HTTP POST請求而發送。

在區塊1916，配件1904可接收該對移除開始請求。如同對驗證工作階段中的來自控制器之任何接收請求，配件1904可藉由使用適當工作階段金鑰解密該請求而開始；若解密失敗，則配件1904可傳回一錯

誤回應(或根本不回應)。在區塊1918，配件1904可判定是否准許控制器1902執行對移除。舉例而言，如上所述，控制器可被選擇性地授予管理員權限，且對移除可限於具有管理員權限之控制器。作為另一實例，具有使用者介面之配件可提示使用者以指示是否准許該對移除請求。作為再一實例，如上所述，在一些情況下，使用者可經由機械操作而使配件處於配對模式中，且一些配件可經組態以僅在處於配對模式中時准許對移除請求。其他技術亦可用以判定配件1904是否應准許特定對移除請求。若該請求不被准許，則在區塊1920，配件1904可發送一錯誤訊息。

參看圖19B，若該對移除請求被准許，則在區塊1932，配件1904可自其已建立配對之清單移除接收資料區塊中所規定的與控制器之配對(例如，藉由自安全儲存元件刪除該配對記錄)。

在一些實施例中，配件1904未必要提供一往復指令以在程序1900期間移除長期公用金鑰(LTPKA)。在配件1904移除該配對記錄之後，已移除控制器將不能夠執行關於配件1904之對驗證，且此可防止已移除控制器與配件1904互動，不管已移除控制器是否亦移除其配對記錄。然而，在其他實施例中，可能希望配件1904規定待移除之配對。在情況如此的情況下，配件1904可準備一資料區塊，其含有應由新移除之控制器移除的長期公用金鑰及配件識別符。舉例而言，在區塊1934，配件1904可識別應自新移除之控制器移除的長期公用金鑰；此可為(例如)當新增控制器時在程序1800之區塊1834所識別之金鑰。在區塊1936，配件1904可產生一資料區塊，其含有在區塊1934所識別之長期公用金鑰及與此長期公用金鑰相關聯之配件識別符。

在區塊1938，配件1904可將對移除回應發送至控制器1902。若資料區塊係在區塊1936產生，則該資料區塊可包括於該對移除回應中。如同對驗證工作階段中之所有其他通信，該回應可使用適當工作階段

金鑰來加密。該對移除回應可包括更新狀態指示符以指示該對移除回應已發送。

在區塊1940，控制器1902可接收該對移除回應。如同對驗證工作階段中的來自配件之任何接收回應，控制器1902可藉由使用適當工作階段金鑰解密該回應而開始；若解密失敗，則該回應可忽略且程序1900可以錯誤終止。

在區塊1944，控制器1902可判定該回應是否指示成功。若不指示成功，則程序1900可在區塊1946結束，且控制器1902可通知使用者該錯誤。若該回應指示成功，則在區塊1948，控制器1902可通知已移除控制器其配對已被移除。在一些實施例中，控制器1902亦可將用於配件1904之配件識別符及/或長期公用金鑰LTPKA傳達至已移除控制器。此後，已移除控制器不再能夠執行關於配件1904之對驗證程序，此可導致已移除控制器不能與配件1904互動。已經由程序1900移除之控制器可(例如)經由對新增程序1800在稍後時間再次新增。一些實施例可為配件1904提供一選項以將已移除控制器「加入黑名單」，該選項可防止已移除控制器重新建立與配件1904之配對。舉例而言，來自控制器1902之對移除請求可包括關於已移除控制器是否應被加入黑名單之指示，且配件1904可持久地儲存已加入黑名單之控制器的清單。在對設置或對新增期間，配件1904可檢查黑名單且在控制器在該黑名單上之情況下傳回一錯誤。

應瞭解，程序1900係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。舉例而言，每當控制器將訊息發送至配件或反過來(例如，當配對程序狀態改變時)時，可偵測到錯誤。儘管指示一些錯誤條件，但應理解，若在任何點處偵測到錯誤，則程序1900可結束，且控制器可通知使用者該錯誤。此外，參考特定加密及/或鑑認演算法係出於說

明目的，且用於資料之安全交換的其他密碼協定及演算法可取代。在一些實施例中，對移除程序1900可結合委派配對來使用，如下所述。

上文所述之實施例允許配件及控制器建立(設置)、驗證、新增及移除配對，其中配對可包括配對中之每一合作夥伴器件對另一合作夥伴器件之長期公用金鑰及/或憑證的持久性儲存。

在一些實施例中，使用者獲得與給定配件配對之控制器的清單或與給定控制器配對之配件的清單可能有用。在後一情況(與控制器配對之配件)下，執行於控制器上之程式(例如，作業系統或應用程式程式)可藉由讀取控制器之儲存配對資訊而產生一清單且在控制器之自身使用者介面上呈現該清單給使用者。為了提供與給定配件配對之控制器的清單，某些實施例允許控制器自配件擷取所有配對控制器的清單。

舉例而言，如圖12中所示，配件可具有配對清單特性1204以作為其配對設定檔之部分。特性1204可包括關於具有與配件之已建立配對之每一控制器的資訊(例如，控制器ID或類似者)，但不必包括任何控制器之長期公用金鑰。在一些實施例中，控制器可(例如)使用HTTP GET請求或類似者來讀取配對清單特性1204，如同讀取任何其他特性。在一些實施例中，控制器可藉由發送對/pairings URL (或其他適當URL)之HTTP POST請求來獲得配件之配對清單；該POST請求可包括指示該配對清單正被請求之項目。

在一些實施例中，控制器可被允許僅在對驗證工作階段內讀取配對清單1204，使得配件回應可經加密。此外，在一些實施例中，配對清單1204之讀取可限於具有管理員權限之控制器。

在一些實施例中，配件可一次與僅一個控制器建立配對，且僅建立配對之控制器被准許稍後移除該配對。此可增強安全性。然而，對於一些應用，其可為不方便地限制。舉例而言，就家庭環境100 (圖1)而言，若多個人生活在該家庭中，則每一個人可能希望具有可解除鎖

定門鎖104之控制器102 (例如，行動電話)。

因此，本發明之某些實施例可允許一配件同時維持與多個控制器之配對。舉例而言，每一控制器可使用上文所述之對設置程序單獨地建立配對。然而，允許控制器獨立地建立配對對於一些應用而言可能不夠安全。舉例而言，就家庭之前門上之鎖而言，房主可能想要防止任何其他人在沒有房主之明確准許的情況下建立配對。

為了考慮受管理配對，某些實施例可提供「委派」配對程序。在委派配對程序中，第一(「admin」或「主控」)控制器可(例如)使用如上所述之對設置與配件建立配對且藉此獲得管理員權限。此後，可需要admin控制器參與針對任何後續(「委派」)控制器之對設置程序。

一種類型之委派配對可為「直接」委派。在直接委派中，主控控制器可使用圖18A至圖18B之對新增程序1800或類似程序將用於委派控制器之控制器公用金鑰(及控制器使用者名稱)傳遞至配件。為了直接委派，主控控制器可與委派控制器通信以獲得委派控制器之長期公用金鑰。

另一類型之委派配對可為「外部」或「轉送」委派。在外部委派中，配件可經組態以將對設置及對驗證委派至「授權者」器件，該器件可併入至主控控制器或可與主控控制器通信之某一其他器件中。授權者器件可如上所述地執行關於配件之對設置，且在對設置之後，授權者可維持(或使用對驗證重新建立)至配件之安全頻道。若配件接收對設置或對驗證請求，則配件可經由該安全頻道將該請求轉送至授權者。授權者可執行該操作及/或向配件指示是否應允許該操作。

第三類型之委派配對可為「基於憑證之」委派。在基於憑證之委派中，主控控制器可用信任憑證鏈結來組態配件。舉例而言，主控控制器可使用圖18A至圖18B之對新增程序1800類似程序將信任憑證鏈結安全地傳遞至配件。舉例而言，「設定憑證鏈結請求」訊息可針對

控制器定義以發送至配件(此可為例如對為了接收憑證鏈結而定義之特性或URL之HTTP PUT請求)。此請求訊息之內容可包括含有憑證鏈結的TLV項目或多個系列之TLV項目，例如按自根至最深子授權之次序。該(該等) TLV項目可用在對驗證期間所建立且使用主控控制器之長期秘密金鑰LTSKC用數位方式簽署的對稱金鑰來加密。配件可使用儲存LTPKC來驗證該簽章且使用對稱金鑰來解密該(該等)加密TLV項目以提取憑證鏈結。在一些實施例中，憑證鏈結可儲存於配件之安全儲存元件中。配件可發送指示成功或失敗之回應訊息。

當另一控制器嘗試執行關於配件之對設置時，可需要彼控制器提供除其長期公用金鑰外或替代其長期公用金鑰之憑證。配件可判定憑證是否藉由先前接收之信任憑證鏈結簽署且可部分地基於憑證是否如此簽署來接受或拒絕該對設置。委派控制器可藉由經由某一其他頻道(例如，來自主控控制器、受信任憑證授權單位或類似者)獲得恰當簽署之憑證及向配件呈現該憑證而變為對於配件而言經授權。

熟習此項技術者將瞭解，本文中所描述之配對程序及架構係說明性的且變化及修改係可能的。不同加密演算法、金鑰及協定可取代，且多個不同演算法、金鑰及協定可在給定操作環境中同時得到支援。

實例配件：門鎖

為了進一步說明可存在於本發明之實施例中之各種態樣及特徵，現將描述特定配件實例。

第一實例為門鎖配件，其可包括可安裝在門上的耦接至門鎖之電子鎖定單元。在一些實施例中，門鎖本身可為機械鎖(例如，死栓類型)，且電子鎖定單元可操作機電致動器以使機械鎖在已鎖定位置與解除鎖定位置之間移動。亦可提供位置感測器或類似者以允許電子鎖定單元判定機械鎖當前是否處於鎖定或解除鎖定位置中。在其他實施例中，可使用其他類型之門鎖，例如磁鎖、電子鎖及可藉由供應電控制

信號及/或施加機械力來鎖定及解除鎖定的任何其他類型之鎖。電子鎖定單元可容納或連接至用以實施如上所述之統一配件協定之邏輯電路及用以與一或多個控制器通信之通信電路。電子鎖定單元可產生電信號(例如，一或多個電線上之電壓或電流位準)以(例如)經由機電致動器或類似者來操作門鎖。在一些實施例中，電子鎖定單元及門鎖可實體上位於共同外殼(諸如附接至門之模組)內或在門或門框內。在其他實施例中，電子鎖定單元及門鎖可在單獨外殼中。舉例而言，門鎖可在門內，而電子鎖定單元係安裝在附近牆壁上。可提供門鎖及電子鎖定單元中之致動器之間的有線連接。亦可使用無線連接而不背離本發明範疇，儘管熟習此項技術者將瞭解，在此背景下之無線連接可使額外安全性擔憂增加。

參看圖20，展示了根據本發明之一實施例的用於門鎖配件2004之操作環境2000。操作環境2000可實施於(，例如)辦公室建築物、家庭、公寓或旅館建築物或具有至少一個內部或外部門2006之任何其他結構中。出於說明目的，假定希望為多個個人提供鎖定及解除鎖定門2006之能力。進一步假定門2006具有「擁有者」(亦即，合法或藉由合約而有權利判定應或不應允許何人通過門2006之某一人或實體)。舉例而言，若環境2000係實施於辦公室建築物中，則建築物之擁有者(或起擁有者之權利作用的租用戶)可為門2006之擁有者。若環境2000實施於家庭中，則擁有者可為房主、家庭之領導或由居住者指定之其他個人。

在此實例中，門鎖配件2004可經組態而以無線方式一或多個使用者操作之控制器2012 (展示了三個，但可使用任何數目)通信。舉例而言，門鎖配件2004可提供可藉由實體接近控制器2012中之一者來觸發以起始通信之感測器2020。門鎖配件2004亦可與主控控制器(亦被稱作管理員) 2018通信。在此實例中，與主控控制器2018之通信係藉由無線連接，但亦可使用有線連接。

主控控制器2018可為門2006之擁有者擁有或操作之計算器件，包括桌上型電腦、膝上型電腦、行動電話、平板等。就辦公室建築物而言，操作主控控制器2018之個人可為指定安全性代理。主控控制器2018可實體上相對於門2006位於任何地方。舉例而言，主控控制器2018可在門2006提供進入之房間中、在位於建築物中之別處的安全性辦公室中或完全在另一建築物中。在一些實施例中，主控控制器2018亦可充當使用者器件(例如，行動電話)。

在安裝門鎖配件2004之後，主控控制器2018可執行如上所述之對設置程序以將本身建立為主控控制器；舉例而言，作為執行對設置之結果，主控控制器2018可獲得管理員權限(例如，如上所述)。此外，可使用委派配對技術(例如，如上所述之對新增)在門鎖配件2004與使用者器件2012中之每一者之間建立配對。或者，門鎖配件2004可經組態以使得對設置僅可在特定實體條件(例如，實體上插入至配件2004中之鑰匙)下執行，當獲得用於配對之實體條件時，門鎖配件2004可執行關於使用者器件2012中之每一者之對設置。

在一些實施例中，門鎖配件2004之配件模型可包括提供鎖定及解除鎖定門之能力的鎖機構服務(例如，圖2G之鎖機構服務254之執行個體)。門鎖配件2004之配件模型亦可包括鎖管理服務(例如，圖2H之鎖管理服務255之執行個體)，且該鎖管理服務可支援其他鎖相關功能，諸如具有指示何人在何時已鎖定或解除鎖定門之條目的鎖定記錄檔。該鎖定記錄檔可(例如)由主控控制器2018來存取。

圖21展示根據本發明之一實施例的用於門鎖配件2004之配件物件2100之實例。物件2100係以表格形式展示，但亦可表示為類似於圖3A至圖3C之JSON物件。如所示，門鎖配件2004可包括配件識別服務執行個體2102、鎖機構服務執行個體2104及鎖管理服務執行個體2106。每一服務執行個體可包括如所示之特性；該等特性可根據圖2A

至圖2D及圖2J來定義。舉例而言，當前狀態特性2110可藉控制器讀取以判定門當前係鎖定或解除鎖定(或已卡住等)，且目標狀態特性2112可由控制器寫入以請求門之鎖定或解除鎖定。

鎖定記錄檔特性2116可含有鎖定記錄檔事件記錄之陣列，該等記錄中之每一者可為資料物件。在此實例中，每一鎖定記錄檔事件記錄可包括使用門鎖2004之實體(個人或器件)之識別符、使用發生之時間及所執行之操作(例如，鎖定或解除鎖定、讀取鎖定記錄檔、清除鎖定記錄檔)。可提供選用之字串元素以提供關於使用之額外供應商特定資訊。在一些實施例中，控制器可讀取特性2116以存取鎖定記錄檔。

鎖管理控制點特性2114可用以(例如)發送對讀取或清除鎖定記錄檔之請求。舉例而言，控制器可發送用以將資料物件寫入至特性2114之請求，且該資料物件可解譯為特定請求。在此實例中，受支援請求可包括讀取鎖定記錄檔(自資料物件中所規定之開始時間開始)、清除鎖定記錄檔(其可自鎖定記錄檔刪除所有條目或規定範圍之條目，如資料物件中所規定)及設定門鎖配件2004可用作為用於記錄未來鎖定記錄檔條目之基礎的當前時間(設定時間對(例如)說明日間節省時間或類似者可有用)。如上文參看圖5G至圖5K所描述，在一些實施例中，門鎖配件2004可選擇是以內嵌方式或經由查詢結果機制來回應控制點特性2114之寫入請求。該決策可基於每個請求。

圖21中所示之其他特性可如上文參看圖2A至圖2D及圖2J所述地操作。

將瞭解，圖21中所示之服務及特性係說明性的且變化及修改係可能的。可針對鎖配件視該鎖之功能性而定義服務及特性之其他集合及子集。

為了進一步說明，現將描述特定實施情境。在此情境下，門2006之擁有者可購買門鎖配件2004並將其安裝於門2006上。(門鎖配件2004

可作為門2006之部分來銷售或作為售後升級)。門2006之擁有者可組態主控控制器2018以與門鎖配件2004通信。舉例而言，主控控制器2018可為桌上型或攜帶型(例如，膝上型、手持型、行動、可穿戴式)電腦系統，其可執行用以發送及接收遵守上文所述之統一配件協定之訊息且用以產生允許門2006之擁有者與門鎖配件2004互動之圖形使用者介面(或其他類型之使用者介面)的程式(例如，作業系統程式或使用者安裝之應用程式程式)。

在執行此安裝後，門2006之擁有者可配對主控控制器2018與門鎖配件2004。圖22為根據本發明之一實施例的使用者(諸如門2006之擁有者)可用來配對主控控制器2018與門鎖配件2004 (或任何其他控制器與任何其他配件)之程序的流程圖。

在區塊2202，門鎖配件2004 (或任何其他配件)可進入配對模式。在一些實施例中，使用者可使配件處於配對模式中。在一些實施例中，每一配件製造商可定義用以使其配件處於配對模式中之特定使用者動作。舉例而言，就門鎖配件2004而言，配件製造商可在配件外殼中之某處提供實體鑰匙孔或鑰匙槽，使用者將由配件製造商提供之鑰匙插入至該實體鑰匙孔或鑰匙槽中。作為另一實例，門鎖配件2004可具有在其外殼上或內部之機械開關以啟用或停用配對模式；此開關可經置放以使得該開關在門2006關閉時不可使用。一般而言，使配件處於配對模式中可涉及各種動作以向配件指示經授權使用者存在且正在嘗試配對控制器與配件；然而，並未要求使用用於使配件處於配對模式中之任何特定技術。此外，在一些實施例中，門鎖配件2004可在該配件第一安裝及通電時或每當該配件不具有與任何控制器之已建立配對時自動地進入配對模式。

在區塊2204，控制器可尋找配件。舉例而言，就門鎖配件2004及主控控制器2018而言，配件2004可在其處於配對模式中時開始(例如)

使用如上所述之器件探索服務廣告該配件對於配對之可用性。主控控制器2018可執行可(例如)藉由執行圖4之配件探索程序400來定位門鎖配件2004之統一控制器程式(或其他程式碼)，直至區塊422。作為另一實例，一些控制器可經組態以自動地搜尋配件(以規律間隔或回應於諸如進入區域之事件)或回應於諸如致動由控制器提供之「尋找(FIND)」控制之使用者輸入而搜尋配件。

在區塊2206，使用者可指示控制器與在區塊2204所找到之配件配對。舉例而言，如上所述，配件探索程序400可包括控制器呈現關於配件之資訊給使用者及提示使用者指示配對是否應發生。作為另一實例，執行配件探索之控制器可呈現被找到之所有配件之清單給使用者，且使用者可自該清單選擇待配對之配件。使用者指令可採用各種形式。在一些情況下，使用者指令可包括鍵入門鎖配件2004之設置碼；在其他情況下，設置碼之鍵入可為單獨的使用者動作。

在區塊2208，回應於使用者指令，控制器可起始關於在區塊2204所找到之配件之對設置程序。舉例而言，上文所述之對設置程序(程序1300、1400、1500、1600)中之任一者可在區塊2208起始。

在區塊2210，在對設置程序期間之某一點，使用者可將與起始對設置之特定控制器之配對應發生的驗證提供至配件。是否需要驗證及需要何種驗證可由配件製造商來判定。在一些實施例中，配件不需要超出如下事實以外的任何額外驗證：配件處於配對模式中且控制器正在嘗試配對。此外，在一些實施例中，區塊2206處之使用者輸入(其可包括配件設置碼)亦可充當區塊2210處之驗證。在配件要求驗證之情況下，此驗證可(例如)藉由將使用者執行由配件可檢測之某一動作的要求包括於對設置程序中來實施，其中若該動作未正確進行，則配件產生對控制器之錯誤回應。

舉例而言，配對程序1300及1500包括對配件之驗證，其呈控制器

具有配件之設置碼的控制器之證明之形式。如上所述，控制器可自使用者獲得配件之設置碼且在產生共用秘密中使用該設置碼；控制器正確地產生共用秘密之事實可為對配件之驗證：控制器具有該設置碼。作為另一實例，若控制器及配件均配備近場通信(NFC)技術(例如，符合由NFC論壇(http://nfc-forum.org)頒佈之標準之通信技術)，則配件可需要使用者使控制器到達NFC通信範圍且可與控制器交換資訊以確認NFC頻道上之控制器係正在另一頻道上執行對設置之同一控制器。舉例而言，可需要控制器經由NFC頻道及對設置頻道兩者來提供其關於共用秘密之證明(proofC)。其他驗證操作可取代，且單一使用者動作可提供區塊2206處的用以配對之指令區塊2210處的驗證兩者。

在區塊2212，對設置程序可完成，且(假定無錯誤已發生)使用者可被告知(例如，藉由控制器)與配件之配對已建立。此後，在區塊2214，配件可退出配對模式。在一些實施例中，退出配對模式可包括用以自配對模式移除配件之使用者動作。此使用者動作可為區塊2202處所採用的用以使配件處於配對模式中之使用者動作的反轉，諸如移除實體鑰匙、將配對開關翻轉至其停用位置等。在一些實施例中，配件可在對設置完整後即自動地退出配對模式。

參看圖20，在環境2000中，可針對每一控制器2012重複程序2200：門2006之擁有者希望與門鎖配件2004配對。然而，在一些環境中，個別地配對每一控制器2012可不方便。舉例而言，若配對要求緊密實體接近，則必須使每一控制器2012如此接近，然後進行配對。若大量控制器2012待配對(例如，若門2006係具有許多居住者之大型建築物的前門)，則此可變得非常耗時。另外，在一些實施例中，在第一控制器已成功地建立配對之後，門鎖配件2004可不准許第二控制器執行對設置。

因此，在一些實施例中，程序2200可用以建立門鎖2004與一個控

制器(例如，主控控制器2018)之間的配對。此後，主控控制器2018可使用委派配對程序(例如，上文所述之對新增程序1800或其他委派配對程序)來建立門鎖2004與額外控制器2012之配對。舉例而言，若主控控制器2018具有用於特定控制器2012之長期公用金鑰(或安全性憑證)，則主控控制器2018可使用對新增程序1800將該金鑰(或憑證)提供至門鎖配件2004。作為另一實例，主控控制器2018可將信任憑證鏈結提供至門鎖配件2004 (例如，如上所述)，且每一控制器2012可具有藉由該信任憑證鏈結簽署之憑證，其可用以允許給定控制器2012建立配對及使用門鎖配件2004。如上所述，在一些實施例中，主控控制器2018可將admin權限選擇性地授予任何新增之控制器2012，且具有admin權限之控制器2012可執行對新增以建立配件2004與額外控制器2012之間的配對。

此外，經授權使用門2006之使用者之集合可隨時間改變。舉例而言，在辦公室建築物中，員工可能辭職，此後該員工進入該建築物之權力應終止。在家庭中，同住者可搬出。主控控制器2018 (或具有管理員權限之其他控制器)可(例如)藉由使用上文所述之對移除程序1900移除門鎖配件2004與應不再被授予使用權力之任何控制器2012之配對來進行此等更新。

在一些實施例中，在主控控制器2018 (或具有針對門鎖配件2004之admin權限的其他控制器2012)上執行之統一控制器程式可提供各種使用者介面以促進管理對門2006之使用權力。舉例而言，擁有者或安全性代理可能能夠：查看授權控制器之清單，例如使用如上所述之清單配對請求(在一些實施例中，該清單亦可包括識別授權控制器之使用者)；識別待新增至該授權清單之新控制器；及/或選擇待自該授權清單移除之授權控制器。因此，組織或多使用者環境中之安全性操作可流線化。

一旦特定控制器2012已與門鎖配件2004建立配對(例如，使用上文所述之技術中之任一者，包括直接或委派配對)，彼控制器2012可用以使用門2006。舉例而言，控制器2012可用使控制器2012能夠發送及接收遵守如上所述之統一配件協定之訊息的程式碼(例如，作業系統或應用程式碼)來佈建。該程式亦可定義一圖形使用者介面(或其他類型之使用者介面)以允許控制器2012之使用者與配件互動。

圖23為根據本發明之一實施例的用於解除鎖定門之程序2300之實例。程序2300可例如在圖20之任何控制器2012 (或控制器2018)與門鎖配件2004之間執行。

程序2300可在區塊2302開始，此時控制器2012判定門2006應被解除鎖定。舉例而言，攜帶攜帶型控制器2012之使用者可在門鎖配件2004之範圍內。「在範圍內」可定義為在無線通信範圍內或視需要變得更窄。舉例而言，為了避免門之無意解除鎖定，控制器2012及門鎖配件2004可以接近性感測容量(例如，使用藍芽LE、NFC或類似者)來組態，且控制器2012可經組態以定義用於嘗試解除鎖定門之最大範圍(例如，在幾吋內、2呎、6呎或某一其他範圍)。在一些實施例中，當控制器2012偵測門鎖配件2004在範圍內時，控制器2012可與使用者互動以確認使用者想要解除鎖定門2006。舉例而言，使用者可發動或以其他方式啟動應用程式或系統級程式(或其部分)以在進入範圍內後解除鎖定門。在其他實施例中，控制器2012可執行程序2300之部分以作為用以掃描門鎖配件(控制器具有與其已建立配對)之背景程序；在範圍中偵測此配件後，控制器2012可產生對使用者之提示。此外，當控制器2012提示使用者確認門應被解除鎖定時，控制器2012可需要使用者供應鑑認憑證(例如，密碼或諸如指紋之生物識別憑證)以驗證控制器2012正由授權使用者攜帶。在另其他實施例中，控制器2012可經組態以在控制器2012在門鎖配件2004之範圍內時自動地嘗試解除鎖定門

2006而無需使用者輸入。其他實施亦係可能的。特定實施可取決於特定門鎖配件2004所需之安全性等級，因此同一控制器可視使用者已接近哪扇門而表現不同。

此外，其他技術可用以判定門應被解除鎖定，且控制器2012與門鎖配件2004之間的實體接近並非必需的。舉例而言，使用者可能能夠藉由操作控制器2012上之使用者介面以選擇門並指示該門應被解除鎖定來遠端地解除鎖定門2006 (例如，完全自另一房間或另一位置)。在一些實施例中，在執行遠端解除鎖定之前，控制器2012可能需要使用者供應鑑認憑證(例如，密碼或諸如指紋之生物識別憑證)以驗證控制器2012正由授權使用者操作。

在區塊2306及2308，控制器2012及門鎖配件2004可執行對驗證操作(例如，上文所述之程序1700)。此操作可驗證配對先前建立於該兩個器件之間。在區塊2310，若對驗證程序不成功，則程序2300可在區塊2312結束，且控制器2012可警示使用者該錯誤。在一些實施例中，使用者可被提示重試。每當控制器2012嘗試解除鎖定門鎖配件2004時，可需要對驗證。

若對驗證程序成功，則在區塊2314，控制器2012可將加密請求發送至門鎖配件2004以開啟門。舉例而言，如上文參看圖5A至圖5D所描述，控制器2012可發送HTTP PUT請求以將布林值「真」(開啟)之值寫入至門鎖配件2004之鎖定狀態特性2102。如同對驗證工作階段中之所有通信，該請求可使用在對驗證期間(或在此之後)所建立之工作階段金鑰來加密。在一些實施例中，該請求可用控制器2012之長期秘密金鑰來簽署，儘管此並非必需的。

在區塊2316，門鎖配件2004可接收該加密請求。在區塊2318，門鎖配件2004可驗證並解密該請求。如同對驗證工作階段內之所有通信，若該請求並非用正確的工作階段金鑰加密，則配件可忽略該請求。

此外，若該請求係用控制器之長期秘密金鑰簽署，則配件可使用其對控制器之長期公用金鑰(其可針對已建立配對持久地儲存)之複本來驗證該簽章且且因此驗證控制器之身分識別。配件2004亦可驗證控制器2012經准許解除鎖定門。舉例而言，在一些實施例中，在某些時間之存取可限於具有管理員權限之控制器。此限制可藉由具有寫入至僅admin存取特性2122 (圖21)之管理員特權之控制器來設定或移除，此可為圖2D之特性228之執行個體。亦可應用其他規則或決策準則。

在區塊2320，若該請求有效(例如，若該請求經正確解密且來自准許控制器)，則門鎖配件2004可進行至在區塊2322解除鎖定門。在一些實施例中，門鎖配件2004可向控制器2012報告該解除鎖定(例如，藉由發送HTTP 200 OK回應)。必要時，控制器2012及/或門鎖配件2004亦可提供指示成功之使用者可感測輸出。舉例而言，任一或兩個器件可發出嗶嗶聲或發出滴答聲、閃爍綠光等。在一些實施例中，配件之回饋行為可藉由將適當特性包括於鎖服務執行個體2106 (諸如音訊回饋特性206 (圖2A)或視需要其他特性)之定義中而變得可定製。

若則在區塊2302，該請求無效，則在區塊2324，門鎖配件2004可將一錯誤訊息發送至控制器2012 (例如，藉由發送一HTTP錯誤回應)。在一些實施例中，控制器2012可向使用者告知該錯誤及/或提示使用者再次嘗試。必要時，控制器2012及/或門鎖配件2004亦可提供指示解除鎖定嘗試失敗之使用者可感測輸出。舉例而言，任一或兩個器件可發出錯誤聲音(例如，不同於成功聲音之嗶嗶聲)、閃爍紅光等。

將瞭解，程序2300係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。應注意，程序2300依賴於先前建立之配對的存在，但可獨立於藉以建立配對之方式(例如，基於憑證或基於設置碼、直接或委派)。因此，在此實例中之配件及控制器將需要知道配件及控制器具有

已建立配對，但不知道如何或何時配對經建立。

此外，儘管程序2300說明鎖定門之特定情況下的控制器與配件之間的互動，但有權使用本發明之熟習此項技術者將認識到，可實施類似程序以控制任何配件之任何操作。

在一些實施例中，門鎖配件2004可使門2006解除鎖定，直至用以鎖定門之明確指令被接收(例如，經由類似於程序2300之程序)。在其他實施例中，門鎖配件2004可應用自動重新鎖定間隔。舉例而言，在區塊2322解除鎖定門2006之後，配件2004可等待固定時間段(例如，十秒)，接著重新鎖定。若使用者在區塊2322解除鎖定門之後未即時地(例如，在五秒內)將開啟門，則亦可實施其他安全性措施，諸如自動地重新鎖定門2006。自動重新鎖定行為可(例如)藉由將非零值寫入至自動逾時特性執行個體2124 (圖21)來實施。

在一些實施例中，門鎖配件2004在解除鎖定門之前可需要額外條件或使用者動作。舉例而言，如上文所指出，門鎖配件2004可併有NFC收發器，且門鎖配件2004可需要控制器2012在解除鎖定之前進入NFC範圍。或，門鎖配件2004可具有用以偵測何時使用者在觸摸門的感測器且可如下情況下拒絕解除鎖定：在配件判定解除鎖定請求有效之後，門未被即時(例如，在兩秒或五秒內)觸摸。

作為另一實例，在一些實施例中，門鎖(或任何其他配件)之製造商或供應商可選擇藉由使用在控制器與配件之間交換之「資料斑點」來併入製造商特定行為。如本文中所使用，「資料斑點」係指可由控制器儲存(例如，圖20之控制器2012及主控器件2018中之每一者可儲存器資料斑點)並作為對配對之任何請求之部分發送至彼配件或選擇性地隨特定請求(例如，寫入至特定特性之請求)發送的資料區塊。自控制器之觀點看，資料斑點可不透明；接收資料斑點之配件可以配件特定方式來解譯該資料斑點之內容。

以說明方式，就門鎖配件2004而言，製造商可需要門鎖配件2004之使用者登記為鎖之授權使用者。舉例而言，製造商可提供支援一網站之伺服器，使用者可在該網站獲得用於鎖之授權碼(例如，藉由在該伺服器建立一帳戶)。一授權區塊(其可為含有該授權碼及配件製造商所要之任何額外資訊的資料物件)可藉由該伺服器產生並傳遞至使用者之控制器2012。控制器2012可儲存該授權區塊以作為與配件2004相關聯之資料斑點。當控制器2012隨後將請求發送至配件2004時，控制器2012可將儲存之資料斑點包括於該請求中。

在一些實施例中，發送資料斑點可取決於請求之性質。舉例而言，配件定義記錄可定義特性(例如，如圖3A至圖3C中所示)，包括控制器具有的關於彼特性之權限。在一些實施例中，權限字串(例如，「Blob Required」)可經定義以指示需要資料斑點以存取特性，且配件製造商可將此字串包括於針對任何特性(製造商希望接收用於該特性之資料斑點)之權限之定義中。當產生對特定特性之請求時，控制器2012可查閱來自配件定義記錄(控制器可快取該配件定義記錄)之權限以判定是否需要資料斑點；若需要，則控制器2012可將資料斑點附加至請求。在其他實施例中，是否發送資料斑點之決策可在每個配件層級進行(例如，若控制器具有針對特定配件所儲存之資料斑點，則控制器可將該資料斑點附加至該控制器發送至彼配件之每一個請求)。

實例配件：IP攝影機

根據本發明之各種實施例可控制之配件之第二實例為IP攝影機配件。IP攝影機配件可包括能夠擷取視訊影像(具有或不具音訊)及將所擷取之媒體(音訊及/或視訊)串流至其他器件的攝影機。在一些情況下，IP攝影機亦可提供其他功能性，諸如記錄及/或播放先前記錄之內容。如同使用如本文中所描述之統一配件協定之任何其他配件，此等功能性可模型化為服務且藉由讀取及寫入至各種服務之特性執行個體來控

制。

在上文所述之統一配件協定之實施例中，控制器與配件之間的通信可使用HTTP請求及回應進行。就IP攝影機而言，HTTP請求及回應可用以設置攝影機並控制攝影機之行為(例如，對準攝影機、開始及停止記錄等)；然而，HTTP可能不十分適合媒體內容在器件之間的即時串流。因此，在本文中所描述之IP攝影機實施例中，IP攝影機及控制器可使用不同協定，諸如RTP協定(例如，如IETF RFC 3550中所定義)及用於媒體安全性之SRTP協定(例如，如IETF RFC 3711中所定義)。其他媒體串流協定可取代，如將顯而易見。統一配件協定可定義可用以建立支援串流協定之串流工作階段(其可不同於根據統一配件協定所定義之對驗證工作階段)的特性，串流內容之傳遞可經由串流工作階段進行。

參看圖24，展示了根據本發明之一實施例的用於IP攝影機配件2404之操作環境2400。在此實例中，IP攝影機配件2404可(例如)經由無線存取點2406與控制器2402通信。亦可支援直接通信。IP攝影機配件2404可為永久地或可移除地安裝在一區域中之固定件(例如，安裝在建築物之房間、走廊或入口中之安全性或監視攝影機)，或該攝影機配件可為可用以以多種不同設定來擷取視訊之攜帶型攝影機。控制器2402可為用以控制IP攝影機2404之任何器件。舉例而言，若IP攝影機2404被用作建築物之安全性攝影機，則控制器2402可實施在建築物中之會客區(security station)處。作為另一實例，IP攝影機2404可(例如)作為嬰兒監視器而設置於兒童房中，且控制器2402可為父母通常可攜帶的父母之行動電話、平板或其他器件。作為再一實例，使用者可將IP攝影機2404帶到公園或野生動物保護區且將該攝影機設置在不顯眼之處，接著退回遠端位置以使用控制器2402來控制IP攝影機2404，由此增加獲得野生動物或類似者之品質視訊的可能性。因此，IP攝影機2404之

使用不限於任何特定環境或任何特定控制器。

如同本文中所描述之其他配件，IP攝影機配件2404可模型化為服務之集合。圖25A至圖25B展示根據本發明之一實施例的針對可包括於用於IP攝影機配件2404之配件模型中之服務2501至2505的定義。類似於上文展示於圖2G至圖2H中之服務定義實例，服務定義2501至2505可規定必需及/或選用之特性。圖26A至圖26D展示針對圖25A至圖25B之服務之特性的實例定義。圖26A至圖26D中未提供的圖25A至圖25B中所列出之特性之實例定義可在圖2A至圖2D中找到。此等服務及/或特性中之任一者可定義為核心服務及特性，或若並非如此定義，則可定義為延伸服務及特性。

參看圖25A，IP攝影機串流服務2501可描述用以管理媒體工作階段之即時通信服務。舉例而言，IP攝影機串流服務2501可包括有助於控制器2402與IP攝影機配件2404之間的媒體串流之設置及控制的特性，例如如下所述。

記錄服務2502可描述用以控制記錄器件(例如，開始、停止或排程記錄)之服務。類似地，播放服務2503可描述用以藉由配件來控制儲存媒體之播放(例如，開始及暫停播放)之服務。儘管此實例中未展示，但熟習此項技術者將認識到，可定義額外特性以用於選擇儲存之媒體項目進行播放，以作為播放服務2503之部分或作為單獨內容選擇服務。

參看圖25B，攝影機服務2504可提供對攝影機設定之控制，諸如接通或關斷攝影機。在一些實施例中，與攝影機設定相關之其他特性可作為選用之特性而包括於此服務中，諸如攝影機定向特性(例如，平移、傾斜、變焦、旋轉)。其他選用之特性可包括影像處理特性，諸如夜視(接通或關斷)及鏡像模式(啟用或停用所擷取影像之鏡像處理)。特定攝影機配件提供之任何使用者選用之設定可具有經定義且包括於攝影機服務2504中之對應特性。

麥克風服務2505可提供對可操作以記錄聲音之麥克風之控制。服務2505可包括於用於具有麥克風輸入之任何攝影機配件之定義中且針對不具有麥克風輸入之任何攝影機配件省略。

揚聲器服務2506可提供對可操作以輸出聲音之揚聲器之控制。服務2506可包括於用於具有揚聲器輸出之任何攝影機配件之定義中且針對不具有揚聲器輸出之任何攝影機配件省略。

參看圖26A至圖26B，具有IP攝影機管理用途之特性可包括工作階段開始特性2601、工作階段結束特性2602及額外特性2603至2615。工作階段開始特性2601及工作階段結束特性2602 (展示於圖26A中)可由控制器寫入以開始及結束串流工作階段。額外特性2603至2615可由控制器讀取以獲得關於IP攝影機之視訊及/或音訊串流之性質的資訊。

工作階段開始特性2601可以資料物件(例如，以TLV格式或其他金鑰值格式)為值，控制器可寫入該值以提供可由IP攝影機配件使用以開始串流工作階段之資訊。圖26C展示可包括於工作階段開始特性2601中之資料元素之實例。工作階段ID 2631可為用於待開始之串流工作階段之UUID。控制器IP位址2632及控制器埠2633可識別串流資料應發送至(例如，使用IPv4或IPv6格式)的目的地。控制器SRTP主控金鑰2634及控制器SRTP主控salt 2635可提供待用於加密在工作階段內串流之媒體的salt及主控加密金鑰。視訊最大頻寬2636及音訊最大頻寬2637可指示串流資料頻寬(例如，以每秒千位元(kbps)計)之上限。

再次參看圖26A，工作階段結束特性2602可以資料物件(例如，以TLV格式或其他金鑰值格式)作為值，其提供待結束之工作階段之工作階段識別符。在一些實施例中，不需要其他資訊來結束工作階段。

視訊轉碼器名稱2603可提供表示由IP攝影機服務執行個體之視訊轉碼器提供之媒體類型的字串。在一些實施例中，可定義用於該字串之一組有效值(例如，由IANA (網際網路賦值主管當局，可經由

http://www.iana.org存取)定義之一組轉碼器名稱)。在一些實施例中，IP攝影機服務2501之給定執行個體支援一個轉碼器(例如，如IETF RFC 6184中所定義之H.264轉碼器)，且支援多個轉碼器之IP攝影機配件可定義IP攝影機服務2501之多個執行個體。控制器可藉由寫入至IP攝影機服務2501之對應執行個體之工作階段開始特性來選擇用於工作階段之所要轉碼器。

視訊轉碼器參數2604可提供用於視訊轉碼器之額外參數。所包括之特定參數可取決於視訊轉碼器名稱2603且可以金鑰值格式表達。舉例而言，就H.264轉碼器而言，視訊轉碼器參數2604可包括規定子設定檔及H.264轉碼器之層級的設定檔-層級ID及規定轉碼器是否支援單一NAL單元模式或非交錯模式的封包化模型。可視藉由服務執行個體支援之特定視訊轉碼器來定義其他參數。

視訊屬性特性2605可提供服務-層級屬性(例如，SDP屬性)。實例包括影像屬性及方向屬性(例如，僅發送、僅接收或雙向(發送且接收))。在一些實施例中，若方向未規定，則可假定「僅發送」為預設值。

RTP視訊有效負載類型特性2606可提供7位元整數有效負載類型，例如針對RTP所規定。

RTP協定特性2607可提供識別使用中的特定基於RTP之設定檔。舉例而言，「RTP/SAVP」可指IETF RFC 3550中所定義之設定檔，而「RTP/SAVPF」可指IETF RFC 5104中所定義之設定檔。亦可定義其他設定檔及字串。

RTP延伸特性2608可提供列出由IP攝影機服務2501之此執行個體支援之RTP延伸的字串之陣列。RTP延伸之實例可包括圖像損失指示、時間-空間權衡請求、臨時最大媒體串流位元速率等。

SRTP密碼編譯套件特性2609可提供識別待用於安全RTP串流之

密碼編譯套件的字串。在一些實施例中，字串可符合密碼編譯套件之IANA登記名稱。在一些實施例中，SRTP密碼編譯套件特性2609可允許值「無」來指示SRTP未使用(例如，串流之視訊資料未加密)。

參看圖26B，音訊轉碼器名稱特性2610可提供表示由音訊轉碼器提供之媒體類型的字串。在一些實施例中，可定義用於該字串之一組有效值(例如，由IANA (網際網路賦值主管當局)定義之一組轉碼器名稱)。在一些實施例中，IP攝影機服務2501之給定執行個體可支援音訊及視訊轉碼器之一個組合，且IP攝影機配件可藉由定義IP攝影機服務2501之多個執行個體來支援轉碼器之多個組合。控制器可藉由寫入至IP攝影機服務2501之對應執行個體之工作階段開始特性來選擇用於工作階段之所要音訊及視訊轉碼器。

音訊轉碼器參數2611可提供用於音訊轉碼器之額外參數。所包括之特定參數可取決於音訊轉碼器名稱2610且可以金鑰值格式表達。舉例而言，就Opus轉碼器而言，音訊轉碼器參數2604可包括關於是否啟用恆定位元速率或可變位元速率之指示符。可視特定音訊轉碼器來定義其他參數。

音訊屬性參數2613可提供媒體-層級屬性(例如，SDP屬性)。實例包括方向屬性(例如，僅發送、僅接收或雙向(發送且接收))。在一些實施例中，若方向未規定，則可假定「僅發送」為預設值。

RTP音訊時脈速率特性2614可提供用於音訊之RTP時脈速率，例如如針對RTP所規定。

RTP音訊有效負載類型特性2615可提供7位元整數有效負載時間，例如針對RTP所規定。

在各種實施例中，亦可針對串流媒體定義其他特性及服務。在一些實施例中，並非所有特性將用於每一個服務執行個體中。舉例而言，用於不接收或串流音訊之IP攝影機配件的配件模型可省略特性2610至

2615。

圖26D展示根據本發明之一實施例的用於攝影機服務2503之各種特性2651至2656之實例定義。若攝影機服務支援對應行為，則可定義此等特性(該等特性可為選用的)。控制器可寫入至此等特性以控制攝影機定向及成像行為。舉例而言，夜視特性2651可具有可用以啟用或停用夜視成像模式之布林值。

平移特性2652可用以控制攝影機之平移。舉例而言，攝影機可在水平面中可旋轉。平移之量可規定(例如)為攝影機相對於中心位置之最大水平旋轉的百分比。中心位置可經定義為具有零的平移值，其中平移特性2652之正值指示向右平移且平移特性2652之負值指示向左平移。可使用其他單位，諸如度。

類似地，傾斜特性2653可用以控制攝影機之傾斜角(例如，光軸相對於水平線之角)。傾斜之量可規定(例如)為攝影機相對於中心位置之最大傾斜的百分比。中心位置可經定義為具有零的傾斜值，其中傾斜特性2653之正值指示朝上傾斜且傾斜特性2652之負值指示負傾斜。可使用其他單位，諸如度。

旋轉特性2654可用以控制攝影機關於其光軸之旋轉角。旋轉量可(例如)按度規定。在一些實施例中，可使用列舉值(例如，以支援右90度、左90度、180度及不旋轉之旋轉設定)。

變焦特性2655可用以規定用於攝影機之變焦(或放大)因數。

鏡像特性2656可為用以指示在顯示、串流或儲存影像之前影像是否應經受鏡像處理變換(例如，關於豎軸之鏡像處理)的布林值。

圖26E展示可包括於圖25A之記錄服務2502及播放服務2503中之額外特性的定義。記錄控制特性2661可由控制器寫入以開始或停止記錄。值可為資料物件(例如，以TLV格式或其他金鑰值格式)，其可包括執行之操作(例如，開始記錄、停止記錄、排程記錄)的識別符及適合

操作之額外參數(例如，記錄之持續時間、經排程記錄之開始及/或停止時間等)。記錄狀態特性2662可由控制器讀取以判定記錄服務是否在記錄。值可為資料物件(例如，以TLV格式或其他金鑰值格式)，其可包括攝影機當前是否在記錄的指示；亦可包括其他資訊(例如，用於記錄之經排查結束時間、關於經排程之未來記錄之資訊、用於記錄之可用及/或已用儲存空間之量等)。

播放控制特性2663可由控制器寫入以控制儲存媒體內容(例如，先前記錄之內容)的播放。值可為資料物件(例如，以TLV格式或其他金鑰值格式)，其可包括執行之操作(例如，開始播放、暫停播放、結束播放等)的識別符。亦可包括額外參數，諸如待播放之內容項目之識別符。播放狀態特性2664可由控制器讀取以判定當前播放狀態。值可為資料物件(例如，以TLV格式或其他金鑰值格式)，其可包括播放是否在進行中的指示；亦可包括其他資訊(例如，正在播放之內容項目之識別符、該內容項目之持續時間、播放位置等)。播放速度特性2665可用以控制播放速度，其中值指示相對於1.0之正常播放速度的加速因數。在一些實施例中，用於播放速度特性2665之有效值可限於播放服務2503之特定執行個體支援的速度。

本文中所描述之服務及特性係出於說明目的。亦可定義其他服務及特性。舉例而言，為了促進識別待播放之特定內容項目，可能希望啟用控制器以巡覽(例如，瀏覽或搜尋)可用內容項目之資料庫或其他清單。可定義額外特性以促進控制器對資料庫之巡覽。此等特性可視需要包括於播放服務2503或不同服務(例如，內容瀏覽服務)中。

圖27A至圖27D一起展示根據本發明之一實施例的用於IP攝影機配件2404之配件物件2700。在此實例中，配件物件2700係以JSON表達且在結構上類似於圖3A至圖3C之配件物件300。亦可使用其他格式及語言。

圖27A中所示之配件資訊服務執行個體2702可類似或等同於上文所定義之配件資訊服務261。在此實例中，配件物件2700包括三個其他服務之執行個體：圖27B至圖27C中所示之IP攝影機串流服務2704 (符合圖25A之服務定義2501)、圖27D中所示之攝影機服務2706 (符合圖25B之服務定義2503)及圖27D中所示之麥克風服務2708 (符合圖25B之服務定義2504)。在此實例中，IP攝影機配件2404不具有揚聲器，亦不具有本機記錄或播放能力，且因此，未定義此等服務之執行個體。(可利用本發明之熟習此項技術者將能夠建構用於彼等服務之執行個體的適當配件物件)。在此實例中，每一特性執行個體之當前值係在配件物件2700中規定；空值係針對僅寫入特性規定。

圖24的與IP攝影機配件2404及控制器2402之使用者互動可類似於上文所述之互動。舉例而言，使用者可操作控制器2402以指示所要行為，且控制器2402可將請求(例如，HTTP請求)發送至配件2404以實現所要行為。圖28為根據本發明之一實施例的展示互動情境之程序2800之流程圖。

在區塊2802，使用者可設置IP攝影機配件2404。舉例而言，使用者可以所要操作位置及定向來置放或安裝攝影機、連接電力電纜、使配件2404處於配對模式中(若配件2404未自動地進入配對模式)等。在區塊2804，控制器2402可探索IP攝影機配件2404。舉例而言，如上所述，控制器2402可執行可實施圖4之程序400之控制器可執行部分的應用程式程式。該應用程式程式可回應於明確使用者指令或作為背景程序而執行，且使用者可經提示以確認已找到所要配件或自可用於配對之配件之清單選擇配件2404。在區塊2806，控制器2402及IP攝影機配件2404可建立對驗證工作階段。舉例而言，控制器2402及IP攝影機配件2404可執行上文所述之對設置程序中之任一者，繼而執行如上所述之對驗證程序。可視需要應用對設置期間之驗證要求；舉例而言，可

使用上文參考門鎖配件2004所描述之選項中之任一者。特定驗證要求可取決於特定IP攝影機配件之性質或意欲用途。舉例而言，建築物安全性攝影機可能需要多個形式之驗證，而消費型「網路攝影機」類型之攝影機可能僅需要攝影機處於配對模式中且使用者鍵入印刷在攝影機上之標籤上的設置碼。

在區塊2808，使用者可(例如)藉由發送將值「真」寫入至IP攝影機串流服務2704之「接通」特性(執行個體ID 8)的請求而使用配對控制器2402為IP攝影機配件2404通電。在此實例中，IP攝影機配件2404可具有低功率模式，在該模式中，該配件之收發器能夠自配對控制器接收信號，但其他服務(例如，配件物件2700中所列出之服務)被斷電。

如圖25A至圖25B中所示，服務2501至2505中之不同服務可各自具有單獨的「接通」特性。此可允許控制器藉由在服務執行個體被使用時選擇性地為該等服務執行個體供電來管理電力消耗。在一些實施例中，改變一個服務之「接通」特性可影響其他服務。舉例而言，對IP攝影機串流服務2501斷電可導致停止所有視訊串流之傳輸，但不需要停止麥克風服務2505或揚聲器服務2506之操作。IP攝影機串流服務2501可在其他服務保持關斷時通電，儘管若媒體串流為主動式，則與彼串流相關聯之任何服務執行個體應保持通電，或串流可停止。又，在一些實施例中，IP攝影機串流服務2501不允許新工作階段在與用於新工作階段之串流中之一者相關聯的服務執行個體被斷電的情況下開始。使IP攝影機服務2501斷電可終止所有媒體工作階段且自動地使其他相關服務執行個體(例如，麥克風服務2506、揚聲器服務2506)斷電。對IP攝影機服務2501通電可導致對所有相關服務執行個體通電(該等服務執行個體可隨後在未使用之情況下斷電)，儘管不需要恢復任何先前媒體工作階段。亦可實施其他電力管理規則。

在區塊2810，使用者可(例如)藉由與控制器2402之使用者介面互

動來指示控制器2402開始串流來自IP攝影機配件2404之視訊。舉例而言，使用者可指示該攝影機將串流視訊至控制器2402 (在一些實施例中，使用者可規定不同目的地器件)。作為回應，在區塊2812，控制器2402可產生並發送一請求至IP攝影機配件2404以開始媒體工作階段。

在一些實施例中，開始媒體工作階段請求可作為對IP攝影機配件2404之/characteristics URL之HTTP PUT請求而發送。一實例展示於圖29中以用於使用圖27A至圖27D之配件物件2700之實施例。請求訊息2900可具有訊息主體2902。訊息主體2902可包括待寫入之執行個體之執行個體識別符2904 (執行個體ID 9對應於IP攝影機服務執行個體2704 (圖27B)之工作階段開始特性)。值2906可包括可由IP攝影機配件2404使用以建立關於控制器2402之串流工作階段的資訊，諸如工作階段ID、IP位址及用於控制器2402之埠(或其他目的地器件)，及將用於SRTP串流資料之加密金鑰及salt。

在區塊2814，IP攝影機配件2404可發送對開始媒體工作階段請求之回應。在一些實施例中，該回應可作為HTTP回應來發送。實例展示於圖30中以用於開始媒體工作階段請求係如圖29所示之實施例。回應訊息3000可具有訊息主體3002。訊息主體3002可包括值3004。值3004可包括錯誤碼3002，其可具有指示成功完成(例如。錯誤碼0)或出現之特定錯誤(例如，無效參數、資源忙、拒絕存取等)的值。假定無錯誤，則值3004可提供可由控制器2402使用以連接至關於IP攝影機配件2404之串流工作階段的額外資訊，諸如配件之IP位址及埠，及配件之SRTP加密參數。

在此實例中，SRTP加密參數可包括於開始工作階段請求及回應中。應理解，此等參數不必無阻礙地發送。在請求2900及回應3000係在控制器2402與配件2404之間的對驗證工作階段內交換的實施例中，該等參數係以加密形式發送(使用對驗證工作階段之工作階段金鑰)且

因此免於遭受闖入者。

亦可實施該請求及回應之替代實施例。在上文所述之實例服務定義中，IP攝影機串流服務2501之給定執行個體具有相關聯轉碼器、屬性、有效負載等；此等可為服務執行個體之固定特性，且可定義不同組之特性以作為服務之不同執行個體。在其他實施例中，可使用不同實施。舉例而言，串流工作階段開始請求可充分利用SDP以組態可視所要安全性而使用RTP或SRTP傳遞之媒體串流。如本文中所使用，「媒體串流」可由一或多個「媒體流」(其中每一媒體流係音訊或視訊資料在一個方向上之傳送)製成。舉例而言，「單向視訊」串流可含有自IP攝影機配件2404至控制器2402之一個視訊流。「單向音訊」串流可含有自IP攝影機配件2404至控制器2402之一個音訊流。「單向音訊及視訊」串流可含有自IP攝影機配件2404至控制器2402之一個音訊流及一個視訊流。「單向視訊及雙向音訊」串流可含有自控制器2402至IP攝影機配件2404之一個音訊流及自IP攝影機配件2404至控制器2402之兩個媒體流(一個視訊，一個音訊)；後兩個流可同步。SDP可提供用於描述媒體工作階段之命名法及語法，包括媒體能力及傳輸參數。舉例而言，SDP支援描述以下資訊：媒體類型(例如，音訊、視訊)；媒體轉碼器(例如，LPCM音訊、H.264視訊)；網路傳輸(例如，接收IP位址及埠)；串流屬性(例如，僅接收、僅發送、發送及接收)；及媒體安全性(例如，是否使用SRTP)。SDP亦可提供用於協商控制器與攝影機配件之間的媒體工作階段之方便模型，其中該等器件集中於相互可接受之媒體設定，諸如媒體類型、媒體轉碼器等。

因此，在IP攝影機串流服務之一些替代實施中，控制器(例如，控制器2402)可將SDP提供包括於開始媒體工作階段請求內(例如，包括於請求2900中之資料物件內)。接收該請求之配件(例如，IP攝影機配件2404)可將SDP回應包括於其對開始媒體工作階段請求之回應內(例

如，包括於回應3000中之資料物件內)以作為對媒體工作階段請求之回應之部分。

再次參看圖28，一旦串流工作階段已建立，在區塊2816，IP攝影機配件2404可開始串流媒體至控制器2404 (或開始媒體工作階段請求中所規定之另一目的地器件)。所串流之特定媒體及串流格式可取決於配件之IP串流服務之特性；舉例而言，串流可包括視訊及/或音訊。此外，在一些情況下，串流服務可支援相反方向上之流，且彼流可同時開始。控制器2402 (或另一目的地器件)可呈現接收的媒體給使用者及/或儲存接收的媒體以供稍後呈現。媒體內容之串流可無限地繼續。

在某一點，在區塊2818，使用者可指示控制器2402停止媒體串流，例如藉由操作使用者介面之「停止」控制項。作為回應，在區塊2820，控制器2402產生並發送結束媒體工作階段請求至IP攝影機配件2404。圖31展示用於交換請求2900及回應3000之實施例的結束媒體工作階段請求訊息3100之實例。如同開始媒體工作階段請求2900，結束媒體工作階段請求3000可為HTTP PUT請求。請求訊息3100可具有訊息主體3102。訊息主體3102可包括待寫入之執行個體之執行個體識別符3104 (執行個體ID 10對應於IP攝影機服務執行個體2704 (圖27B)之工作階段結束特性)。值3106可包括可由IP攝影機配件2404使用以終止關於控制器2402之串流工作階段的資訊；在此實例中，該工作階段識別符足夠了。

再次參看圖28，在區塊2822，配件2404可發送對該請求之回應。圖32展示配件2404可回應於圖31之請求3100而產生的結束媒體工作階段回應3200之實例。回應訊息3200可具有訊息主體3202。訊息主體3202可包括值3204。值3204可包括指示錯誤是否出現之錯誤碼。該等錯誤碼可類似於用於回應於媒體工作階段開始請求之錯誤碼地定義。

在區塊2824，IP攝影機配件2404可停止串流媒體至控制器2402。

(若所定義之串流包括相反方向上之流，則彼流可同時結束)。在區塊2824之後，控制器2402及配件2404可保持在對驗證工作階段中，且控制器2402可在對驗證工作階段內再次起始串流及/或調用控制器2402之其他功能。

將瞭解，程序2800係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。在不同內容脈絡中，使用者可使用程序2800之適當部分於IP攝影機配件2404互動。在一些實施例中，可需要對驗證在執行某些動作(諸如開始或終止媒體工作階段)之前，或對驗證可為與IP攝影機串流服務之任何互動之先決條件。在對驗證工作階段內，所有請求及回應可加密。此外，儘管特定媒體相關協定(諸如SDP、RTP及SRTP)係用於說明目的，但其他協定可取代。

程序2800可理解為可藉由使用者操作控制器來控制配對配件執行的廣泛多種互動式控制操作之實例，包括(但不限於)媒體擷取操作。配件能夠執行的任何類型之功能或操作可類似於本文中所描述之彼等程序的程序來控制。

實例：串流介面

一些配件可支援本身與控制器之間的IP串流。如在上文之IP攝影機實例中，即時媒體串流係一個選項，但亦可支援其他類型之資料串流。舉例而言，可支援TCP或UDP串流。在一些實施例中，可需要配件以加密形式串流所有資料。舉例而言，對於TCP串流，可使用TLS-PSK(ChaCha20/Poly1305)，而對於UDP串流，可使用DTLS-PSK(ChaCha20/Poly1305)。在一些實施例中，IP串流之實施可類似於上文所述之IP攝影機服務實例。替代實施亦係可能的。現將描述一實例。

圖33展示根據本發明之一實施例的用於IP串流服務3301之實例服

務定義。特性在圖34中經定義為串流能力特性3401、串流控制輸入特性3402及串流控制結果3403。此等特性中之每一者可為資料物件，其金鑰及值可如所指示的。選用之「協定資訊(protocol-info)」金鑰(其值為物件)包括於每一特性3401至3403中，且此可用以提供額外的協定特定後設資料。

在此實例中，控制器可寫入至串流控制輸入特性3402以開啟或關閉串流且可藉由讀取串流控制結果特性3403來獲得串流之狀態。舉例而言，如上所述，配對控制器可訂用用於串流控制結果特性3403之事件通知，且只要串流控制結果特性3403之值改變，配件即可將非請求型事件回應發送至控制器。另外，配對控制器亦可讀取串流控制結果特性3403 (例如，使用如上所述之HTTP GET請求)。

在一些實施例中，配件可具有用以基於每個請求來判定是否回應以內嵌結果或查詢結果的選項。內嵌結果及查詢結果之實例在上文參看圖5G至圖5K來描述且可在此內容脈絡中應用。在此實例中，「接通(on)」未展示為IP串流服務3301之特性；必要時，其可包括於定義中。

支援IP串流之配件可將IP串流服務包括於其配件模型中。可利用本發明之熟習此項技術者將能夠以JSON或其他描述語言或記數法來組成適當表示。

圖35為根據本發明之一實施例的用於可由控制器執行之IP串流之程序3500的流程圖。在區塊3502，控制器可與具有如圖33及圖34中所定義之IP串流服務的配件配對。舉例而言，可使用上文所述之對設置及對驗證程序，且控制器可讀取配件定義記錄以判定配件具有IP串流服務。

在區塊3504，控制器可(例如)藉由發送關於串流能力特性3401之HTTP GET請求而自配件讀取串流能力特性3401。此請求可根據上文所述之實例來建構。在區塊3506，控制器可產生串流識別符；可使用用

於產生識別符(例如，UUID)之習知技術。在區塊3508，控制器可(例如)藉由發送對請求類型(request-type)為1且串流id (stream-id)經設定為區塊3506處所產生之串流識別符之串流控制輸入特性3402的HTTP PUT請求而將「開啟串流(open stream)」請求發送至配件。其他資訊(諸如用於串流工作階段之IP位址及埠)可包括於(例如)協定資訊物件中。請求可根據上文所述之實例來建構。

在區塊3510，控制器可自配件接收回應。在一些實施例中，該回應可為內嵌結果回應(例如，類似於圖5I之回應573)或查詢結果回應，從而在控制器讀取串流控制結果特性3403之後建立異動id (transaction-id)及參考所建立之異動id (例如，類似於圖5J之回應574及圖5K的後續請求578)。在任一情況下，該回應可包括一埠識別符及可由控制器使用以連接至串流工作階段之任何其他資訊。

在區塊3512，控制器可使用提供於該回應中之資訊而連接至串流工作階段。在區塊3514，控制器可設置用於資料串流之加密。舉例而言，用於TLS或DTLS加密之金鑰(傳輸層安全性或資料包傳輸層安全性，例如記錄於IETF RFC 4279或IETF Draft draft-keoh-lwig-dtls-iot-01，可在https://tools.ietf.org/html/draft-keoho-lwig-dtls-iot-01得到)可自在對設置或對驗證(在區塊3502)期間所產生之共用秘密及串流ID (在區塊3506所產生)衍生。配件可自相同資訊衍生金鑰。在區塊3516，該等器件可串流經加密資料。資料可視需要而在任一方向或兩個方向上流動(自控制器至配件及/或自配件至控制器)。

當控制器決定中止串流時，在區塊3518，控制器可(例如)藉由發送對請求類型(request-type)為2且串流id (stream-id)經設定為區塊3506處所產生之串流識別符之串流輸入點特性3402的HTTP PUT請求來發送「關閉串流(close stream)」請求。此請求亦可根據上文所述之實例建構。在區塊3520，控制器可接收確認配件已關閉埠之回應。此回應

可以相同於區塊3510處之回應的方式提供。

將瞭解，程序3500係說明性的且變化及修改係可能的。描述為順序之步驟可並列執行，步驟之次序可改變，且步驟可修改、組合、新增或省略。串流服務可提供用於在配件與控制器之間的任一方向上安全地串流任何種類之資料的一般IP串流介面。在所展示之實例中，TCP及UDP並非即時協定。其他實施例可(例如)使用上文所述之IP攝影機串流服務或類似服務來提供即時串流。

在一些實施例中，控制器可訂用通知以允許配件在配件之狀態改變之情況下(例如，在錯誤在串流期間出現之情況下)警示控制器。舉例而言，參看圖34，控制器可針對串流控制結果特性3403訂用事件通知(或可支援的其他類型之通知)。若串流狀態在配件端改變，則配件可更新狀態碼並產生通知(例如，如上所述之非請求型事件訊息)至控制器。

實例器件

本文中所描述之實施例可實施於電子器件中，該等電子器件可具有大體上習知設計且經調適以符合統一配件協定以支援命令及控制操作，控制器(第一電子器件)可藉由該等操作來控制配件(第二電子器件)之操作。

圖36為根據本發明之一實施例的控制器3600之簡化方塊圖。控制器3600可實施本文中所描述之控制器功能、行為及能力中之任一者或全部，以及未明確描述之其他功能、行為及能力。控制器3600可包括處理子系統3610、儲存器件3612、使用者介面3614、通信介面3616、安全元件3618及密碼編譯邏輯模組3620。控制器3600亦可包括其他組件(未明確展示)，諸如電池、功率控制器及可操作以提供各種增強型能力之其他組件。在各種實施例中，控制器3600可實施於桌上型電腦、膝上型電腦、平板電腦、智慧型手機、可穿戴式計算器件或具有任何

所要外觀尺寸之其他系統中。此外，如上文所指出，控制器3600可部分地實施於基地台中且部分地實施於與基地台通信且提供使用者介面之行動單元中。

儲存器件3612可(例如)使用磁碟、快閃記憶體或任何其他非暫時性儲存媒體或媒體之組合來實施，且可包括揮發性及/或非揮發性媒體。在一些實施例中，儲存器件3612可儲存待由處理子系統3610執行之一或多個應用程式及/或作業系統程式，包括用以實施本文中描述為由控制器執行之任何或所有操作的程式。舉例而言，儲存器件3612可儲存可讀取配件定義記錄並產生用於基於其中之資訊來控制控配件之圖形使用者介面的統一控制器應用程式。在一些實施例中，本文中所描述之控制器功能性之部分(或全部)可以作業系統程式而非應用程式來實施。在一些實施例中，儲存器件3612亦可儲存針對特定配件或特定類別之配件設計的應用程式(例如，用以管理IP配件配件之IP攝影機應用程式或用以與門鎖配件互動之安全性應用程式)。

使用者介面3614可包括輸入器件(諸如觸控板、觸控式螢幕、滾輪、點選輪、撥號盤、按鈕、開關、小鍵盤、麥克風或類似者)，以及輸出器件(諸如視訊螢幕、指示燈、揚聲器、頭戴式耳機插口或類似者)，連同支援電子(例如，數位至類比或類比至數位轉換器、信號處理器或類似者)。使用者可操作使用者介面3614之輸入器件以調用控制器3600之功能性且可經由使用者介面3614之輸出器件而看到及/或聽到來自控制器3600之輸出。

處理子系統3610可實施為一或多個積體電路(例如一或多個單核心或多核心微處理器或微控制器)，該一或多個積體電路之實例是此項技術中已知的。在操作中，處理子系統3610可控制控制器3600之操作。在各種實施例中，處理子系統3610可回應於程式碼而執行多種程式且可為多個同時執行之程式或程序。在任何給定時間，待執行之程式碼

中之一些或全部可駐留於處理子系統3610中及/或諸如儲存器件3612之儲存媒體中。

經由合適程式設計，處理子系統3610可為控制器3600提供各種功能性。舉例而言，在一些實施例中，處理子系統3610可實施上文描述為藉由控制器實施之各種程序(或其部分)。處理子系統3610亦可執行用以控制控制器3600之其他功能的其他程式，包括可儲存於儲存器件3612中之程式。在一些實施例中，此等程式可(例如)藉由產生待發送至配件之訊息及/或自配件接收訊息而與配件互動。此等訊息可符合如上所述之統一配件協定。

通信介面3616可為控制器3600提供語音及/或資料通信能力。在一些實施例中，通信介面3616可包括用於存取無線語音及/或資料網路(例如，使用蜂巢式電話技術、諸如3G、4G/LTE、Wi-Fi (IEEE 802.11同族標準)之資料網路技術，或其他行動通信技術，或其任何組合)的射頻(RF)收發器組件、用於短程無線通信(例如，使用藍芽及/或藍芽LE標準、NFC等)的組件及/或其他組件。在一些實施例中，除無線介面外或替代無線介面，通信介面3616亦可提供有線網路連接性(例如，乙太網路)。通信介面3616可使用硬體組件(例如，驅動器電路、天線、調變器/解調變器、編碼器/解碼器及其他類比及/或數位信號處理電路)與軟體組件之組合來實施。在一些實施例中，通信介面3616可使用相同傳輸或不同傳輸來同時支援多個通信頻道。

安全儲存模組3618可為可安全地儲存用於控制器3600之密碼編譯資訊的積體電路或類似者。可儲存於安全儲存模組3618內之資訊之實例包括控制器之長期公用及秘密金鑰3622 (如上所述之LTPKC、LTSKC)，及配對配件之清單3624 (例如，將配件ID映射至用於已完成如上所述之對設置或對新增程序的配件之配件長期公用金鑰LTPKA的查找表)。

在一些實施例中，密碼編譯操作可實施於與安全儲存模組3618通信之密碼編譯邏輯模組3620中。實體上，密碼編譯邏輯模組3620可視需要而實施於具有安全儲存模組3618之同一積體電路或不同積體電路(例如，處理子系統3610中之處理器)中。密碼編譯邏輯模組3620可包括實施或支援控制器3600之密碼編譯操作(包括上文所述之任何或所有密碼編譯操作)的各種邏輯電路(視需要固定或可程式化)。安全儲存模組3618及/或密碼編譯邏輯模組3620對控制器3600之其餘部分可表現為「黑箱」。因此，舉例而言，通信介面3616可接收呈該通信介面不能解密之加密形式的訊息且可僅將該訊息傳遞至處理子系統3610。處理子系統3610亦可能不能解密該訊息，但處理子系統可將該訊息辨識為經加密且將該訊息傳遞至密碼編譯邏輯模組3620。密碼編譯邏輯模組3620可解密該訊息(例如，使用自安全儲存模組3618提取之資訊)且判定將什麼資訊傳回至處理子系統3610。結果，某些資訊僅可在安全儲存模組3618及密碼編譯邏輯模組3620內得到。若安全儲存模組3618及密碼編譯邏輯模組3620係實施於僅執行來自內部安全儲存庫之碼的單一積體電路上，則此可使提取該資訊極其困難，此可提供高度安全性。其他實施亦係可能的。

圖37為根據本發明之一實施例的配件3700之簡化方塊圖。配件3700可實施本文中所描述之配件功能、行為及能力中之任一者或全部，以及未明確描述之其他功能、行為及能力。配件3700可包括儲存器件3728、處理子系統3730、使用者介面3732、配件特定硬體3734、通信介面3736、安全元件3738及密碼編譯邏輯模組3740。配件3700亦可包括其他組件(未明確展示)，諸如電池、功率控制器及可操作以提供各種增強型能力之其他組件。

配件3700表示可由諸如控制器3600之控制器操作的廣泛類別之配件，且此等配件可在能力、複雜度及外觀尺寸上廣泛地變化。各種

配件可包括圖37中未明確展示之組件，包括(但不限於)：具有固定或抽取式儲存媒體之儲存器件(磁碟、快閃記憶體等)；用於連接至外部音訊/視訊器件之視訊螢幕、揚聲器或埠；攝影機組件，諸如透鏡、影像感測器及其控制項(例如，孔隙、變焦、曝光時間圖框率等)；用於記錄音訊之麥克風(單獨地或與視訊記錄結合)；等。

儲存器件3728可(例如)使用磁碟、快閃記憶體或任何其他非暫時性儲存媒體或媒體之組合來實施，且可包括揮發性及/或非揮發性媒體。在一些實施例中，儲存器件3728可儲存待由處理子系統3730執行之一或多個程式，該一或多個程式包括用以實施上文描述為由配件執行之各種操作以及與特定配件行為相關之操作的程式。儲存器件3728亦可儲存可供給至例如如上所述之控制器器件的配件物件或配件定義記錄(例如，如上所述)。儲存器件3728亦可儲存配件狀態資訊及可在配件3700之操作期間使用的任何其他資料。

處理子系統3730可包括(例如)執行程式碼以執行與配件3700相關聯之各種功能的一或多個單核心或多核心微處理器及/或微控制器。舉例而言，處理子系統3730可實施本文中描述為由配件實施(例如藉由執行儲存於儲存器件3728中之程式碼)的任何或所有操作。處理子系統3730亦可執行其他程式以控制配件3730之其他功能。在一些情況下，由處理子系統3730執行之程式可(例如)藉由產生待發送至控制器之訊息及/或自控制器接收訊息而與控制器(例如，控制器3600)互動。此等訊息可符合如上所述之統一配件協定。

使用者介面3732可包括使用者可操作之輸入器件(諸如觸控板、觸控式螢幕、滾輪、點選輪、撥號盤、按鈕、開關、小鍵盤、麥克風或類似者)，以及輸出器件(諸如視訊螢幕、指示燈、揚聲器、頭戴式耳機插口或類似者)，連同支援電子(例如，數位至類比或類比至數位轉換器、信號處理器或類似者)。視特定配件3700之實施而定，使用者可

操作使用者介面3732之輸入器件以調用配件3700之功能性且可經由使用者介面3734之輸出器件而看到及/或聽到來自配件3700之輸出。一些配件可提供最少使用者介面或無使用者介面。

配件特定硬體3734可包括可存在於配件3700中以實現或支援其功能性之任何其他組件。舉例而言，在各種實施例中，配件特定硬體3734可包括：使用固定或抽取式儲存媒體之一或多個儲存器件；GPS接收器；電源供應器及/或電力管理電路；攝影機；麥克風；一或多個致動器；環境感測器(例如，溫度感測器、壓力感測器、加速計、化學感測器等)；等。應理解，任何類型之配件功能性可藉由提供適當配件特定硬體3734來支援。

通信介面3736可為配件3700提供語音及/或資料通信能力。在一些實施例中，通信介面3736可包括用於存取無線語音及/或資料網路(例如，使用蜂巢式電話技術、諸如3G、4G/LTE、Wi-Fi (IEEE 802.11同族標準)之資料網路技術，或其他行動通信技術，或其任何組合)的射頻(RF)收發器組件、用於短程無線通信(例如，使用藍芽及/或藍芽LE標準、NFC等)的組件及/或其他組件。在一些實施例中，除無線介面外或替代無線介面，通信介面3736亦可提供有線網路連接性(例如，乙太網路)。通信介面3736可使用硬體組件(例如，驅動器電路、天線、調變器/解調變器、編碼器/解碼器及其他類比及/或數位信號處理電路)與軟體組件之組合來實施。在一些實施例中，通信介面3736可使用相同傳輸或不同傳輸來同時支援多個通信頻道。

安全儲存模組3738可為可安全地儲存用於配件3700之密碼編譯資訊的積體電路或類似者。可儲存於安全儲存模組3738內之資訊之實例包括配件之長期公用及秘密金鑰3742 (如上所述之LTPKA、LTSKA)，及配對控制器之清單3744 (例如，將控制器ID映射至用於已完成如上所述之對設置或對新增程序的控制器之控制器長期公用金鑰

LTPKC的查找表)。

在一些實施例中，密碼編譯操作可實施於與安全儲存模組3738通信之密碼編譯邏輯模組3740中。實體上，密碼編譯邏輯模組3740可視需要而實施於具有安全儲存模組3738之同一積體電路或不同積體電路(例如，處理子系統3730中之處理器)中。密碼編譯邏輯模組3740可包括實施或支援配件3700之密碼編譯操作(包括上文所述之任何或所有密碼編譯操作)的各種邏輯電路(視需要固定或可程式化)。安全儲存模組3738及/或密碼編譯邏輯模組3740對配件3700之其餘部分可表現為「黑箱」。因此，舉例而言，通信介面3736可接收呈該通信介面不能解密之加密形式的訊息且可僅將該訊息傳遞至處理子系統3730。處理子系統3730亦可能不能解密該訊息，但處理子系統可將該訊息辨識為經加密且將該訊息傳遞至密碼編譯邏輯模組3740。密碼編譯邏輯模組3740可解密該訊息(例如，使用自安全儲存模組3738提取之資訊)且判定將什麼資訊傳回至處理子系統3730。結果，某些資訊僅可在安全儲存模組3738及密碼編譯邏輯模組3740內得到。若安全儲存模組3738及密碼編譯邏輯模組3740係實施於僅執行來自內部安全儲存庫之碼的單一積體電路上，則此可使提取該資訊極其困難，此可提供高度安全性。其他實施亦係可能的。

配件3700可為與諸如控制器3600之控制器互動之任何電子裝置。在一些實施例中，控制器3600可提供對配件3700之操作的遠端控制，如上所述。舉例而言，控制器3600可提供用於配件3700之遠端使用者介面，其可包括輸入及輸出控制項兩者(例如，用以顯示自配件3700獲得之當前狀態資訊的顯示螢幕，及諸如用以允許狀態資訊改變之觸控式螢幕覆疊片的輸入控制項)。各種實施例中之控制器3600可控制配件3700之任何功能且亦可自配件3700接收資料。

圖38展示根據本發明之一實施例的用於控制器3800之控制器架

構之實例。該控制器架構經展示為一組互動子系統，其中每一子系統包括一或多個模組。應理解，該等模組中之每一者可使用執行於一或多個可程式化處理器上之程式碼來實施及/或實施於一或多個固定功能處理器中，且該(該等)處理器可包括用以控制其他硬體器件之輸出發信(例如，致動器、顯示器等)及/或用以自其他硬體器件接收信號之輸入發信(例如，鍵盤；觸控式螢幕；來自致動器、馬達或感測器之回饋或狀態信號；等)。該等子系統中之一些可包括持續性資料儲存器，其可使用任何之非揮發性儲存器件(例如，半導體快閃記憶體、EEPROM、磁碟或光碟等)來實施。儘管未圖示，但該等子系統中之一些或全部可包括額外硬體元件，諸如顯示器、鍵盤、觸控式螢幕、麥克風、揚聲器、感測器等。

安全性子系統3802可包括安全儲存元件3804、對設置模組3806、對驗證模組3808、對新增模組3810、對移除模組3812及密碼編譯邏輯模組3814。安全儲存元件3804可類似或等同於上文所述之安全儲存元件3618或其他安全儲存元件。在一些實施例中，安全儲存元件3804用以安全地儲存用於控制器3800之長期公用/秘密金鑰對(例如，如上所述之LTPKC、LTSKC)以及用於每一配件(控制器3800具有與該配件之已建立配對)之配對記錄。如上所述，每一配對記錄可包括配對配件之識別符、該配對配件之長期公用金鑰，及視情況之其他資訊，諸如用於控制器3800與該配對配件之互動的權限設定(例如，控制器3800是否具有管理員權限)。在控制器3800關於不同配件使用不同長期公用金鑰之實施例中，每一配對記錄亦可包括待供配對配件使用之長期公用金鑰的指示符。必要時，可包括其他資訊。

對設置模組3806可實施對設置程序之控制器部分。對設置程序可為控制器3800及配件藉以安全地交換每一器件可隨後使用以驗證另一者之身分識別的長期公用金鑰之任何程序。在一些實施例中，對設置

程序可包括控制器3800與配件之間的資訊項目(例如，設置碼、配件之安全性憑證之驗證)的頻帶外交換以驗證配件之身分識別。可使用上文所述之對設置程序(例如，程序1300、1400、1500及/或1600)或其他程序中之任一者。在一些實施例中，對設置模組3806可與配件互動子系統3850 (描述如下)互動以在對設置期間實現與配件之通信。在一些實施例中，對設置模組3806可調用密碼編譯邏輯模組3814之功能以執行關於對設置程序之密碼編譯操作。

對驗證模組3808可實施對驗證程序之控制器部分。對驗證程序可為控制器3800及配件藉以使用先前儲存之長期公用金鑰以驗證另一器件之身分識別的任何程序。可使用上文所述之對驗證程序(例如，程序1700)或其他程序中之任一者。在一些實施例中，對驗證模組3808可與配件互動子系統3850 (描述如下)互動以在對驗證期間實現與配件之通信。在一些實施例中，對驗證模組3808可調用密碼編譯邏輯模組3814之功能以執行關於對驗證程序之密碼編譯操作。

對新增模組3810可實施對新增程序之控制器部分。對新增程序可為控制器3800在與配件建立配對之後藉以將用於「新」控制器(配件將與之建立配對)之長期公用金鑰提供至配件的任何程序；該新控制器可為不同於控制器3800之器件。可使用上文所述之對新增程序(例如，程序1800)或其他程序中之任一者。在一些實施例中，對新增模組3810可與配件互動子系統3850 (描述如下)互動以在對新增期間實現與配件之通信。在一些實施例中，對新增模組3810亦可與另一控制器或金鑰資訊之其他外部源通信以獲得用於待新增之新控制器的長期公用金鑰(或憑證)。在一些實施例中，對新增模組3810可調用密碼編譯邏輯模組3814之功能以執行關於對驗證程序之密碼編譯操作。

對移除模組3812可實施對移除程序之控制器部分。對移除程序可為控制器3800在與配件建立配對之後藉以將配對待由配件移除之控制

器之識別符提供至配件的任何程序；已移除控制器可為不同於控制器3800之器件。可使用上文所述之對移除程序(例如，程序1900)或其他程序中之任一者。在一些實施例中，對移除模組3812可與配件互動子系統3850 (描述如下)互動以在對移除期間實現與配件之通信。在一些實施例中，對移除模組3812亦可與另一控制器或資訊之其他外部源通信以獲得用於待移除之控制器之識別資訊。在一些實施例中，對移除模組3808可調用密碼編譯邏輯模組3812之功能以執行關於對移除程序之密碼編譯操作。

密碼編譯邏輯模組3814可實施可由控制器3800使用之密碼編譯演算法。實例包括：金鑰產生演算法；用於SRP中之演算法及函數；雜湊演算法；基於金鑰之加密/解密演算法，諸如ChaCha20-Poly1305、Curve25519、Ed25519及/或其他演算法。在一些實施例中，密碼編譯邏輯模組3814可提供可由控制器3800之其他模組使用以調用密碼編譯演算法及相關服務的API (應用程式介面)。可支援任何數目及組合之密碼編譯演算法及相關服務。

使用者互動子系統3830可管理與控制器3800之使用者的互動。舉例而言，使用者介面產生模組3832可產生待呈現給使用者(例如，在顯示器件上)之使用者介面。該使用者介面可包括可由使用者操作以與配件互動之控制元件。舉例而言，如上所述，控制器3800可基於提供於配件物件中之資訊來顯現圖形使用者介面。使用者輸入接收器模組3834可自使用者介面接收輸入且處理該輸入以判定回應於該輸入將採取之動作(例如，產生待發送至配件之訊息)。在一些實施例中，使用者輸入接收器模組3834可回應於使用者輸入而調用控制器3800之其他模組之功能。

配件互動子系統3850可支援控制器3800與配件之間的互動。配件物件儲存元件3852可使用揮發性或非揮發性儲存媒體(例如，半導體快

閃記憶體、EEPROM、DRAM、SRAM、磁碟或光碟等)來實施。在一些實施例中，配件物件儲存元件3852可用以儲存每一配件之表示，控制器3800具有針對配件之資訊。舉例而言，如上所述，在與配件建立配對之後，諸如控制器3800之可自配件獲得配件定義記錄，該配件定義記錄可包括一或多個配件物件。控制器3800可將如此獲得之配件物件儲存於配件物件儲存元件3852中。所儲存之配件物件可以許多方法使用，包括產生使用者介面(例如，藉由使用者介面產生模組3832)、解譯使用者輸入(例如，藉由使用者輸入接收器模組3834)、產生對配件之請求及/或自配件接收回應或通知。

配件探索模組3854可執行與探索配件相關之操作，例如收聽廣播、判定是否與所探索配件配對等。舉例而言，配件探索模組3854可實施上文參看圖4所描述之控制器操作。

請求產生模組3856可產生並發送請求至配件。舉例而言，回應於來自使用者輸入接收器模組3834之指令(例如，解除鎖定門)，請求產生模組3856可產生適當請求訊息至配件(例如，寫入至如上所述之鎖定狀態特性)。請求訊息之實例係在上文描述。在一些實施例中，產生該訊息可包括加密該訊息，且請求產生模組3856可調用由密碼編譯邏輯模組3814支援的關於產生請求之功能。在一些實施例中，請求產生模組3856可與安全性子系統3802互動以在對設置、對驗證、對新增或對移除操作期間產生並發送請求至配件(例如，上文參看圖13至圖19所描述之請求中之任一者)。

回應處理模組3858可接收並處理對可自配件接收之請求訊息的任何回應。舉例而言，在請求產生模組3856將請求訊息發送至配件(例如，以寫入至如上所述之鎖定狀態特性)之後，回應處理模組3858可自配件接收回應訊息且可解譯該訊息。在一些實施例中，該回應訊息可以加密形式接收，且回應處理模組3858可調用由密碼編譯邏輯模組

3814支援的關於解釋該回應之功能。回應處理模組3858亦可基於該回應(例如，狀態碼、錯誤是否出現等)而將資訊提供至使用者介面子系統3830，且使用者介面子系統3830可基於此資訊而產生回饋至使用者。在一些實施例中，回應處理模組3858亦可基於包括於該回應訊息中之資訊來更新配件物件儲存元件3852。在一些實施例中，回應處理模組3858可與安全性子系統3802互動以在對設置、對驗證、對新增或對移除操作期間接收並處理自配件接收之回應(例如，上文參看圖13至圖19所描述之回應中之任一者)。

通知處理模組3860可接收並處理可自配件接收之通知訊息。如上所述，可支援各種通知機制，且通知處理模組3860可支援此等通知機制中之任一者或全部(例如，上文所述之程序700、800、900、1000中之任一者或全部)。舉例而言，就被動式通知而言，通知處理模組3860可比較藉由配件報告之狀態計數器值與儲存的狀態計數器值(例如，在配件物件儲存元件3852中)且可偵測不一致。在一些實施例中，在偵測不一致後，通知處理模組3860隨即可指示請求產生模組3856產生並發送請求至配件以獲得額外狀態資訊(例如，經更新之配件定義記錄或其部分)。就廣告式通知而言，通知處理模組3860可處理經由配件探索模組3854接收之廣告以偵測已知配件的狀態改變(例如，基於儲存於儲存元件3852中之配件物件之狀態計數器)。就事件通知而言，非請求型回應訊息可由回應處理模組3858接收，該回應處理模組可將該訊息辨識為非請求型回應(例如，如上所述之EVENT訊息)且可將該訊息提供至通知模組3860以供進一步處理。不管特定通知機制如何，通知模組3860可判定改變之狀態資訊的性質並將適當資訊提供至互動子系統3830。在一些實施例中，通知模組3860亦可更新配件物件儲存元件3852中之儲存的配件物件。

通信介面模組3870可提供服務以支援與包括配件之其他器件的

通信。在一些實施例中，通信介面模組3870可實施藍芽LE協定堆疊3872及/或HTTP/IP協定堆疊3874。藍芽LE協定堆疊3872可根據藍芽LE傳輸協定來提供傳出訊息之格式化及接收的訊息之解譯。HTTP/IP協定堆疊3874可根據HTTP及IP傳輸協定來提供傳出訊息之格式化及接收的訊息之解譯。儘管使用藍芽LE及HTTP/IP作為實例，但應理解，傳輸協定之任何組合在通信介面模組3870內可得到支援且控制器3800之給定例子可支援一或多個傳輸協定。如上所述，控制器3800在器件互動之用戶端/伺服器模型中可充當客戶端器件，且藍芽LE協定堆疊3872及/或HTTP/IP協定堆疊3874可經組態以支援用戶端行為。

在一些實施例中，通信介面模組3870內之協定堆疊可經修改以辨識某些非標準訊息。舉例而言，如上所述，HTTP/IP協定堆疊3874可經組態以辨識來自配件之非請求型「事件」訊息(例如，上文所述的圖11B之事件訊息1120)。

在一些實施例中，通信介面模組3870可提供可由其他模組使用以發送及/或接收訊息至外部器件的API。該API可經設計以為傳輸不可知的，且對用於特定訊息之傳輸的選擇可在通信介面模組3870內以對控制器3800內之其他模組透明的方式進行。在控制器3800之通信埠(未圖示)接收之訊息可基於埠組態而發送至藍芽LE堆疊3872或HTTP/IP堆疊3874，且藍芽LE堆疊3872及HTTP/IP堆疊3874中之每一者可將傳出訊息發送至經適當組態之通信埠。

圖39展示根據本發明之一實施例的用於配件3900之配件架構之實例。該配件架構經展示為一組互動子系統，其中每一子系統包括一或多個模組。應理解，該等模組中之每一者可使用執行於一或多個可程式化處理器上之程式碼來實施及/或實施於一或多個固定功能處理器中，且該(該等)處理器可包括用以控制其他硬體器件之輸出發信(例如，致動器、顯示器等)及/或用以自其他硬體器件接收信號之輸入發

信(例如，鍵盤；觸控式螢幕；來自致動器、馬達或感測器之回饋或狀態信號；等)。該等子系統中之一些可包括持續性資料儲存器，其可使用任何之非揮發性儲存器件(例如，半導體快閃記憶體、EEPROM、磁碟或光碟等)來實施。儘管未圖示，但該等子系統中之一些或全部可包括額外硬體元件，諸如顯示器、鍵盤、觸控式螢幕、麥克風、揚聲器、馬達、致動器感測器等。

安全性子系統3902可包括安全儲存元件3904、對設置模組3906、對驗證模組3908、對新增模組3910、對移除模組3912及密碼編譯邏輯模組3914。安全儲存元件3904可類似或等同於上文所述之安全儲存元件3738或其他安全儲存元件。在一些實施例中，安全儲存元件3904用以安全地儲存用於配件3900之長期公用/秘密金鑰對(例如，如上所述之LTPKA、LTSKA)以及用於每一控制器(配件3900具有與該控制器之已建立配對)之配對記錄。如上所述，每一配對記錄可包括配對控制器之識別符、該配對控制器之長期公用金鑰，及視情況之其他資訊，諸如用於配對控制器與配件3900之互動的權限設定(例如，配對控制器是否具有管理員權限)及/或用於配對控制器之訂用設定(例如，控制器是否已訂用除被動模式外之特定通知模式的指示符)。在配件3900關於不同控制器使用不同長期公用金鑰之實施例中，每一配對記錄亦可包括待供配對控制器使用之長期公用金鑰的指示符。必要時，可包括其他資訊。

對設置模組3906可實施對設置程序之配件部分。對設置程序可為配件3900及控制器藉以安全地交換每一器件可隨後使用以驗證另一者之身分識別的長期公用金鑰之任何程序。在一些實施例中，對設置程序可包括配件3900與控制器之間的資訊項目(例如，設置碼、配件之安全性憑證之驗證)的頻帶外交換以驗證配件3900之身分識別。可使用上文所述之對設置程序(例如，程序1300、1400、1500及/或1600)或其他

程序中之任一者。在一些實施例中，對設置模組3906可與控制器互動子系統3950 (描述如下)互動以在對設置期間實現與控制器之通信。在一些實施例中，對設置模組3906可調用密碼編譯邏輯模組3914之功能以執行關於對設置程序之密碼編譯操作。

對驗證模組3908可實施對驗證程序之配件部分。對驗證程序可為配件3900及控制器藉以使用先前儲存之長期公用金鑰以驗證另一器件之身分識別的任何程序。可使用上文所述之對驗證程序(例如，程序1700)或其他程序中之任一者。在一些實施例中，對驗證模組3908可與控制器互動子系統3950 (描述如下)互動以在對驗證期間實現與控制器之通信。在一些實施例中，對驗證模組3908可調用密碼編譯邏輯模組3914之功能以執行關於對驗證程序之密碼編譯操作。

對新增模組3910可實施對新增程序之配件部分。對新增程序可為具有與配件3900之已建立配對之控制器藉以將用於「新」控制器(配件3900將與之建立配對)之長期公用金鑰提供至配件3900的任何程序。可使用上文所述之對新增程序(例如，程序1800)或其他程序中之任一者。在一些實施例中，對新增模組3910可與控制器互動子系統3950 (描述如下)互動以在對新增期間實現與先前配對之控制器之通信。在一些實施例中，對新增模組3910亦可與金鑰資訊之外部源通信以獲得用於待新增之新控制器的長期公用金鑰(或憑證)。在一些實施例中，對新增模組3910可調用密碼編譯邏輯模組3914之功能以執行關於對驗證程序之密碼編譯操作。

對移除模組3912可實施對移除程序之配件部分。對移除程序可為具有與配件3900之已建立配對之控制器藉以將配對待由配件3900移除之控制器的識別符提供至配件3900的任何程序；已移除控制器可為不同於調用對移除程序之控制器的器件。可使用上文所述之對移除程序(例如，程序1900)或其他程序中之任一者。在一些實施例中，對移除

模組3912可與配件互動子系統3950 (描述如下)互動以在對移除期間實現與配件之通信。在一些實施例中，對移除模組3912亦可與另一控制器或資訊之其他外部源通信以獲得用於待移除之控制器之識別資訊。在一些實施例中，對移除模組3908可調用密碼編譯邏輯模組3914之功能以執行關於對移除程序之密碼編譯操作。

密碼編譯邏輯模組3914可實施可由配件3900使用之密碼編譯演算法。實例包括：金鑰產生演算法；用於SRP中之演算法及函數；雜湊演算法；基於金鑰之加密/解密演算法，諸如ChaCha20-Poly1305、Curve25519、Ed25519及/或其他演算法。在一些實施例中，密碼編譯邏輯模組3914可提供可由配件3900之其他模組使用以調用密碼編譯演算法及相關服務的API (應用程式介面)。可支援任何數目及組合之密碼編譯演算法及相關服務。

配件動作子系統3930可(例如)回應於經由控制器互動子系統3950自控制器接收之請求而管理配件3900之硬體及/或軟體組件之各種操作。舉例而言，配件3900可併有可採取特定動作(例如，開啟或關閉門、操作攝影機等)之各種操作組件3932 (或與該等操作組件通信)。操作組件3932可包括硬體及/或軟體組件，且給定操作組件3932可回應來自執行器模組3934之接收的控制信號(例如，數位或類比形式之電信號)及/或產生至回饋模組3936之回饋信號(例如，數位或類比形式之電信號)。

執行器模組3934可產生至操作組件3932之控制信號(例如)以實現或實施使用者所請求之操作。該等特定信號可取決於將定址之特定操作組件3932。以說明方式，操作組件3932可包括可對開關通電或斷電之開關電路，且執行器模組3934可產生至該開關電路之信號以接通或關斷電力。作為另一實例，操作組件3932可包括機電致動器，其可回應於電控制信號而產生實體物件之運動(例如，閂鎖或解除閂鎖死栓、開啟或關閉門)，且執行器模組3934可產生至該致動器之信號。作為再

一實例，操作組件3932可包括用於控制數位攝影機之API (視實施而定，攝影機本身可為或可不為操作組件)，且執行器模組3934可調用API呼叫以控制數位攝影機。在各種實施例中，執行器模組3934可回應於來自控制器的經由控制器介面子系統3950接收之請求及/或在配件3900之使用者介面處所接收之輸入而操作。

回饋模組3936可自操作組件3932接收回饋信號。該等特定信號可取決於特定操作組件3932。舉例而言，開關電路可提供指示開關之當前狀態的回饋信號。機電致動器可提供指示當前狀態(例如，實體物件之位置及/或運動)之回饋信號。API可提供錯誤或狀態碼(例如，在自API呼叫傳回後)。作為另一實例，操作組件3932可包括用於各種環境條件之一或多個感測器(例如，運動感測器、位置感測器、溫度感測器、障礙感測器等)，且回饋模組3936可自該等感測器接收感測器資料信號。在一些實施例中，回饋模組3936可將基於接收的回饋信號之回饋資訊提供至控制器互動子系統3950。

控制器互動子系統3950可支援配件3900與控制器之間的互動。配件物件儲存元件3952可使用揮發性或非揮發性儲存媒體(例如，半導體快閃記憶體、EEPROM、DRAM、SRAM、磁碟或光碟等)來實施。在一些實施例中，配件物件儲存元件3852可用以儲存可由控制器使用以與配件3900互動之一或多個配件物件之表示。該(該等)儲存的配件物件可在請求後(例如，在執行與控制器之對驗證程序之後)供給控制器，且該(該等)儲存的配件物件可在配件之狀態改變時經更新。舉例而言，回饋模組3936可基於自操作組件3932接收之回饋信號而更新該(該等)儲存之配件物件。

探索模組3954可執行與使配件3900可由控制器探索相關之操作，諸如廣播廣告、自不具有已建立配對之控制器接收執行對設置之請求等。舉例而言，探索模組3954可實施上文參看圖4所描述之配件操

作。

請求處理模組3956可接收並處理來自控制器之請求訊息。舉例而言，回應於接收之請求訊息(例如，寫入至如上所述之鎖定狀態特性)，請求處理模組3956可判定該請求是否被准許(例如，是否存在關於控制器之對驗證狀態，訊息是否係使用有效工作階段金鑰加密，及控制器是否具有執行所請求之動作的權限)。假定該請求有效，則請求處理模組3956可產生至執行器模組3934之指令(例如，以致動鎖機構)。在一些實施例中，判定該請求是否被准許可包括解密該訊息，且請求處理模組3956可結合處理該請求而調用由密碼編譯邏輯模組3914支援之功能。在一些實施例中，請求處理模組3956可與安全性子系統3902互動以在對設置、對驗證、對新增或對移除操作期間接收並處理自控制器接收之請求(例如，上文參看圖13至圖19所描述之請求中之任一者)。

回應產生模組3958可產生並發送對請求訊息之回應且將回應訊息發送至控制器。舉例而言，若請求處理模組3956接收一請求且判定該請求未經准許，則請求處理模組3956可如此告知回應產生模組3958，且回應產生模組3958可產生錯誤回應。另一方面，若請求處理模組3956接收一請求且判定該請求經准許，則請求處理模組3956可向回應產生模組3958告知經准許請求已接收且正由執行器模組3934處理。在一些實施例中，回應模組3958可等待以自回饋模組3936接收回饋資訊，接著產生併有該回饋資訊之回應訊息。舉例而言，若回應產生模組3958接收對讀取感測器或開啟鎖之請求，則回應產生模組3958可等待以自回饋模組3936接收感測器讀數或鎖開啟之確認，接著產生適當回應訊息。在一些實施例中，回應訊息可在發送之前加密，且回應產生模組3958可結合加密該訊息而調用由密碼編譯邏輯模組3914支援之功能。在一些實施例中，回應產生模組3958可與安全性子系統3902互動以在對設置、對驗證、對新增或對移除操作期間產生並發送回應

至控制器(例如，上文參看圖13至圖19所描述之請求中之任一者)。

通知產生模組3960可自回饋模組3936接收資訊(例如，只要儲存於配件物件儲存元件3952中之配件物件經更新)且可基於該資訊而產生至控制器之通知訊息。如上所述，可支援各種通知機制，且通知產生模組3960可支援此等通知機制中之任一者或全部(例如，上文所述之程序700、800、900、1000中之任一者或全部)。舉例而言，就被動式通知而言，通知處理模組3960可僅更新維持在配件物件儲存元件3952中之內部狀態計數器。就廣告式通知而言，通知產生模組3960可更新狀態計數器且指示探索模組3954產生包括經更新之狀態計數器值的廣告。就事件通知而言，通知模組3960可指示回應產生模組3958產生如上所述的待發送至訂用控制器之非請求型回應(例如，如上所述之EVENT訊息)。在一些實施例中，通知模組3960可針對各種通知機制及/或各種特性而維持訂用控制器之清單且可視是否訂用任何控制器而策動一或多個機構。在一些實施例中，訂用資訊可維持在配件物件儲存元件3952中。

通信介面模組3970可提供服務以支援與包括控制器之其他器件的通信。在一些實施例中，通信介面模組3970可實施藍芽LE協定堆疊3972及/或HTTP/IP協定堆疊3974。藍芽LE協定堆疊3972可根據藍芽LE傳輸協定來提供傳出訊息之格式化及接收的訊息之解譯。HTTP/IP協定堆疊3974可根據HTTP及IP傳輸協定來提供傳出訊息之格式化及接收的訊息之解譯。儘管使用藍芽LE及HTTP/IP作為實例，但應理解，傳輸協定之任何組合在通信介面模組3970內可得到支援且控制器3900之給定例子可支援一或多個傳輸協定。如上所述，配件3900在器件互動之用戶端/伺服器模型中可充當伺服器器件，且藍芽LE協定堆疊3972及/或HTTP/IP協定堆疊3974可經組態以支援伺服器行為。

在一些實施例中，通信介面模組3970內之協定堆疊可經修改以產

生某些非標準訊息。舉例而言，如上所述，HTTP/IP協定堆疊3974可經組態以自配件產生非請求型「事件」訊息(例如，上文所述的圖11B之事件訊息1120)。

在一些實施例中，通信介面模組3970可提供可由其他模組使用以發送及/或接收訊息至外部器件的API。該API可經設計以為傳輸不可知的，且對用於特定訊息之傳輸的選擇可在通信介面模組3970內以對配件3900內之其他模組透明的方式進行。在配件3900之通信埠(未圖示)接收之訊息可基於埠組態而發送至藍芽LE堆疊3972或HTTP/IP堆疊3974，且藍芽LE堆疊3972及HTTP/IP堆疊3974中之每一者可將傳出訊息發送至經適當組態之通信埠。

應瞭解，本文中所描述之系統組態及組件係說明性的且變化及修改係可能的。應理解，控制器3600 (或控制器3800)之實施可執行上文描述為由控制器執行之操作中之任一者或全部，且配件3700 (或配件3800)之實施可執行上文描述為由配件執行之操作中之任一者或全部；關於不同圖式的不同參考數字之使用不欲暗示其他。控制器及/或配件可具有本文中未特定描述之其他能力(例如，行動電話、全球定位系統(GPS)、寬頻帶資料通信、網際網路連接性等)。視實施而定，該等器件可相互操作以提供由任一(或兩個)器件支援之任何功能性或提供部分地實施於每一器件中之功能性。在一些實施例中，特定配件可具有某一功能性，該功能性經由特定控制器不可存取或調用，但可經由另一控制器或藉由直接與配件互動來存取。

此外，儘管控制器及配件在本文中係參考特定區塊描述，但應理解，此等區塊係為了描述方便而定義且不欲暗示組件部分之特定實體配置。此外，該等區塊不必對應於實體上相異之組件。區塊可經組態以執行各種操作，例如藉由程式化處理器或提供適當控制電路，且視如何獲得初始組態而定，各種區塊可以或不可重新組態。本發明之實

施例可在包括使用電路及軟體之任何組合實施之電子器件的多種裝置中實現。

可支援眾多操作及互動。舉例而言，在一些實施例中，配件可在器件探索服務上廣播廣告，其指示該配件可用於與控制器配對。控制器可(例如)藉由偵測該廣告來尋找配件，且可(例如)藉由安全地交換長期金鑰及頻帶外資訊項目(諸如設置碼或安全性憑證)來起始對設置程序(例如，上文參看圖13至圖16所描述之程序中之任一者)以建立配對。一旦對設置程序完成，配件即可使本身不可用於執行與任何額外控制器之對設置(例如，藉由回應於任何對設置開始請求而忽略或傳回一錯誤)，且執行對設置之控制器可經授予管理員權限。具有管理員權限之控制器可指示配件藉由執行對新增程序(例如，如上文參看圖18所描述)或使用上文所述之其他委派配對程序(例如，將信任憑證鏈結供給至配件)來與一或多個額外控制器建立配對。具有管理員權限之控制器亦可指示配件藉由執行對移除程序(例如，如上文參看圖19所描述)來移除與一或多個其他控制器(或與具有管理員權限之控制器)之已建立配對。

以此方式，控制器及配件之使用者可維持對與配件之什麼其他控制器配對的控制，此係因為可能需要使用者之控制器參與建立任何額外配對。在一些實施例中，使用者可(例如)藉由指示配件將管理員權限授予給一或多個額外控制器而與其他人共用彼控制。具有管理員權限之控制器之使用者亦可指示配件移除已建立配對，包括不再需要之任何配對。

已與配件建立配對之控制器(亦被稱作「配對控制器」)可鍛煉對該配件之控制，而無需必定維持至該配件之連續連接。舉例而言，當配對控制器重新連接至配件時，該控制器可起始允許該配件及該控制器驗證一已建立配對存在於該兩者之間的對驗證程序(例如，如上文參

看圖17所描述)。該對驗證程序亦可提供可用以保全可在該配件及該控制器保持連接時發送之任何後續訊息的一或多個工作階段金鑰；此條件可被稱作「對驗證工作階段」。

當連接時，該控制器可將命令及控制訊息(或請求訊息)發送至該配件。藉由使用適當請求訊息，該控制器可判定該配件之當前狀態，且在一些情況下可指示該配件改變其當前狀態之態樣。舉例而言，該配件可維持將其狀態描述為特性及服務之集合的配件模型(例如，作為配件物件)。該控制器可藉由讀取或以其他方式詢問該等特性中之一或多者(其可包括所有該等特性或其任何子集)來判定該配件之當前狀態的態樣且可指示該配件藉由寫入或以其他方式修改該等特性中之一或多者來改變該配件之當前狀態的態樣。若該配件需要所有此等請求在對驗證工作階段內作為加密訊息來發送，則該配件之操作可限於授權控制器。

該配件可自定義。舉例而言，在建立配對之後，一配對控制器可向該配件請求一配件定義記錄。該配件定義記錄可定義用於每一配件之配件物件，其可經由控制器與之配對的配件來控制。在一些實施例中，該配件定義記錄之全部或部分可在配件已建立任何配對之前供控制器使用，從而允許來自該配件定義記錄之資訊用於判定是否產生配對中。在其他實施例中，控制器可基於包括於配件之廣告(例如，如上所述之TXT記錄)中之資訊來判定是否建立配對，且該配件定義記錄可僅在配對已建立之後供控制器使用。配對控制器可使用該配件定義記錄產生詢問及或修改特性之請求，藉此實現對配件之控制。控制器可視需要回應於使用者輸入或自動地(例如，基於控制器偵測各種條件)而產生此等請求。在一些實施例中，控制器可能夠動態地產生可操作以控制配件之使用者介面，其中該使用者介面係基於提供於該配件定義記錄中之資訊。

在一些實施例中，配件可通知任何配對控制器該配件之狀態之改變。舉例而言，可支援被動式通知程序(例如，如圖7中所示)、廣告式通知程序(例如，如圖8中所示)、主動式通知程序(例如，如圖9中所示)及/或事件訊息通知程序(例如，如圖10中所示)之任何組合。在一些實施例中，配對控制器可將一請求發送至配件以訂用關於特定特性之特定通知方法(例如，廣告式、主動式及/或事件訊息)。配件可維持用於各種控制器之訂用狀態資訊且可基於當前訂用狀態而產生特定類型之通知。

其他實施例

雖然本發明已關於特定實施例加以描述，但熟習此項技術者將認識到，大量修改係可能的。單一控制器可使用本文中所描述之程序來與任何數目個配件建立配對且在不同時間選擇性地與不同配件通信。類似地，單一配件可由多個控制器(該配件具有與該等控制器之已建立配對)來控制(例如，使用如上所述之對設置及對新增)。配件之任何功能可藉由將功能模型化為具有一或多個特性之服務及允許控制器與該服務及/或其特性互動(例如，讀取、修改、接收更新)來控制。因此，如本文中所描述之協定及通信程序可「統一」，此意味該等協定及通信程序可在具有一或多個控制器及一或多個配件之任何內容脈絡中應用，與配件功能或控制器外觀尺寸或特定介面無關。

此外，上文之一些實例特定參考HTTP，可在支援標準網際網路協定(IP傳輸堆疊(例如，TCP/IP))之區域及廣域網路上使用之協定。然而，亦可使用其他傳輸協定。舉例而言，藍芽LE協定堆疊包括允許一個器件詢問及修改另一器件之屬性的一般屬性(GATT)層。在一些實施例中，配件特性之執行個體可作為基於GATT模型之屬性而暴露於控制器。因此，控制器亦可使用藍芽來詢問(例如，讀取)並修改(例如，寫入)配件特性。在一些實施例中，特定配件可支援IP及/或藍芽LE傳輸

協定中之任一者或兩者，且控制器可視配件之能力及由控制器建立之偏好而與使用IP之一些配件及使用藍芽LE之其他配件互動。

本文中所描述之各種特徵(例如，方法、裝置、電腦可讀媒體及類似者)可使用專用組件及/或可程式化處理器及/或其他可程式化器件之任何組合來實現。本文中所描述之各種程序可以任何組合實施於相同處理器或不同處理器上。在組件經描述為經組配以執行某些操作之情況下，此組態可(例如)藉由設計電子電路以執行該操作、藉由程式設計可程式化電子電路(諸如微處理器)以執行該操作或其任何組合來實現。此外，儘管上文所述之實施例可參考特定硬體及軟體組件，但熟習此項技術者將瞭解，亦可使用硬體及/或軟體組件之不同組合，且描述為實施於硬體中之特定操作亦可實施於軟體中，或反之亦然。

併有本文中所描述之各種特徵之電腦程式可經編碼並儲存於各種電腦可讀儲存媒體上；合適之媒體包括磁碟或磁帶、諸如光碟(CD)或DVD (數位化通用光碟)之光學儲存媒體、快閃記憶體及其他非暫時性媒體。用程式碼編碼之電腦可讀媒體可與相容電子器件一起封裝，或程式碼可分別提供自電子器件(例如，經由網際網路下載或作為分別封裝之電腦可讀儲存媒體)。

因此，儘管本發明已關於特定實施例加以描述，但應瞭解，本發明意欲涵蓋在以下申請專利範圍之範疇內的所有修改及等效物。

【符號說明】

100	家庭環境
102	控制器
104	門鎖
106	車庫門系統
108	燈具/配件
110	安全性攝影機/配件

112	恆溫器/配件
114	無線網路存取點
201	標準特性
202	標準特性/「使用中插座」特性
203	標準特性/亮度特性
204	標準特性/色調特性
205	標準特性/飽和度特性
206	標準特性/音訊回饋特性
207	標準特性/輸出音量特性
208	標準特性/記錄檔特性
209	標準特性/當前溫度特性
210	標準特性/目標溫度特性
211	標準特性/溫度單位特性
212	標準特性/當前熱/冷狀態特性
213	標準特性/目標熱/冷模式特性
214	標準特性/冷卻臨限溫度特性
215	標準特性/加熱臨限溫度特性
216	標準特性/當前門狀態特性
217	標準特性/目標門狀態特性
218	標準特性/運動偵測特性
219	標準特性/障礙偵測特性
220	標準特性/鎖機構當前狀態特性
221	標準特性/鎖機構目標狀態特性
222	標準特性/鎖機構最後動作特性
223	標準特性/鎖管理自動逾時特性
224	標準特性/鎖管理控制點特性

225 標準特性/旋轉方向特性

226 標準特性/旋轉速度特性

227 標準特性/名稱特性

228 標準特性/僅管理員存取特性

229 標準特性/版本特性

230 「類型」

231 「權限」

232 「通知模式」

233 「格式」

234 「值」

235 「最小值」

236 「最大值」

237 「步長」

238 「有效值」

239 「單位」

240 「使用者描述符」

241 「擁有者」

242 閃光特性

243 方向特性

244 速度特性

251 核心服務/燈泡服務

252 核心服務

253 核心服務/車庫開門器服務

254 核心服務/鎖機構服務

255 核心服務

256 核心服務

257 核心服務

258 核心服務

261 配件資訊服務

271 身分識別特性

272 製造商名稱特性

273 模型名稱特性

274 序號特性

275 韌體修訂特性

276 硬體修訂特性

277 軟體修訂特性

300 配件物件

310 服務執行個體

311 特性執行個體

312 特性執行個體

313 特性執行個體

314 特性執行個體

315 特性執行個體

320 服務執行個體

321 特性執行個體

322 特性執行個體

323 特性執行個體

324 特性執行個體

325 特性執行個體

330 服務執行個體

331 特性執行個體

332 特性執行個體

400	用於藉由控制器來探索配件的程序
402	配件
404	控制器
410	區塊
412	區塊
414	區塊
416	區塊
418	區塊
422	區塊
424	區塊
426	區塊
428	區塊
430	區塊
431	區塊
432	區塊
434	區塊
436	區塊
438	區塊
500	URL
502	協定識別首碼
504	用於配件之主機名稱
506	本機路徑
508	協定關鍵字
510	服務執行個體識別符
512	特性執行個體識別符
520	GET請求

526 本機路徑

530 HTTP回應

532 HTTP回應標頭

534 內容

540 PUT請求

542 內容

546 本機路徑

550 PUT請求

556 本機路徑

560 回應

562 內容

563 已更新特性

564 已更新特性

565 「回應」物件

566 「回應」物件

571 特性執行個體

572 PUT請求

573 請求572之內嵌HTTP回應

574 內容

575 異動回應

576 異動ID

577 異動持續時間

578 HTTP GET請求

600 簡化URL

602 協定識別首碼

604 主機名稱

606 本機URL

610 HTTP GET請求

612 字串

620 HTTP回應

622 HTTP回應標頭

624 內容

630 PUT請求

634 內容

640 錯誤訊息

644 內容

646 狀態碼

648 狀態碼

700 「被動式」通知程序

702 控制器

704 配件

706 區塊

708 區塊

712 區塊

714 區塊

716 區塊

718 區塊

720 區塊

722 區塊

724 區塊

726 區塊

728 區塊

730 區塊

732 區塊

800 「廣告式」通知程序

802 控制器

804 配件

806 區塊

808 區塊

810 區塊

812 區塊

814 區塊

816 區塊

818 區塊

820 區塊

822 區塊

824 區塊

826 區塊

828 區塊

830 區塊

900 「主動式」通知程序

902 控制器

904 配件

906 區塊

908 區塊

910 區塊

912 區塊

914 區塊

916	區塊
918	區塊
920	區塊
922	區塊
924	區塊
926	區塊
928	區塊
930	區塊
932	區塊
934	區塊
1000	「事件通知」程序
1002	控制器
1004	配件
1006	區塊
1008	區塊
1010	區塊
1014	區塊
1016	區塊
1018	區塊
1022	區塊
1024	區塊
1026	區塊
1028	區塊
1030	區塊
1032	區塊
1100	用以訂用針對特性之事件通知的HTTP PUT請求

1102 內容

1120 事件訊息

1122 標頭區段

1124 主體

1201 配對設定檔之實例特性/配對狀態請求特性/配對控制點特性

1202 配對設定檔之實例特性/特徵旗標特性

1203 配對設定檔之實例特性/配對當前狀態特性

1204 配對設定檔之實例特性/配對清單特性

1205 配對設定檔之實例特性/配對ID特性

1300 基於設置碼之對設置程序

1302 控制器

1304 配件

1306 區塊

1308 區塊

1310 區塊

1312 區塊

1314 區塊

1316 區塊

1318 區塊

1320 區塊

1322 區塊

1324 區塊

1326 區塊

1328 區塊

1330 區塊

1332 區塊

1334 區塊

1336 區塊

1338 區塊

1340 區塊

1342 區塊

1344 區塊

1346 區塊

1348 區塊

1350 區塊

1352 區塊

1354 區塊

1356 區塊

1358 區塊

1360 區塊

1362 區塊

1364 區塊

1366 區塊

1368 區塊

1370 區塊

1372 區塊

1374 區塊

1376 區塊

1378 區塊

1380 區塊

1382 區塊

1384 區塊

1386 區塊

1388 區塊

1400 使用鑑認晶片的用於控制器1402及配件1404之對設置程序

1402 控制器

1404 配件

1406 區塊

1408 區塊

1410 區塊

1412 區塊

1414 區塊

1416 區塊

1418 區塊

1420 區塊

1422 區塊

1424 區塊

1426 區塊

1428 區塊

1430 區塊

1432 區塊

1434 區塊

1436 區塊

1438 區塊

1440 區塊

1442 區塊

1444 區塊

1446 區塊

1448 區塊

1450 區塊

1452 區塊

1454 區塊

1456 區塊

1458 區塊

1460 區塊

1462 區塊

1464 區塊

1466 區塊

1468 區塊

1470 區塊

1472 區塊

1474 區塊

1476 區塊

1500 使用安全性憑證及設置碼的用於控制器1502及配件1504的對設置程序

1501 區塊

1502 控制器

1503 區塊

1504 配件

1505 區塊

1506 區塊

1507 區塊

1508 區塊

1509 區塊

1510 區塊

1511 區塊

1512 區塊

1513 區塊

1514 區塊

1516 區塊

1518 區塊

1520 區塊

1522 區塊

1524 區塊

1526 區塊

1528 區塊

1530 區塊

1532 區塊

1534 區塊

1536 區塊

1538 區塊

1540 區塊

1542 區塊

1544 區塊

1546 區塊

1548 區塊

1550 區塊

1552 區塊

1554 區塊

1556 區塊

1558 區塊

1560 區塊

1562 區塊

1564 區塊

1566 區塊

1568 區塊

1570 區塊

1572 區塊

1574 區塊

1576 區塊

1578 區塊

1580 區塊

1582 區塊

1584 區塊

1586 區塊

1588 區塊

1590 區塊

1592 區塊

1594 區塊

1596 區塊

1598 區塊

1600 一般化對設置程序

1602 控制器

1604 配件

1606 區塊

1608 區塊

1610 區塊

1612 區塊

1614 區塊

1616 區塊

1618 區塊

1620 區塊

1622 區塊

1624 區塊

1626 區塊

1628 區塊

1630 區塊

1632 區塊

1634 區塊

1700 對驗證程序

1702 控制器

1704 配件

1706 區塊

1708 區塊

1710 區塊

1712 區塊

1714 區塊

1716 區塊

1718 區塊

1720 區塊

1724 區塊

1726 區塊

1728 區塊

1730 區塊

1732 區塊

1734 區塊

1736 區塊

1738 區塊

1740 區塊

1742 區塊

1744 區塊

1746 區塊

1748 區塊

1750 區塊

1752 區塊

1754 區塊

1756 區塊

1758 區塊

1760 區塊

1762 區塊

1764 區塊

1766 區塊

1768 區塊

1770 區塊

1800 對新增程序

1802 控制器

1804 配件

1806 區塊

1808 區塊

1810 區塊

1812 區塊

1814 區塊

1816 區塊

1818 區塊

1820 區塊

1832 區塊

1834 區塊

1836 區塊

1838 區塊

1840 區塊

1844 區塊

1846 區塊

1848 區塊

1900 對移除程序

1902 控制器

1904 配件

1906 區塊

1908 區塊

1910 區塊

1912 區塊

1914 區塊

1916 區塊

1918	區塊
1920	區塊
1932	區塊
1934	區塊
1936	區塊
1938	區塊
1940	區塊
1944	區塊
1946	區塊
1948	區塊
2000	門鎖配件之操作環境
2004	門鎖配件
2006	內門或外門
2012	使用者操作之控制器
2018	主控制器
2100	用於門鎖配件2004之配件物件
2102	配件識別服務執行個體
2104	鎖機構服務執行個體
2106	鎖管理服務執行個體
2200	程序
2202	區塊
2204	區塊
2206	區塊
2208	區塊
2210	區塊
2212	區塊

2214 區塊

2300 用於解除鎖定門之程序

2302 區塊

2306 區塊

2308 區塊

2310 區塊

2312 區塊

2314 區塊

2316 區塊

2318 區塊

2320 區塊

2322 區塊

2324 區塊

2400 用於IP攝影機配件之操作環境

2402 控制器

2404 IP攝影機配件

2406 無線存取點

2501 服務定義/IP攝影機串流服務

2502 服務定義/記錄服務

2503 服務定義/播放服務

2504 服務定義/攝影機服務

2505 服務定義/麥克風服務

2506 揚聲器服務

2601 工作階段開始特性

2602 工作階段結束特性

2603 額外特性/視訊轉碼器名稱

2604 額外特性/視訊轉碼器參數

2605 額外特性/視訊屬性特性

2606 額外特性/RTP視訊有效負載類型特性

2607 額外特性/RTP協定特性

2608 額外特性/RTP延伸特性

2609 額外特性/SRTP密碼編譯套件特性

2610 額外特性/音訊轉碼器名稱特性

2611 額外特性/音訊轉碼器參數

2612 額外特性

2613 額外特性/音訊屬性參數

2614 額外特性/RTP音訊時脈速率特性

2615 額外特性/RTP音訊有效負載類型特性

2631 工作階段ID

2632 控制器IP位址

2633 控制器埠

2634 控制器SRTP主控金鑰

2635 控制器SRTP主控salt

2636 視訊最大頻寬

2637 音訊最大頻寬

2651 夜視特性

2652 平移特性

2653 傾斜特性

2654 旋轉特性

2655 變焦特性

2656 鏡像特性

2661 記錄控制特性

2662 記錄狀態特性

2663 播放控制特性

2664 播放狀態特性

2665 播放速度特性

2700 用於IP攝影機配件之配件物件

2702 配件資訊服務執行個體

2704 IP攝影機串流服務執行個體

2706 攝影機服務

2708 麥克風服務

2800 展示互動情境之程序

2802 區塊

2804 區塊

2806 區塊

2808 區塊

2810 區塊

2812 區塊

2814 區塊

2816 區塊

2818 區塊

2820 區塊

2822 區塊

2824 區塊

2900 請求訊息

2902 訊息主體

2904 執行個體識別符

2906 值

3000	回應訊息
3002	訊息主體
3004	值
3100	結束媒體工作階段請求訊息
3102	訊息主體
3104	執行個體識別符
3200	結束媒體工作階段回應
3202	訊息主體
3301	IP串流服務
3401	串流能力特性
3402	串流控制輸入特性
3403	串流控制結果
3500	可由控制器執行的用於IP串流之程序
3502	區塊
3504	區塊
3506	區塊
3508	區塊
3510	區塊
3512	區塊
3514	區塊
3516	區塊
3518	區塊
3520	區塊
3600	控制器
3610	處理子系統
3612	儲存器件

3614 使用者介面

3616 通信介面

3618 安全元件/安全儲存模組/安全儲存元件

3620 密碼編譯邏輯模組

3622 控制器之長期公用金鑰及秘密金鑰

3624 已配對配件之清單

3700 配件

3728 儲存器件

3730 處理子系統

3732 使用者介面

3734 配件特定硬體

3736 通信介面

3738 安全元件/安全儲存模組/安全儲存元件

3740 密碼編譯邏輯模組

3742 配件之長期公用金鑰及秘密金鑰

3744 已配對控制器之清單

3800 控制器

3802 安全性子系統

3804 安全儲存元件

3806 對設置模組

3808 對驗證模組

3810 對新增模組

3812 對移除模組

3814 密碼編譯邏輯模組

3830 使用者互動子系統

3832 使用者介面產生模組

3834	使用者輸入接收器模組
3850	配件互動子系統
3852	配件物件儲存元件
3854	配件探索模組
3856	請求產生模組
3858	回應處理模組
3860	通知處理模組
3870	通信介面
3872	藍芽LE協定堆疊
3874	HTTP/IP協定堆疊
3900	配件
3902	安全性子系統
3904	安全儲存元件
3906	對設置模組
3908	對驗證模組
3910	對新增模組
3912	對移除模組
3914	密碼編譯邏輯模組
3930	配件動作子系統
3932	操作組件
3934	執行器模組
3936	回饋模組
3950	控制器互動子系統
3952	配件物件儲存元件
3954	探索模組
3956	請求處理模組

3958	回應產生模組
3960	通知產生模組
3970	通信介面模組
3972	藍芽LE協定堆疊
3974	HTTP/IP協定堆疊

I620430

公告本

發明摘要

※ 申請案號：104104009

※ 申請日：104/02/05 ※IPC 分類：*H04L 29/06* (2006.01)
H04L 9/30 (2006.01)
G06F 9/54 (2006.01)
G06F 21/64 (2013.01)

【發明名稱】

用於控制器與配件之間通信的統一通信協定

UNIFORM COMMUNICATION PROTOCOLS FOR COMMUNICATION BETWEEN CONTROLLERS AND ACCESSORIES

【中文】

一統一協定可有助於一控制器器件與由該控制器控制之一配件器件之間的安全的經鑑認通信。一配件及一控制器可建立一配對，該配對之存在稍後可經驗證且用以建立一安全通信工作階段。該配件可提供將該配件定義為服務之一集合的一配件定義記錄，每一服務具有一或多個特性。在一安全通信工作階段內，該控制器可詢問該等特性以判定配件狀態及/或修改該等特性以指示該配件改變其狀態。

【英文】

A uniform protocol can facilitate secure, authenticated communication between a controller device and an accessory device that is controlled by the controller. An accessory and a controller can establish a pairing, the existence of which can be verified at a later time and used to create a secure communication session. The accessory can provide an accessory definition record that defines the accessory as a collection of services, each service having one or more characteristics. Within a secure communication session, the controller can interrogate the characteristics to determine accessory state and/or modify the characteristics to instruct the accessory to change its state.

圖式

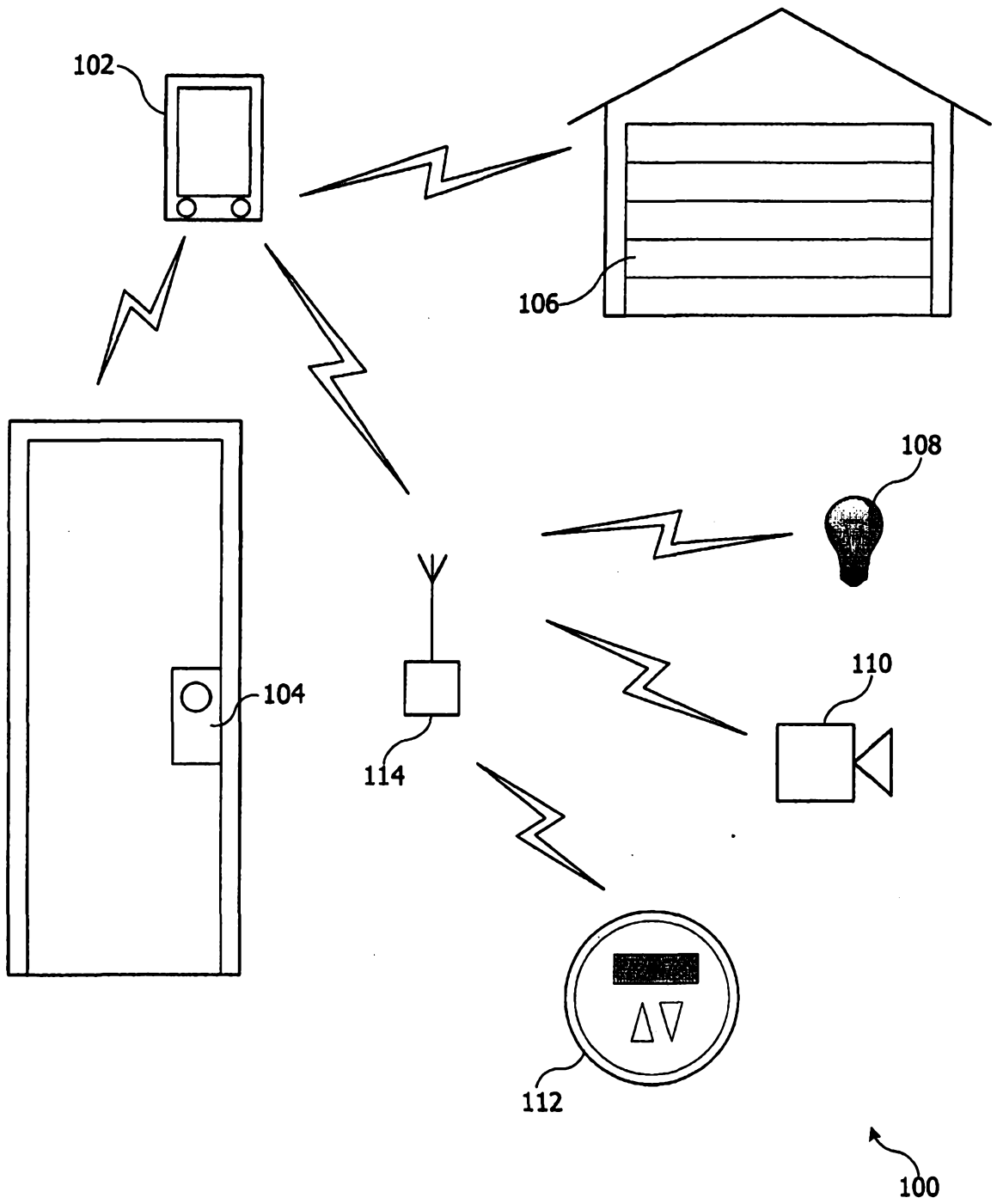


圖1

特性	性質	值
接通 201	類型	com.proto.ch.on
	權限	配對讀取，配對寫入
	格式	<boolean>
使用中插座 202	類型	com.proto.ch.outlet-in-use
	權限	配對讀取
	格式	<boolean>
亮度 203	類型	com.proto.ch.brightness
	權限	配對讀取，配對寫入
	格式	<integer>
	最小值，最大值，步進	0, 100, 1
	單位	百分比
色調 204	類型	com.proto.ch.hue
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	0, 360, 1
	單位	弧度
飽和度 205	類型	com.proto.ch.saturation
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	0, 100, 1
	單位	百分比
音訊回饋 206	類型	com.proto.ch.audio-feedback
	權限	配對讀取，配對寫入
	格式	<boolean>
輸出音量 207	類型	com.proto.ch.volume.output
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	0, 100, 1
	單位	百分比
記錄檔 208	類型	com.proto.ch.logs
	權限	配對讀取
	格式	<tlv>

圖2A

特性	性質	值
當前溫度 209	類型	com.proto.ch.temp.current
	權限	配對讀取
	格式	<float>
	最小值，最大值，步進	0, 100, 0.1
	單位	攝氏度
目標溫度 210	類型	com.proto.ch.temp.target
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	10, 38, 0.1
	單位	攝氏度
溫度單位 211	類型	com.proto.ch.temp.units
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	「攝氏度」、「華氏溫度」
當前熱/冷狀態 212	類型	com.proto.ch.heat-cool.current
	權限	配對讀取
	格式	<enum>
	有效值	「熱」、「冷」、「關斷」
目標熱/冷模式 213	類型	com.proto.ch.heat-cool.target
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	「熱」、「冷」、「自動」、「關斷」
冷卻臨限溫度 214	類型	com.proto.ch.temp.cool-threshold
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	10, 35, 0.1
	單位	攝氏度
加熱臨限溫度 215	類型	com.proto.ch.temp.heat-threshold
	權限	配對讀取，配對寫入
	格式	<float>
	最小值，最大值，步進	0, 25, 0.1
	單位	攝氏度

圖2B

特性	性質	值
當前門狀態 216	類型	com.proto.ch.door-state.current
	權限	配對讀取
	格式	<enum>
	有效值	開啟，開啟中，關閉，關閉中，停止
目標門狀態 217	類型	com.proto.ch.door-state.target
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	開啟，關閉
運動偵測 218	類型	com.proto.ch.motion-detected
	權限	配對讀取
	格式	<boolean>
障礙偵測 219	類型	com.proto.ch.obstruction-detected
	權限	配對讀取
	格式	<boolean>
鎖機構當前狀態 220	類型	com.proto.ch.lock-mech.current-state
	權限	配對讀取
	格式	<enum>
	有效值	未扣緊，已扣緊，已卡住，未知
鎖機構目標狀態 221	類型	com.proto.ch.lock-mech.target-state
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	未扣緊，已扣緊
鎖機構最後動作 222	類型	com.proto.ch.lock-mech.last-action
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	已扣緊/未扣緊，實體/遠端，內部/外部等
鎖管理自動逾時 223	類型	com.proto.ch.lock-mgt.auto-timeout
	權限	配對讀取，配對寫入
	格式	<int>
	最小值，最大值，步進	0，intmax，1
鎖管理控制點 224	類型	com.proto.ch.lock-mgt.control-point
	權限	配對寫入
	格式	<tlv>

圖2C

特性	性質	值
旋轉方向 225	類型	com.proto.ch.rotation-direction
	權限	配對讀取，配對寫入
	格式	<enum>
	有效值	順時針，逆時針
旋轉速度 226	類型	com.proto.ch.brightness
	權限	配對讀取，配對寫入
	格式	<integer>
	最小值，最大值，步進	0, 100, 1
	單位	百分比
名稱 227	類型	com.proto.ch.name
	權限	配對讀取
	格式	<string>
僅管理員存取 228	類型	com.proto.ch.admin-only-access
	權限	配對讀取，管理員寫入
	格式	<boolean>
版本 229	類型	com.proto.ch.version
	權限	配對讀取
	格式	<string>

圖2D

	性質	格式
230	類型	<string>
231	權限	<string>之陣列
232	通知模式	<string>之陣列
233	格式	<string>
234	值	[如格式性質所規定]
235	最小值(Min)	<number>
236	最大值(Max)	<number>
237	步長(Step)	<number>
238	有效值	<string>之陣列
239	單位	<string>
240	使用者描述符	<string>
241	擁有者	<string>

圖2E

性質	閃光 (242)	方向 (243)	速度 (244)
類型	com.discoball.ch.strobe	com.discoball.ch.rotate.direction	com.discoball.ch.rotate.speed
權限	PR, PW	PR, PW	PR, PW
通知模式	事件	事件	事件
格式	布林值	列舉	<int>
值	假	不旋轉	1
最小值	--	--	0
最大值	--	--	1
步長	--	--	1
有效值	--	不旋轉，順時針，逆時針	--
單位	--	--	--
使用者描述符	閃光開啟或關斷	球之旋轉方向	球之旋轉速度
擁有者	Discoball Inc.	Discoball Inc.	Discoball Inc.

圖2F

服務	性質	值
燈泡 251	類型	com.proto.svc.lightbulb
	必需特性	com.proto.ch.on
	選用之特性	com.proto.ch.brightness
		com.proto.ch.hue
		com.proto.ch.saturation
		com.proto.ch.name
恆溫器 252	類型	com.proto.svc.thermostat
	必需特性	com.proto.ch.heat-cool.current
		com.proto.ch.heat-cool.target
		com.proto.ch.temp.current
		com.proto.ch.temp.target
		com.proto.ch.temp.units
	選用之特性	com.proto.ch.temp.cool-threshold
		com.proto.ch.temp.heat-threshold
		com.proto.ch.name
車庫開門器 253	類型	com.proto.svc.garage-door-opener
	必需特性	com.proto.ch.door-state.current
		com.proto.ch.door-state.target
		com.proto.ch.obstruction-detected
	選用之特性	com.proto.ch.lock-mech.current-state
		com.proto.ch.lock-mech.target-state
		com.proto.ch.name
鎖機構 254	類型	com.proto.svc.lock-mech
	必需特性	com.proto.ch.lock-mech.current-state
		com.proto.ch.lock-mech.target-state
	選用之特性	com.proto.ch.name

圖2G

服務	性質	值
鎖管理 255	類型	com.proto.svc.lock-mgt
	必需特性	com.proto.ch.lock-mgt.control-point
		com.proto.ch.version
	選用之特性	com.proto.ch.logs
		com.proto.ch.audio-feedback
		com.proto.ch.admin-only-access
		com.proto.ch.lock-mgt.auto-timeout
		com.proto.ch.lock-mech.last-action
		com.proto.ch.door-state.current
		com.proto.ch.motion-detected
		com.proto.ch.name
插座 256	類型	com.proto.svc.outlet
	必需特性	com.proto.ch.on
		com.proto.ch.outlet-in-use
	選用之特性	com.proto.ch.name
開關 257	類型	com.proto.svc.switch
	必需特性	com.proto.ch.on
	選用之特性	com.proto.ch.name
風扇 258	類型	com.proto.svc.fan
	必需特性	com.proto.ch.on
	選用之特性	com.proto.ch.rotation.direction
		com.proto.ch.rotation.speed
		com.proto.ch.name

圖2H

服務	性質	值
配件資訊 261	類型	com.proto.svc.accessory-info
	必需特性	com.proto.ch.identify
		com.proto.ch.manufacturer
		com.proto.ch.model
		com.proto.ch.name
		com.proto.ch.serial-number
	選用之特性	com.proto.ch.firmware-revision
		com.proto.ch.hardware-revision
		com.proto.ch.software-revision

圖2I

特性	性質	值
身分識別 271	類型	com.proto.ch.identify
	權限	配對寫入
	格式	<boolean>
製造商名稱 272	類型	com.proto.ch.manufacturer
	權限	配對讀取
	格式	<string>
模型名稱 273	類型	com.proto.ch.model
	權限	配對讀取
	格式	<string>
序號 274	類型	com.proto.ch.serial-number
	權限	配對讀取
	格式	<string>
韌體修訂 275	類型	com.proto.ch.firmware-rev
	權限	配對讀取
	格式	<string>
硬體修訂 276	類型	com.proto.ch.hardware-rev
	權限	配對讀取
	格式	<string>
軟體修訂 277	類型	com.proto.ch.software-rev
	權限	配對讀取
	格式	<string>

圖2J

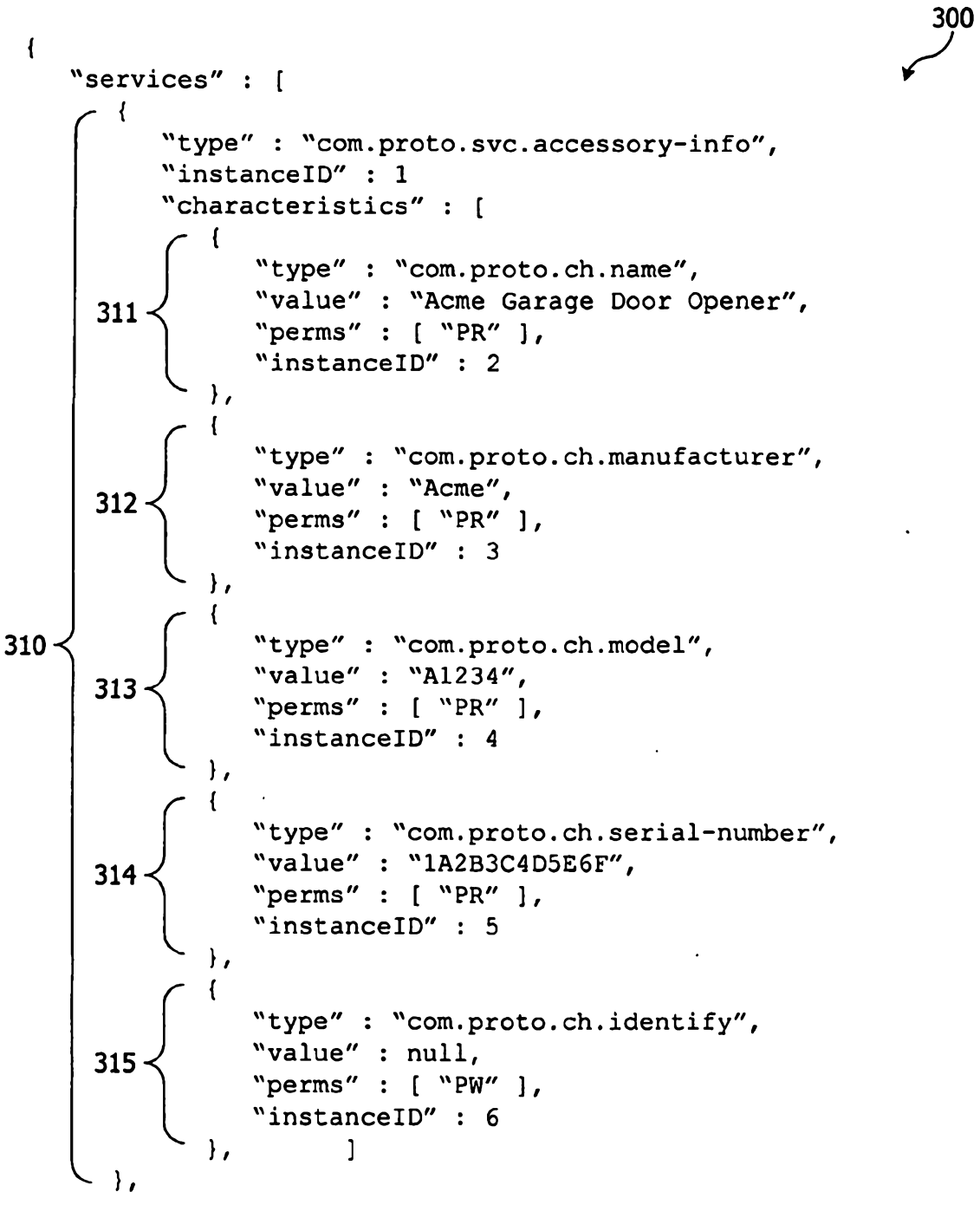

300
{
"services" : [
{
"type" : "com.proto.svc.accessory-info",
"instanceID" : 1
"characteristics" : [
{
"type" : "com.proto.ch.name",
"value" : "Acme Garage Door Opener",
"perms" : ["PR"],
"instanceID" : 2
},
{
"type" : "com.proto.ch.manufacturer",
"value" : "Acme",
"perms" : ["PR"],
"instanceID" : 3
},
{
"type" : "com.proto.ch.model",
"value" : "A1234",
"perms" : ["PR"],
"instanceID" : 4
},
{
"type" : "com.proto.ch.serial-number",
"value" : "1A2B3C4D5E6F",
"perms" : ["PR"],
"instanceID" : 5
},
{
"type" : "com.proto.ch.identify",
"value" : null,
"perms" : ["PW"],
"instanceID" : 6
},
]
},
311
312
313
314
315
310
// 繼續下一頁

圖3A

// 自前一頁繼續

300

```
{
    "type" : "com.proto.svc.garage-door-opener",
    "instanceID" : 7,
    "characteristics" : [
        {
            "type" : "com.proto.ch.door-state.current",
            "value" : 2,
            "perms" : [ "PR", "Events" ],
            "instanceID" : 8
        },
        {
            "type" : "com.proto.ch.door-state.target",
            "value" : 0,
            "perms" : [ "PR", "PW", "Events" ],
            "instanceID" : 9
        },
        {
            "type" : "com.proto.ch.obstruction-detected",
            "value" : true,
            "perms" : [ "PR", "Events" ],
            "instanceID" : 10
        },
        {
            "type" : "com.proto.ch.lock-mech.current",
            "value" : true,
            "perms" : [ "PR", "Events" ],
            "instanceID" : 11
        },
        {
            "type" : "com.proto.ch.lock-mech.target",
            "value" : true,
            "perms" : [ "PR", "PW", "Events" ],
            "instanceID" : 12
        }
    ]
},
```

320 包含 321、322、323、324、325

// 繼續下一頁

圖3B

// 自前一頁繼續

300

```
{
    "type" = com.proto.svc.lightbulb",
    "instanceID" = 13
    "characteristics" : [
        {
            "type" : "com.proto.ch.on",
            "value" : false,
            "perms" : [ "PR", "PW", "Events" ],
            "instanceID" : 14
        },
        {
            "type" : "com.proto.ch.brightness",
            "value" : 100,
            "perms" : [ "PR", "PW", "Events" ],
            "instanceID" : 15
            "maxValue" : 100,
            "minValue" : 20,
            "stepSize": 5,
            "format" : "int",
            "unit" : "percentage"
        }
    ]
}
]
}
```

331 332 330

圖3C

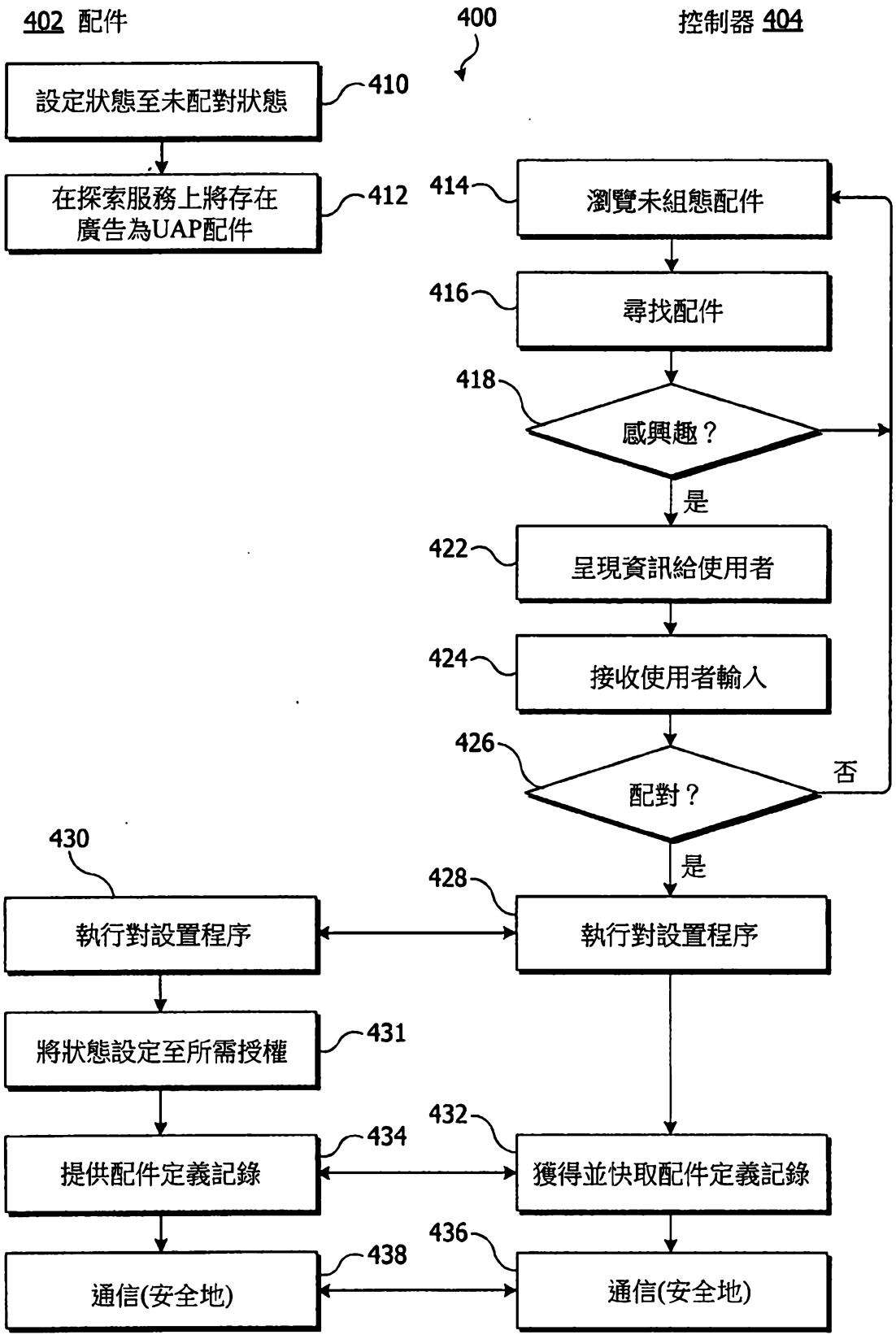

402 配件
400
控制器 404
設定狀態至未配對狀態
410
在探索服務上將存在廣告為UAP配件
412
414
瀏覽未組態配件
416
尋找配件
418
感興趣？
是
否
422
呈現資訊給使用者
424
接收使用者輸入
426
配對？
是
否
430
428
執行對設置程序
執行對設置程序
將狀態設定至所需授權
431
提供配件定義記錄
434
432
獲得並快取配件定義記錄
通信(安全地)
438
436
通信(安全地)

圖4

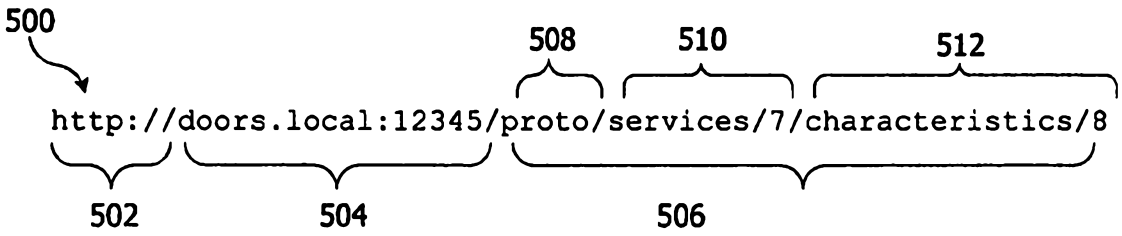


圖5A

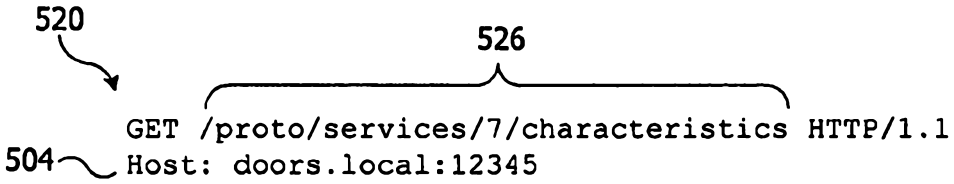


圖5B

530

```
532 HTTP/1.1 200 OK
    Content-Type: application/uap+json
    Content-Length: <length>
    {
       "characteristics" = [
          {
             "type" : "com.proto.ch.door-state.current",
             "value" : 2,
             "instanceID" = 8
          },
534       {
             "type" : "com.proto.door-state.target",
             "value" : 0,
             "instanceID" : 9
          },
    //    ...
       ]
    }
```

圖5C

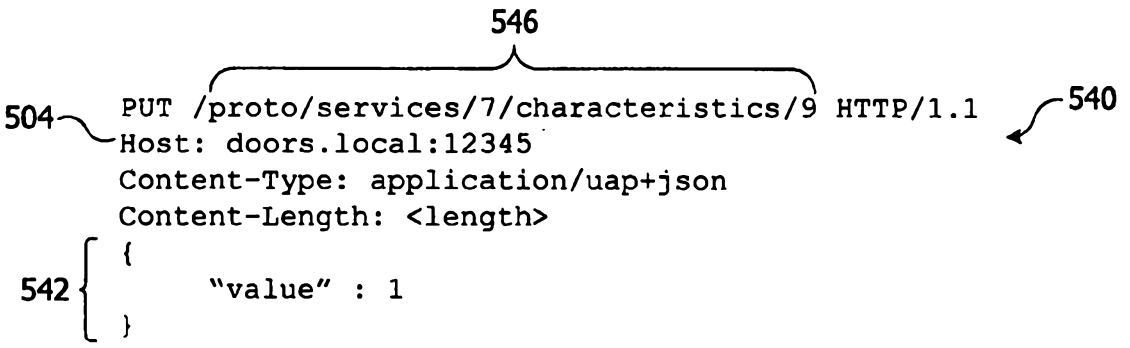

546
504
PUT /proto/services/7/characteristics/9 HTTP/1.1
540
Host: doors.local:12345
Content-Type: application/uap+json
Content-Length: <length>
542
{
"value" : 1
}

圖5D

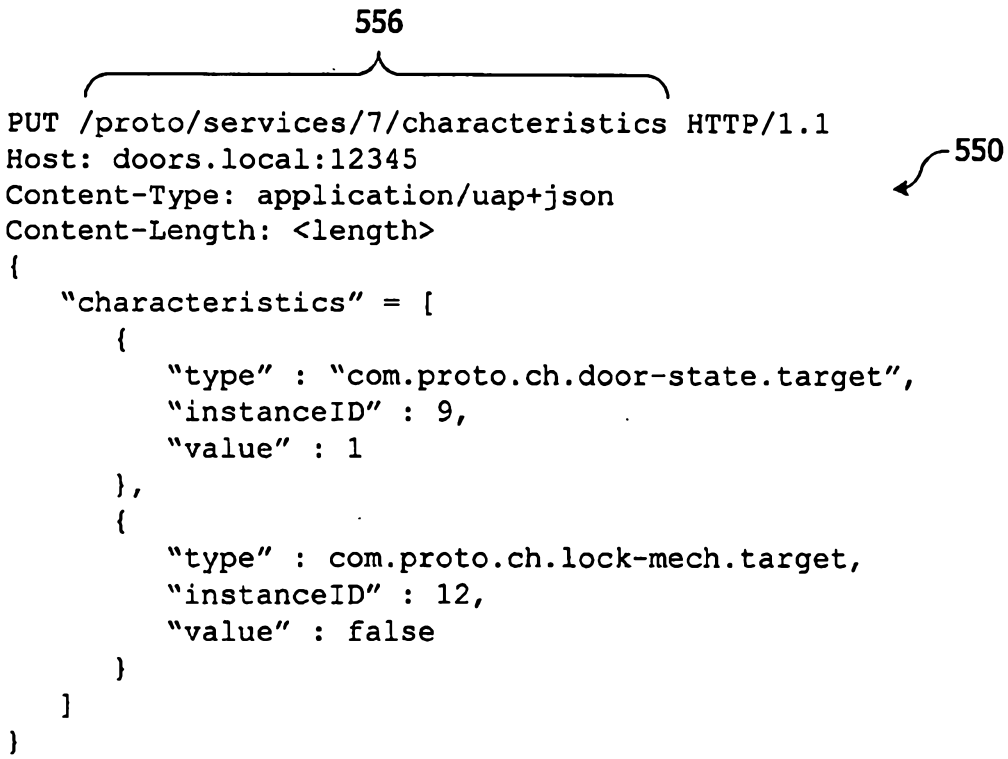

556
PUT /proto/services/7/characteristics HTTP/1.1
Host: doors.local:12345
550
Content-Type: application/uap+json
Content-Length: <length>
{
"characteristics" = [
{
"type" : "com.proto.ch.door-state.target",
"instanceID" : 9,
"value" : 1
},
{
"type" : com.proto.ch.lock-mech.target,
"instanceID" : 12,
"value" : false
}
]
}

圖5E


HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>
560
{
"characteristics" = [
{
"type" : com.proto.ch.door-state.target,
"value" : 0
"instanceID" : 0,
"response: : {
"developerMessage" : "No error occurred.",
"errorCode" : 0,
"moreInfo" : null
}
563
565
},
562
{
"type" : com.proto.ch.lock-mech.target,
"value" : true
"instanceID" : 1,
"response: : {
"developerMessage" : "No error occurred.",
"errorCode" : 0,
"moreInfo" : null
}
564
566
}
]
}

圖5F

```
{
   "type" : com.acme.ch.port.open,
   "perms" : [ "PW" ]
   "value" : null,
   "instanceID" : 33
}
```

571

圖5G

572

```
PUT /proto/services/22/characteristics/33 HTTP/1.1
Host: ipcamera.local:12345
Content-Type: application/uap+json
Content-Length: <length>
{
   "value" : true
}
```

圖5H

573

```
HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>
{
   "value" :
      {
         "port" : 45678,
         "status-code" : 0
      }
}
```

574

圖5I

```
HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>                                    575
{
   "value" :
      {
         "transactionID" : nnnnnnnnnnnn,                    576
         "transactionDuration" : 5                          577
      }
}
```

圖5J

```
                                                            578
GET /proto/services/22/characteristics/33 HTTP/1.1
Host: ipcamera.local:12345
Content-Type: application/json
Content-Length: <length>
{
   "value" :
      {
         "transactionID" : nnnnnnnnnnnn
      }
}
```

圖5K


600
http://doors.local:12345/characteristics
602
604
606

圖6A

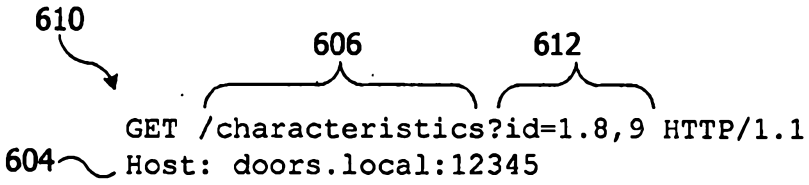

610
606
612
GET /characteristics?id=1.8,9 HTTP/1.1
604
Host: doors.local:12345

圖6B

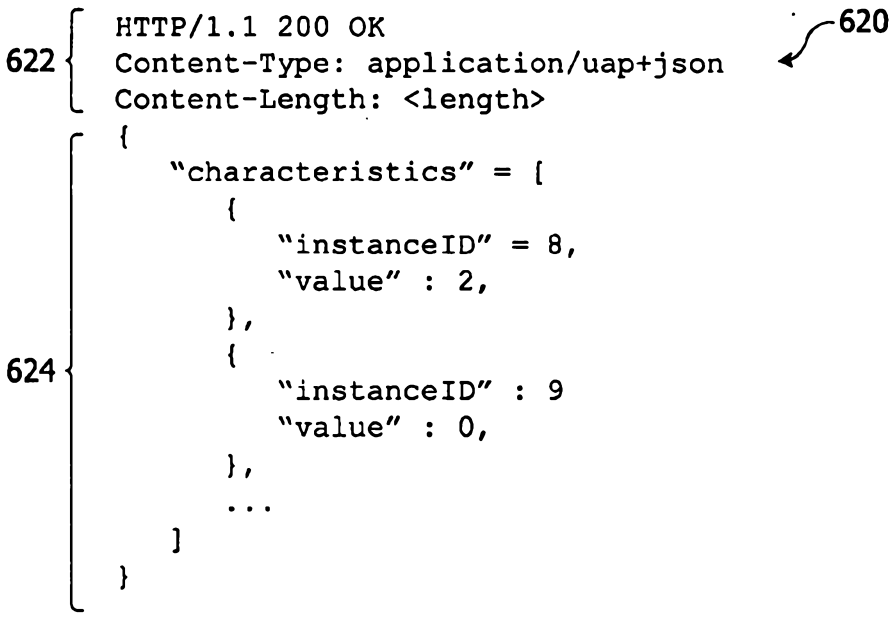

620
622
HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>
624
{
"characteristics" = [
{
"instanceID" = 8,
"value" : 2,
},
{
"instanceID" : 9
"value" : 0,
},
...
]
}

圖6C

```
PUT /characteristics HTTP/1.1
Host: doors.local:12345
Content-Type: application/uap+json
Content-Length: <length>
{
    "characteristics" : [
        {
            "accessory ID" : 1,
            "instance ID" : 8,
            "value" : 1
        },
        {
            "accessory ID" : 1,
            "instance ID" : 10,
            "value" : false
        }
    ]
}
```

630

634

圖6D

```
HTTP/1.1 207 Multi-Status
Content-Type: application/uap+json
Content-Length: <length>
{
    "characteristics" : [
        {
            "accessory ID" : 1,
            "instance ID" : 8,
            "status" : 0
        },
        {
            "accessory ID" : 1,
            "instance ID" : 10,
            "status" : -12345
        }
    ]
}
```

640

644

646

648

圖6E

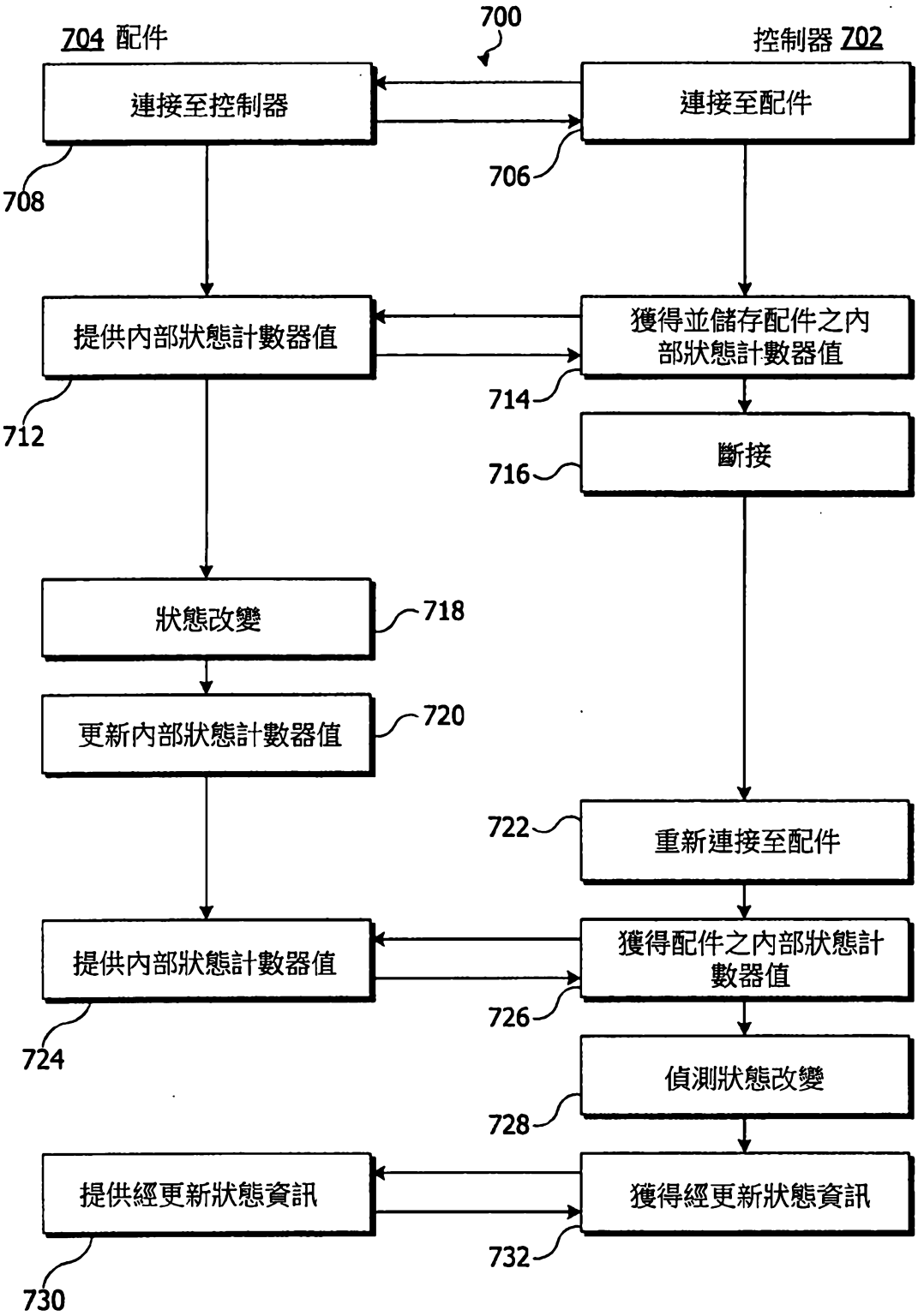

700
704 配件
控制器 702
連接至控制器
連接至配件
708
706
提供內部狀態計數器值
獲得並儲存配件之內部狀態計數器值
712
714
斷接
716
狀態改變
718
更新內部狀態計數器值
720
722
重新連接至配件
提供內部狀態計數器值
獲得配件之內部狀態計數器值
724
726
偵測狀態改變
728
提供經更新狀態資訊
獲得經更新狀態資訊
730
732

圖7

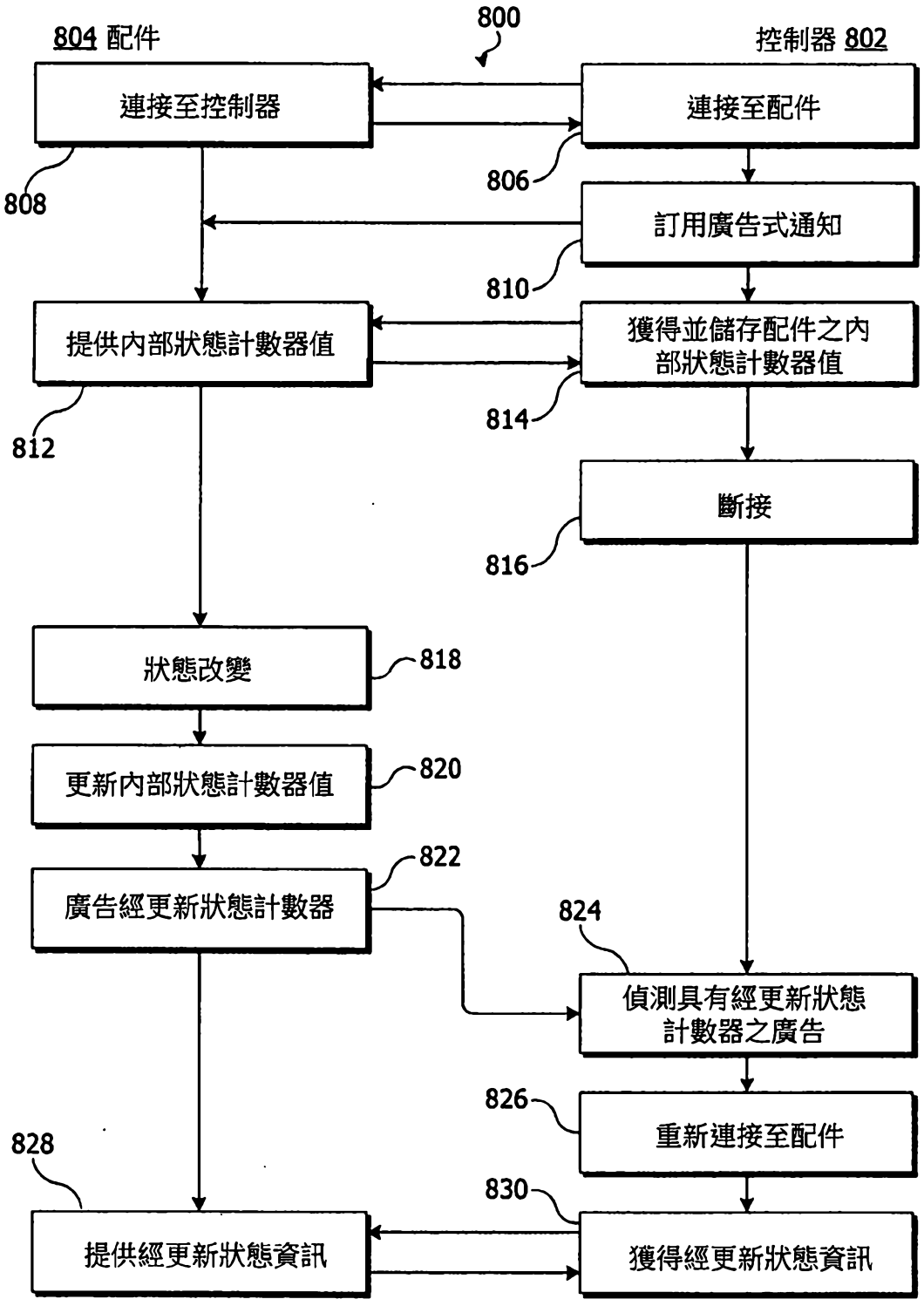

800
804 配件
控制器 802
連接至控制器
連接至配件
808
806
訂用廣告式通知
810
提供內部狀態計數器值
獲得並儲存配件之內部狀態計數器值
812
814
斷接
816
狀態改變
818
更新內部狀態計數器值
820
廣告經更新狀態計數器
822
824
偵測具有經更新狀態計數器之廣告
826
重新連接至配件
828
830
提供經更新狀態資訊
獲得經更新狀態資訊

圖8

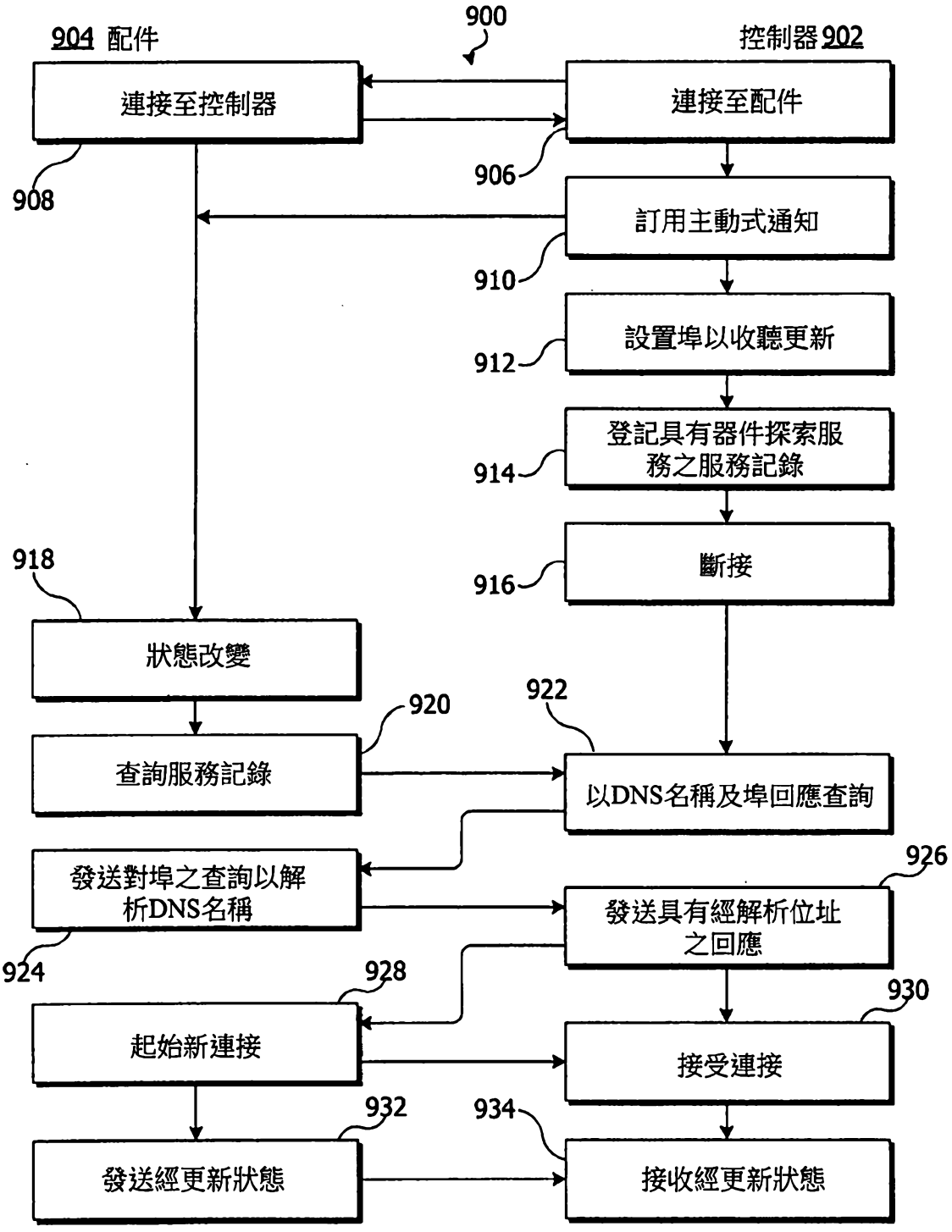

900
904 配件
控制器902
連接至控制器
連接至配件
908
906
訂用主動式通知
910
設置埠以收聽更新
912
登記具有器件探索服務之服務記錄
914
斷接
916
918
狀態改變
920
922
查詢服務記錄
以DNS名稱及埠回應查詢
發送對埠之查詢以解析DNS名稱
926
發送具有經解析位址之回應
924
928
930
起始新連接
接受連接
932
934
發送經更新狀態
接收經更新狀態

圖9

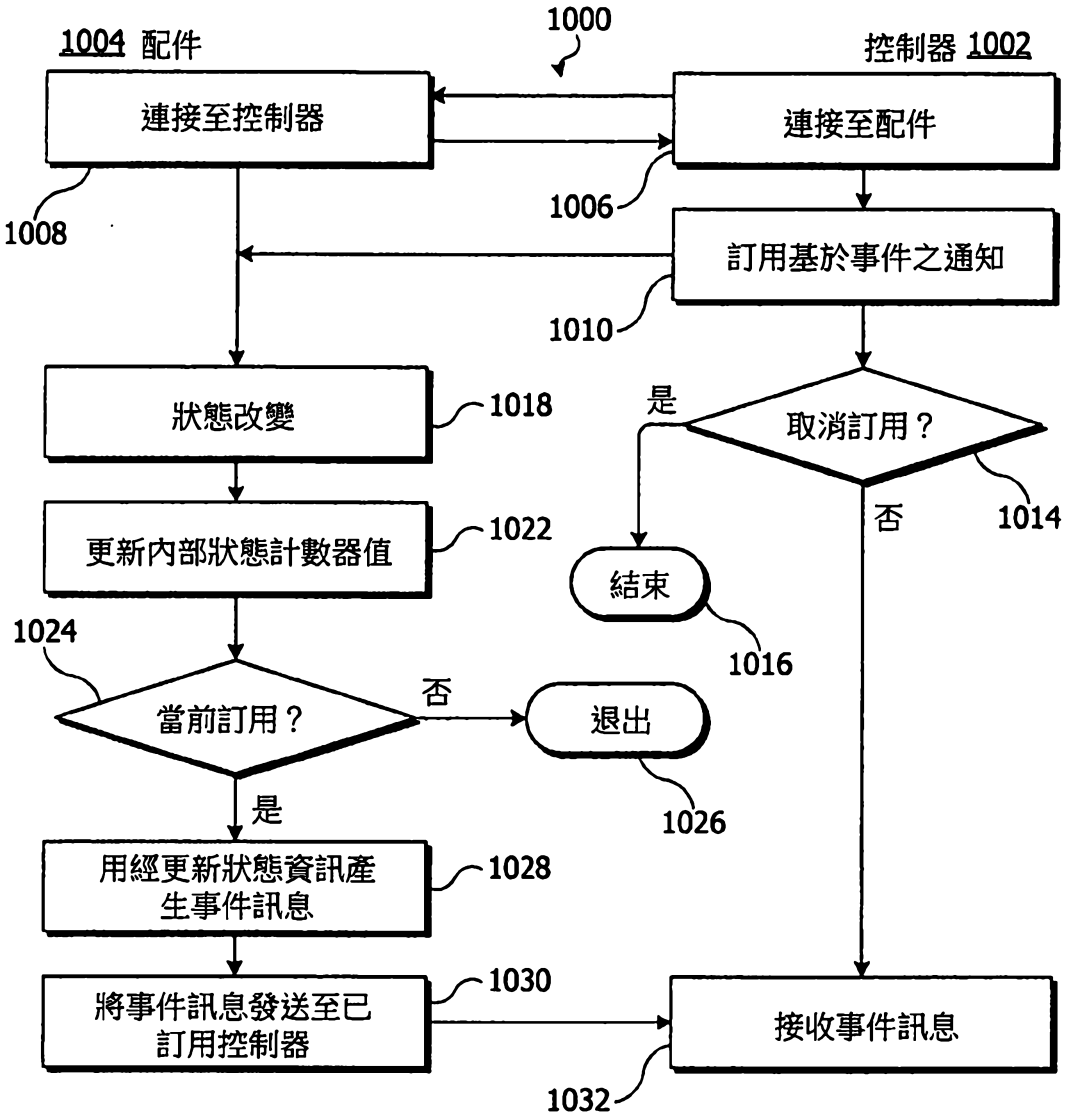

1000
1004 配件
控制器 1002
連接至控制器
連接至配件
1008
1006
訂用基於事件之通知
1010
狀態改變
1018
是
取消訂用？
否
1014
更新內部狀態計數器值
1022
結束
1016
1024
當前訂用？
否
退出
1026
是
用經更新狀態資訊產生事件訊息
1028
將事件訊息發送至已訂用控制器
1030
接收事件訊息
1032

圖10

1100

```
PUT /characteristics HTTP/1.1
Host: doors.local:12345
Content-Type: application/uap+json
Content-Length: <length>
{
    "characteristics" : [
        {
            "accessory ID" : 1,
            "instance ID" : 8,
            "notificationMode" : "ev"
        }
    ]
}
```

1102

圖11A

1120

```
EVENT/1.0 200 OK
Content-Type: application/uap+json
Content-Length: <length>
{
    "characteristics" : [
        {
            "accessory ID" : 1,
            "instance ID" : 8,
            "value" : 1
        }
    ]
}
```

1122

1124

圖11B

特性	性質	值
配對狀態請求 1201	格式	<tlv>
	類型	com.proto.pairing.state-request
	權限	UR, UW, PR, PW
特徵旗標 1202	格式	<int>
	類型	com.proto.pairing-features
	權限	UR, PR
配對當前狀態 1203	格式	<tlv>
	類型	com.proto.pairing.state-current
	權限	UR, PR
配對清單 1204	格式	<tlv>
	類型	com.proto.pairing-list
	權限	PR
配對ID 1205	格式	<string>
	類型	com.proto.pairing-identifier
	權限	UR, PR

圖12

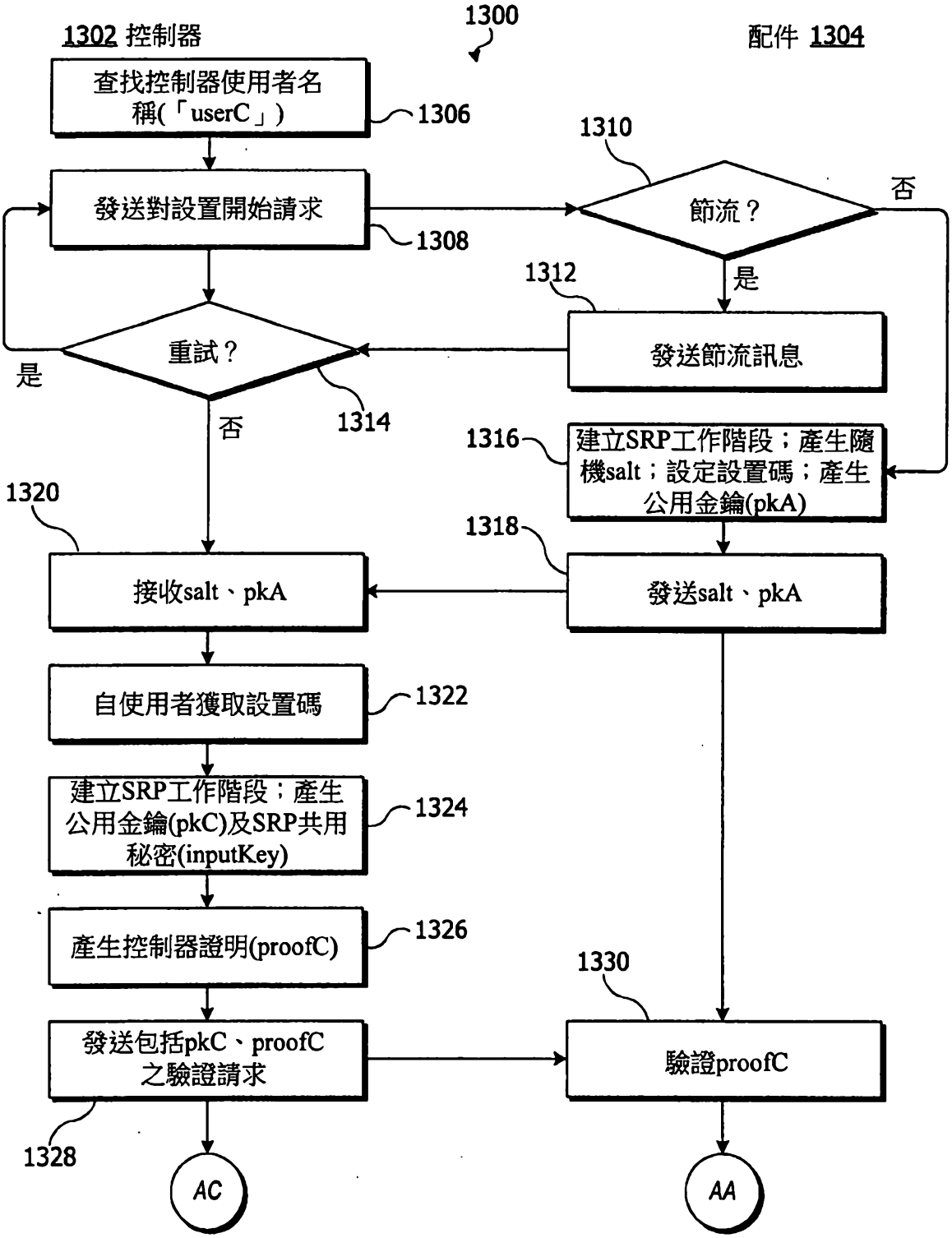

1300
1302 控制器
配件 1304
查找控制器使用者名稱(「userC」)
1306
發送對設置開始請求
1308
1310
節流？
否
是
1312
發送節流訊息
重試？
是
否
1314
1316
建立SRP工作階段；產生隨機salt；設定設置碼；產生公用金鑰(pkA)
1318
發送salt、pkA
1320
接收salt、pkA
自使用者獲取設置碼
1322
建立SRP工作階段；產生公用金鑰(pkC)及SRP共用秘密(inputKey)
1324
產生控制器證明(proofC)
1326
1330
發送包括pkC、proofC之驗證請求
驗證proofC
1328
AC
AA

圖13A

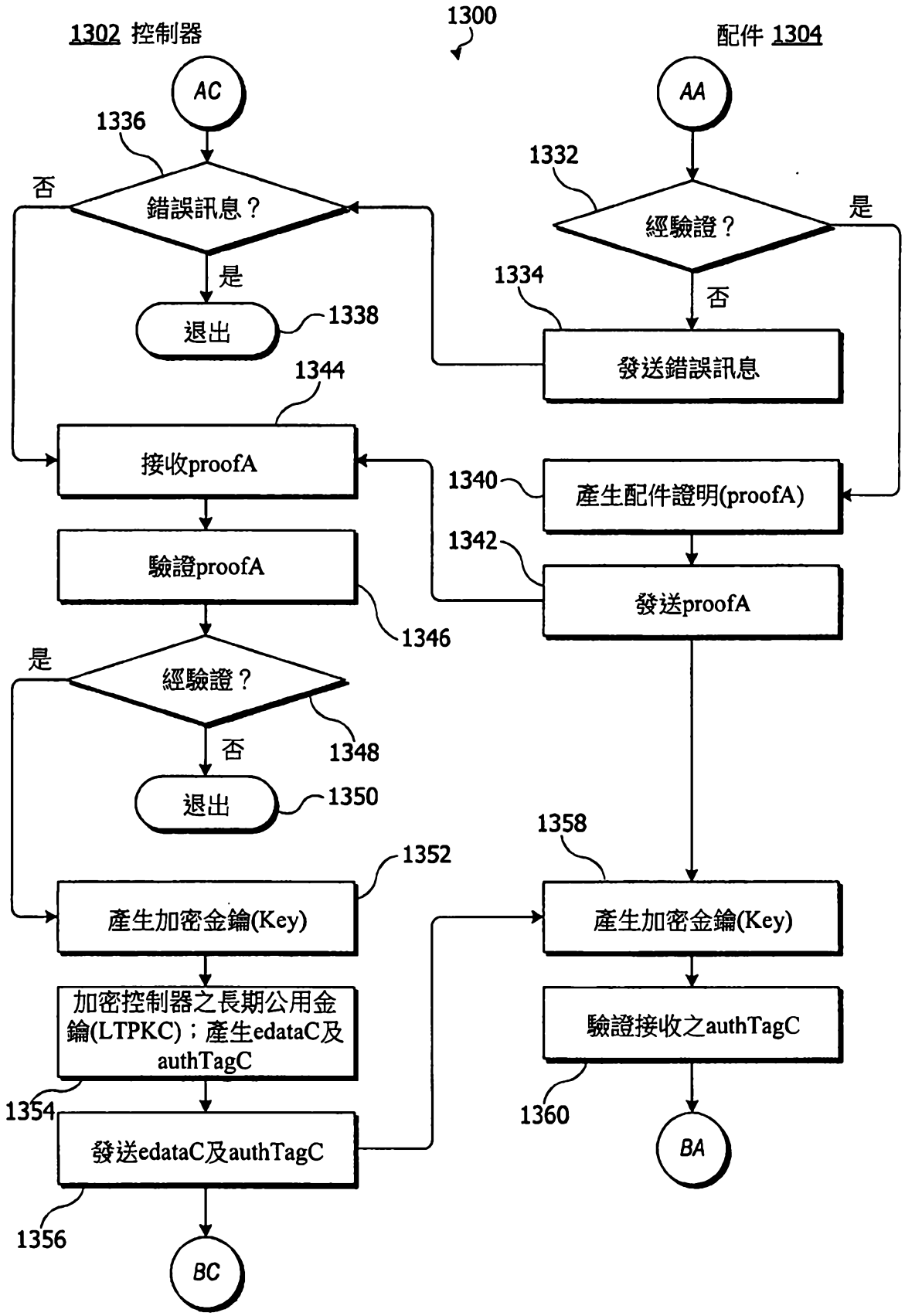

1300
1302 控制器
配件 1304
AC
AA
1336
1332
錯誤訊息？
否
是
經驗證？
是
否
退出
1338
1334
發送錯誤訊息
1344
接收proofA
1340
產生配件證明(proofA)
驗證proofA
1342
發送proofA
1346
是
經驗證？
1348
否
退出
1350
1358
1352
產生加密金鑰(Key)
產生加密金鑰(Key)
加密控制器之長期公用金鑰(LTPKC)；產生edataC及authTagC
驗證接收之authTagC
1354
1360
發送edataC及authTagC
BA
1356
BC

圖13B

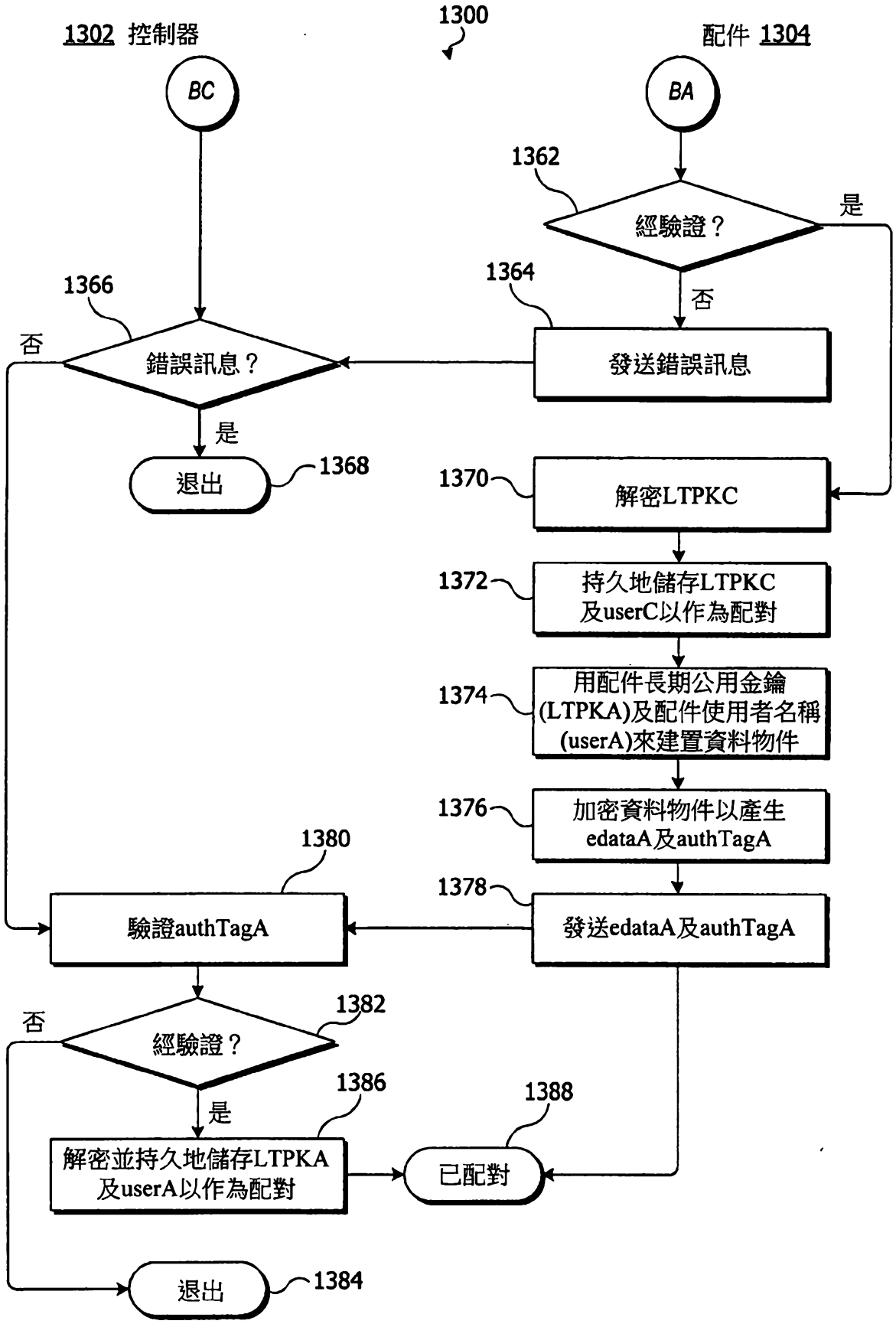

1300
1302 控制器
配件 1304
BC
BA
1362
經驗證？
是
否
1364
1366
否
錯誤訊息？
發送錯誤訊息
是
退出
1368
1370
解密LTPKC
1372
持久地儲存LTPKC
及userC以作為配對
1374
用配件長期公用金鑰
(LTPKA)及配件使用者名稱
(userA)來建置資料物件
1376
加密資料物件以產生
edataA及authTagA
1380
1378
驗證authTagA
發送edataA及authTagA
否
1382
經驗證？
1386
1388
是
解密並持久地儲存LTPKA
及userA以作為配對
已配對
退出
1384

圖13C

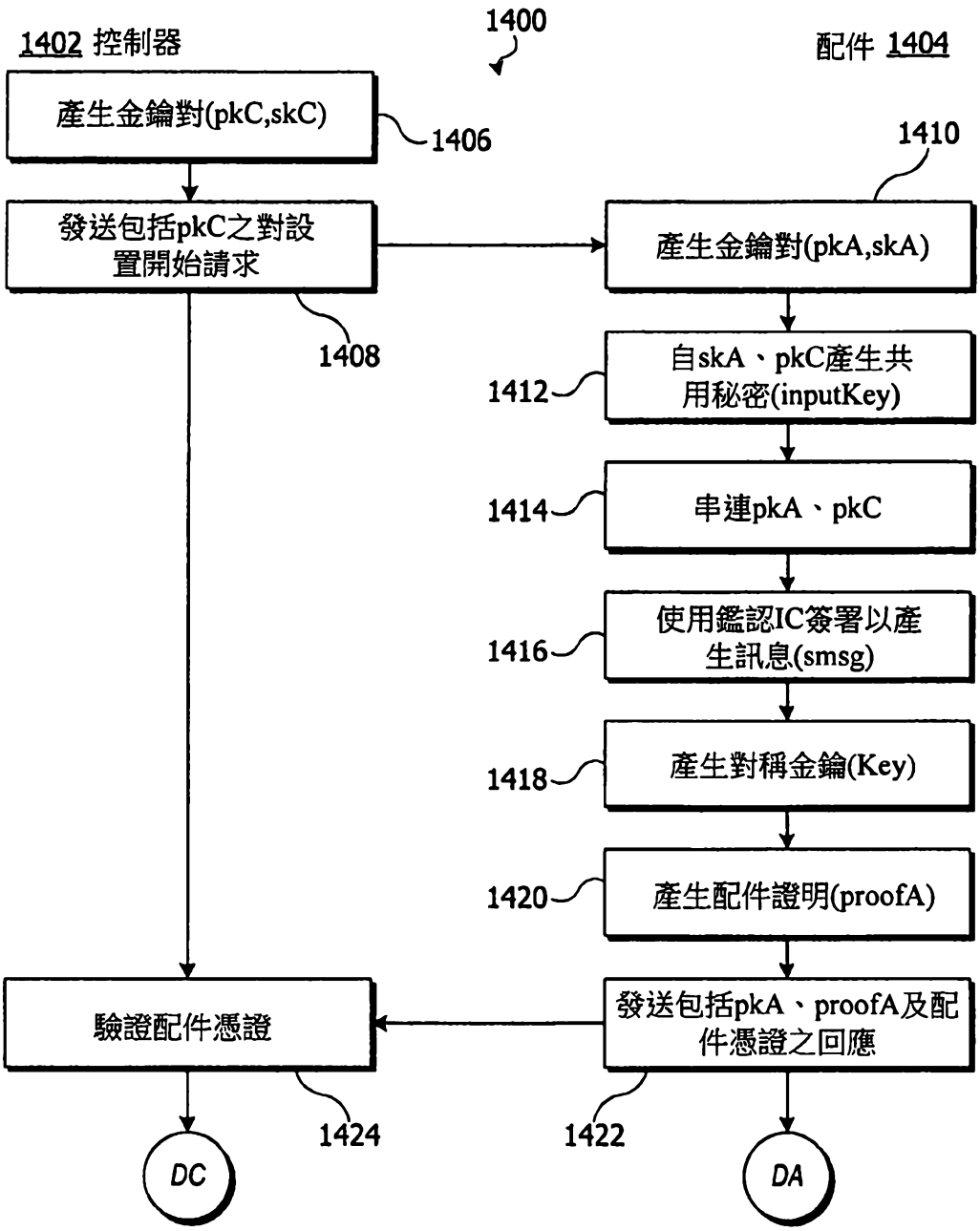

1400
1402 控制器
配件 1404
產生金鑰對(pkC,skC)
1406
1410
發送包括pkC之對設置開始請求
產生金鑰對(pkA,skA)
1408
1412
自skA、pkC產生共用秘密(inputKey)
1414
串連pkA、pkC
1416
使用鑑認IC簽署以產生訊息(smsg)
1418
產生對稱金鑰(Key)
1420
產生配件證明(proofA)
驗證配件憑證
發送包括pkA、proofA及配件憑證之回應
1424
1422
DC
DA

圖14A

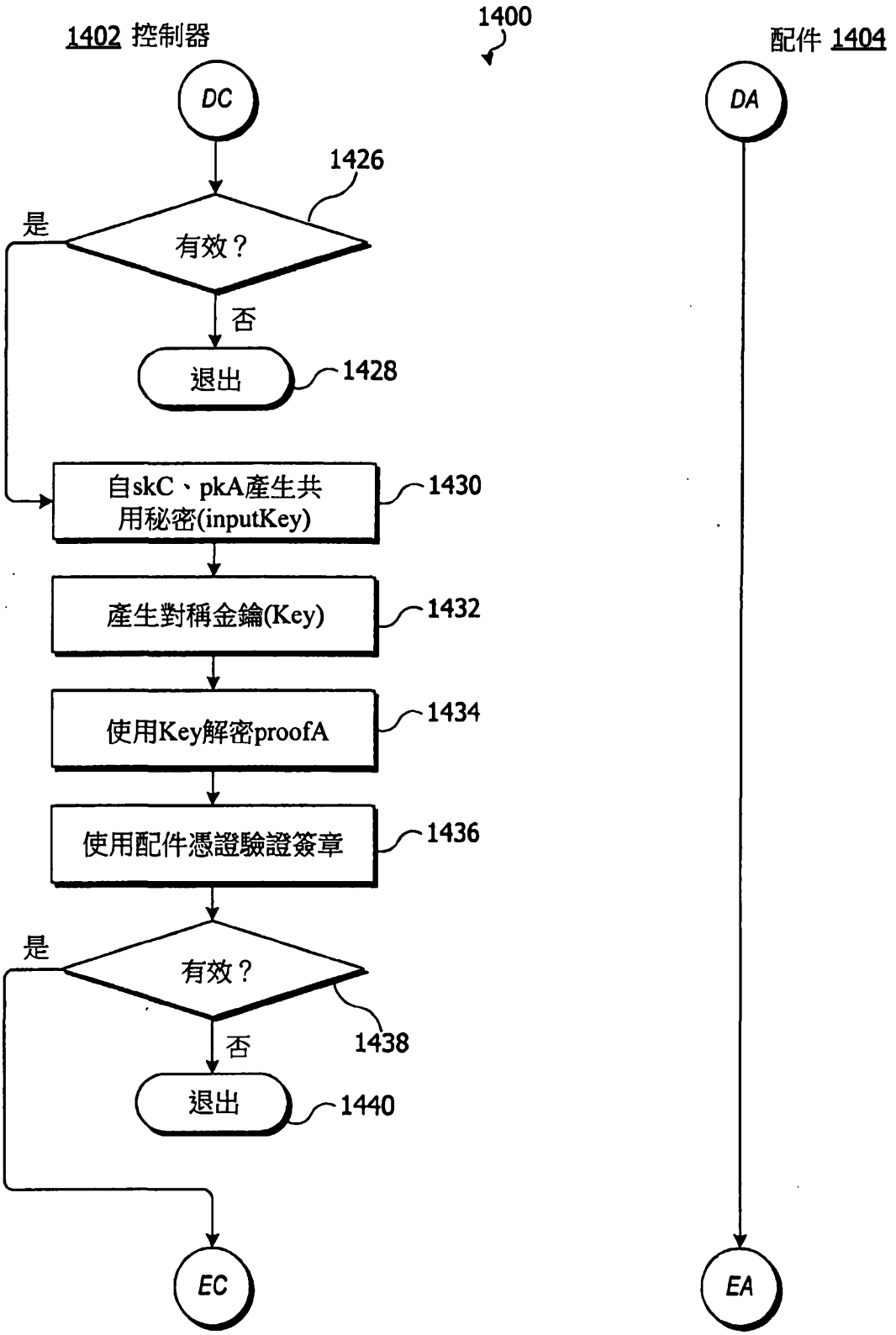

1400
1402 控制器
配件 1404
DC
DA
1426
是
有效？
否
退出
1428
自skC、pkA產生共用秘密(inputKey)
1430
產生對稱金鑰(Key)
1432
使用Key解密proofA
1434
使用配件憑證驗證簽章
1436
是
有效？
1438
否
退出
1440
EC
EA

圖14B

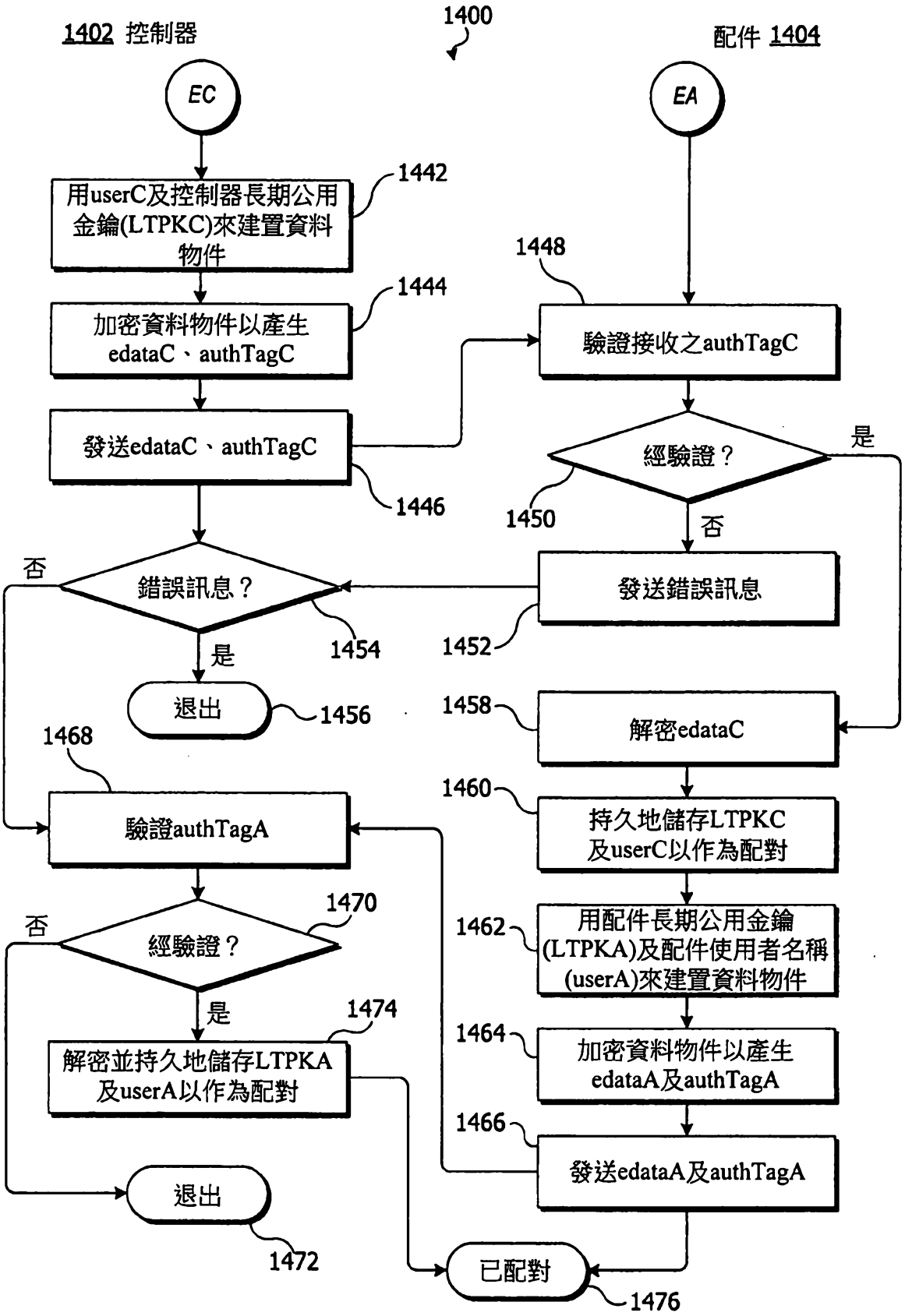

1400
1402 控制器
配件 1404
EC
EA
用userC及控制器長期公用金鑰(LTPKC)來建置資料物件
1442
加密資料物件以產生edataC、authTagC
1444
發送edataC、authTagC
1446
驗證接收之authTagC
1448
經驗證？
是
否
1450
發送錯誤訊息
1452
錯誤訊息？
否
是
1454
退出
1456
解密edataC
1458
持久地儲存LTPKC及userC以作為配對
1460
用配件長期公用金鑰(LTPKA)及配件使用者名稱(userA)來建置資料物件
1462
加密資料物件以產生edataA及authTagA
1464
發送edataA及authTagA
1466
驗證authTagA
1468
經驗證？
1470
解密並持久地儲存LTPKA及userA以作為配對
1474
退出
1472
已配對
1476

圖14C

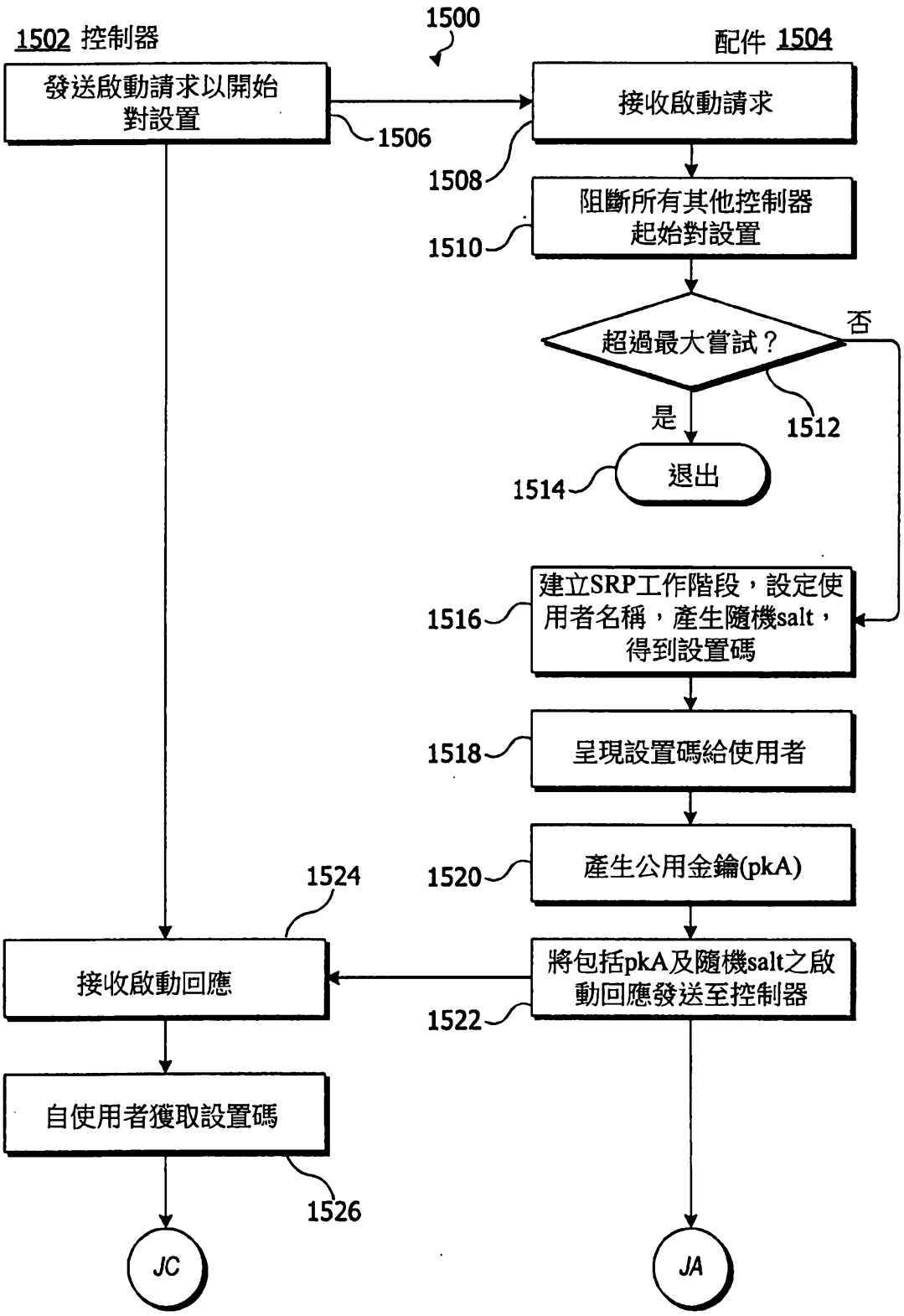

1500
1502 控制器
配件 1504
發送啟動請求以開始對設置
1506
接收啟動請求
1508
阻斷所有其他控制器起始對設置
1510
超過最大嘗試？
否
是
1512
退出
1514
建立SRP工作階段，設定使用者名稱，產生隨機salt，得到設置碼
1516
呈現設置碼給使用者
1518
產生公用金鑰(pkA)
1520
1524
接收啟動回應
將包括pkA及隨機salt之啟動回應發送至控制器
1522
自使用者獲取設置碼
1526
JC
JA

圖15A

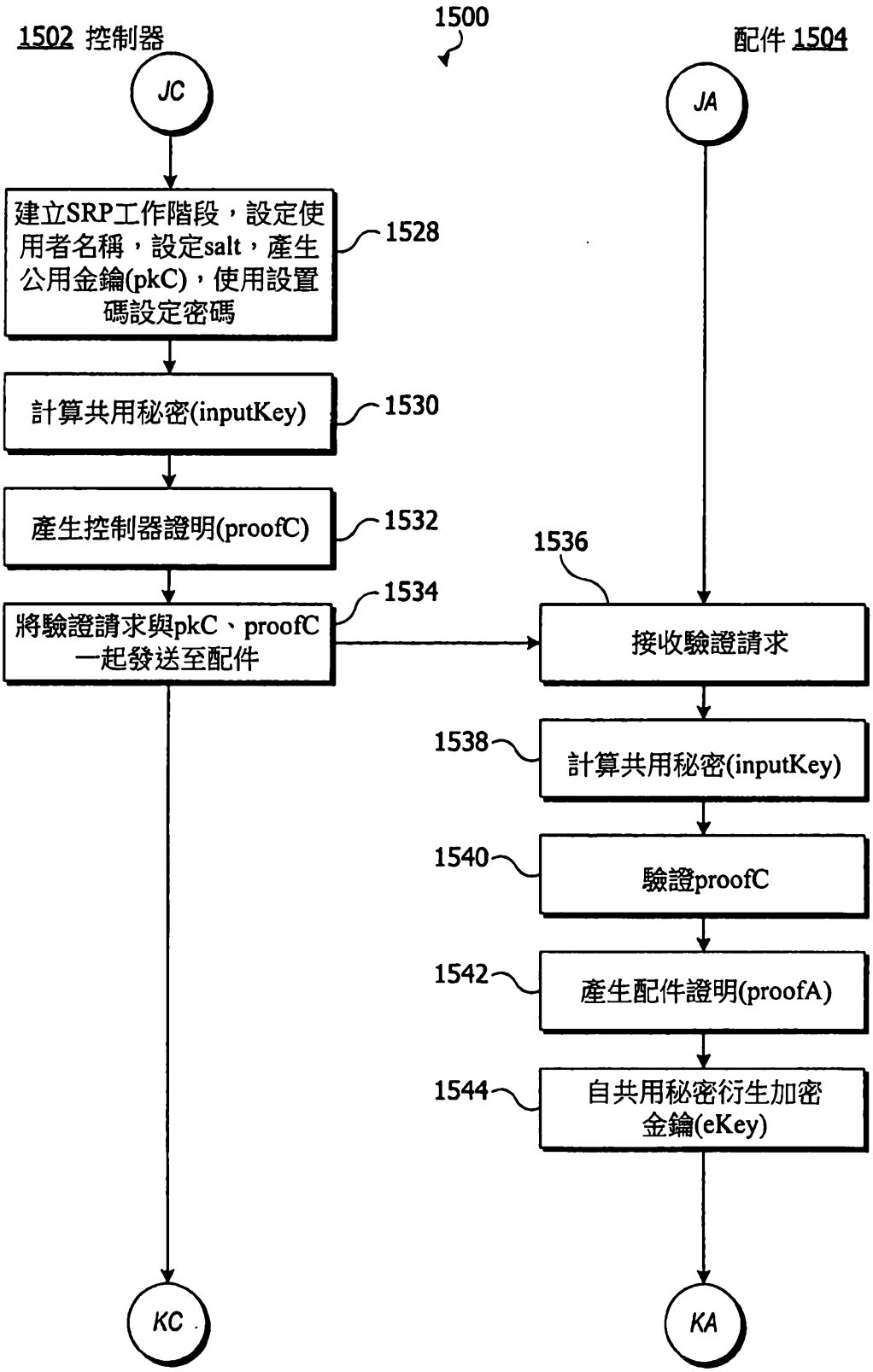

1500
1502 控制器
配件 1504
JC
JA
建立SRP工作階段，設定使用者名稱，設定salt，產生公用金鑰(pkC)，使用設置碼設定密碼
1528
計算共用秘密(inputKey)
1530
產生控制器證明(proofC)
1532
將驗證請求與pkC、proofC一起發送至配件
1534
1536
接收驗證請求
1538
計算共用秘密(inputKey)
1540
驗證proofC
1542
產生配件證明(proofA)
1544
自共用秘密衍生加密金鑰(eKey)
KC
KA

圖15B

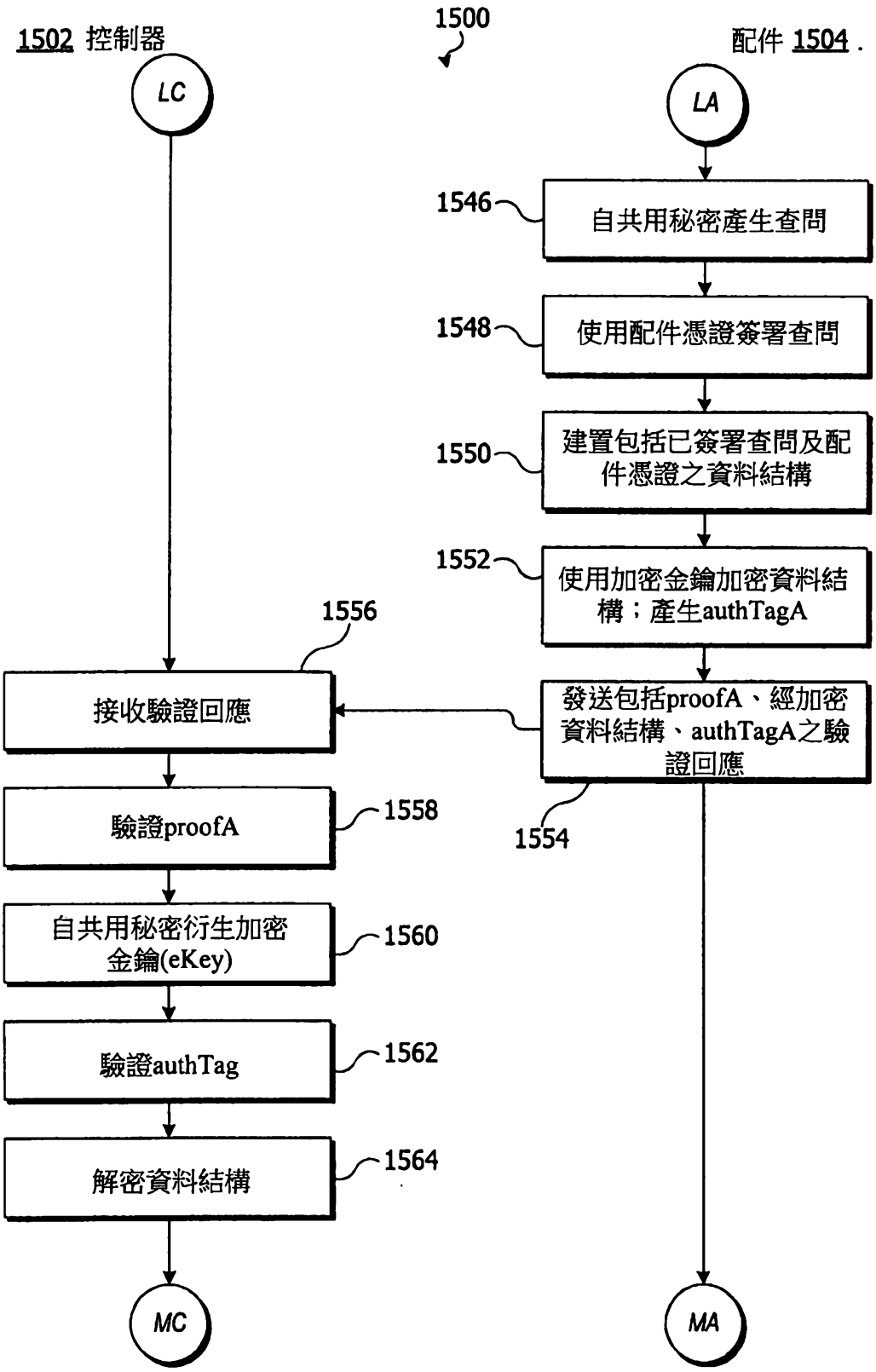

1500
1502 控制器
配件 1504
LC
LA
1546
自共用秘密產生查問
1548
使用配件憑證簽署查問
1550
建置包括已簽署查問及配件憑證之資料結構
1552
使用加密金鑰加密資料結構；產生authTagA
1556
接收驗證回應
發送包括proofA、經加密資料結構、authTagA之驗證回應
1554
驗證proofA
1558
自共用秘密衍生加密金鑰(eKey)
1560
驗證authTag
1562
解密資料結構
1564
MC
MA

圖15C

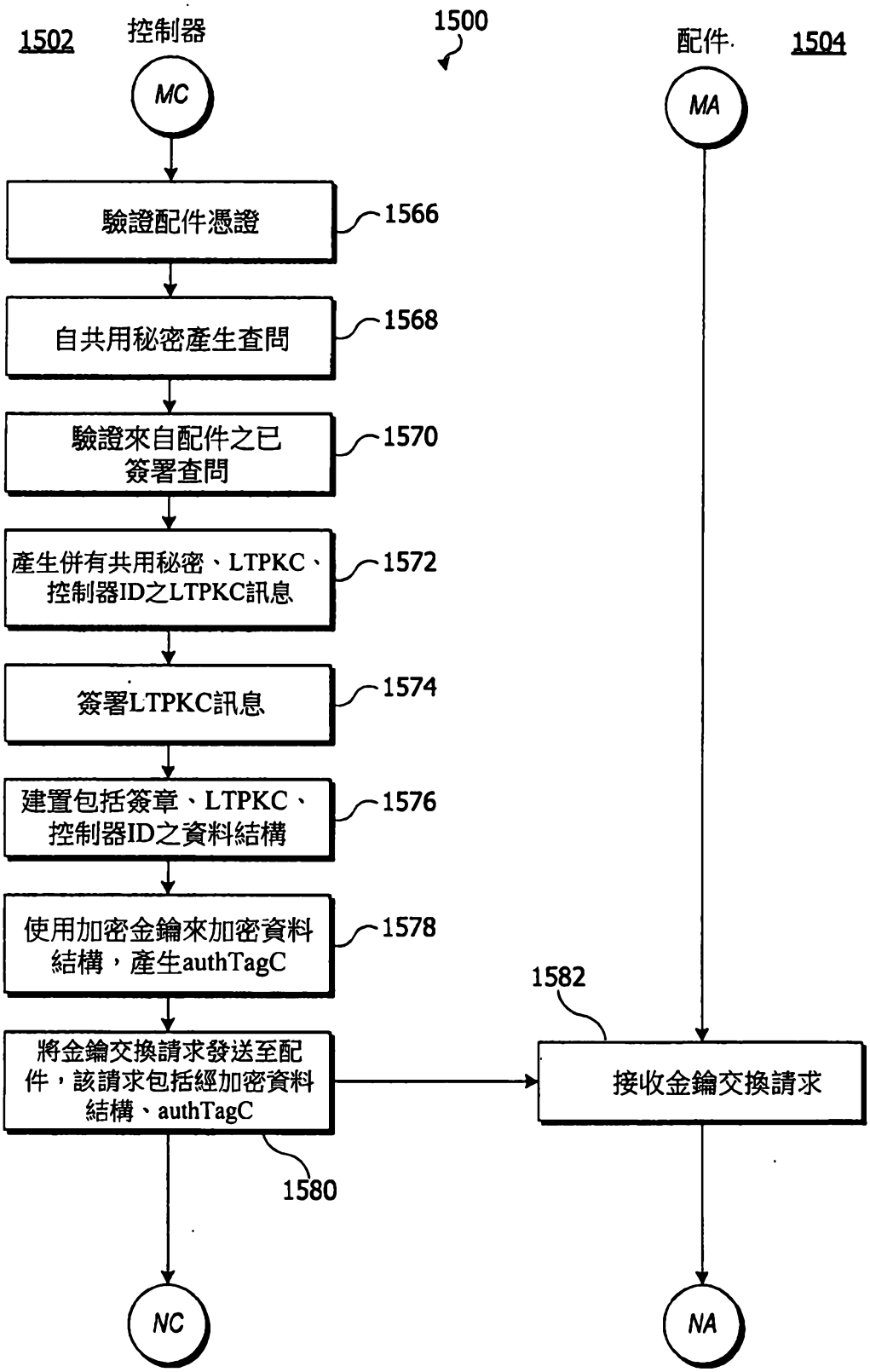

1502
控制器
1500
配件
1504
MC
MA
驗證配件憑證
1566
自共用秘密產生查問
1568
驗證來自配件之已簽署查問
1570
產生併有共用秘密、LTPKC、控制器ID之LTPKC訊息
1572
簽署LTPKC訊息
1574
建置包括簽章、LTPKC、控制器ID之資料結構
1576
使用加密金鑰來加密資料結構，產生authTagC
1578
1582
將金鑰交換請求發送至配件，該請求包括經加密資料結構、authTagC
接收金鑰交換請求
1580
NC
NA

圖15D

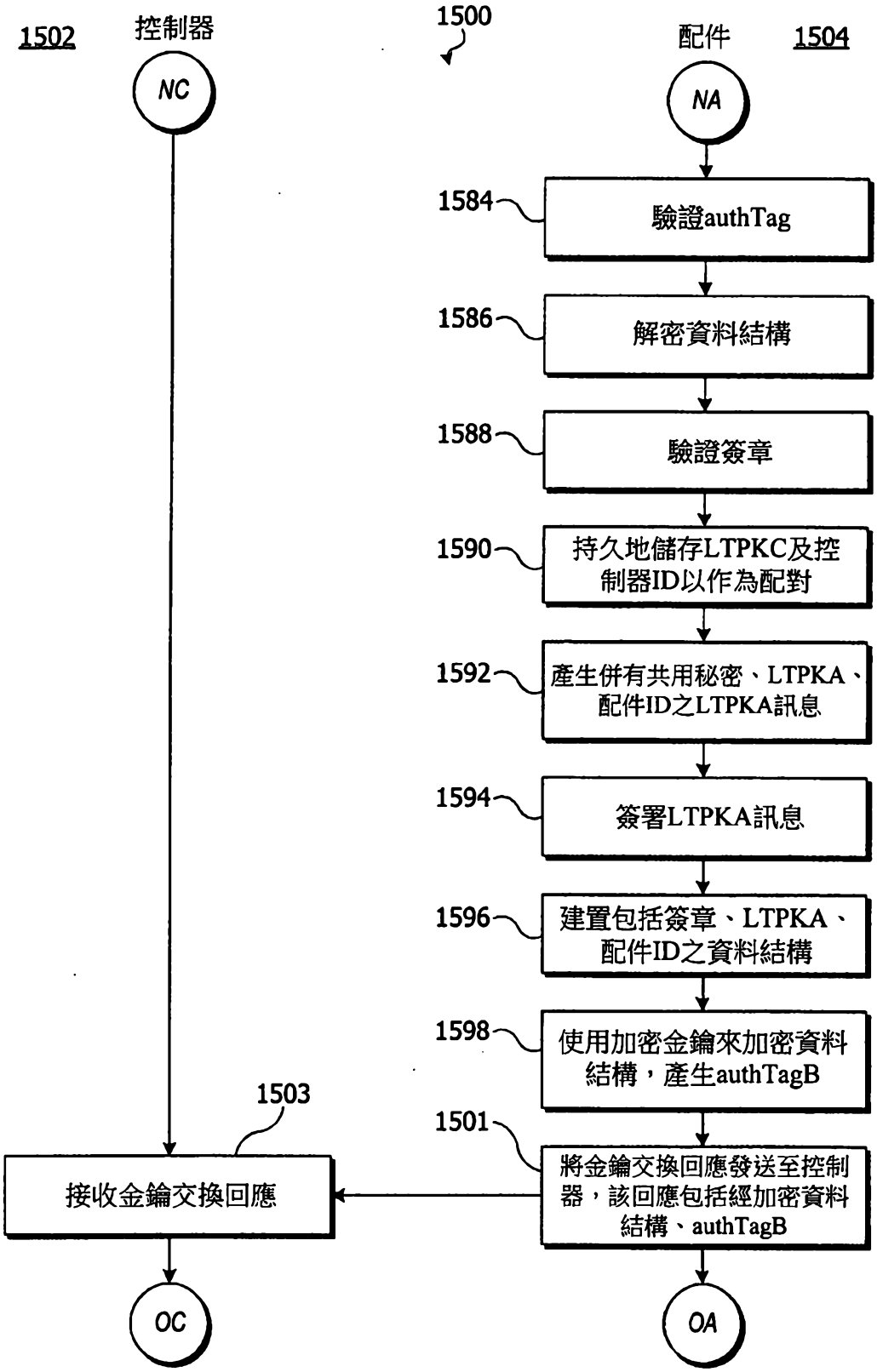

1502
控制器
NC
1500
配件
1504
NA
1584
驗證authTag
1586
解密資料結構
1588
驗證簽章
1590
持久地儲存LTPKC及控制器ID以作為配對
1592
產生併有共用秘密、LTPKA、配件ID之LTPKA訊息
1594
簽署LTPKA訊息
1596
建置包括簽章、LTPKA、配件ID之資料結構
1598
使用加密金鑰來加密資料結構，產生authTagB
1501
將金鑰交換回應發送至控制器，該回應包括經加密資料結構、authTagB
1503
接收金鑰交換回應
OC
OA

圖15E

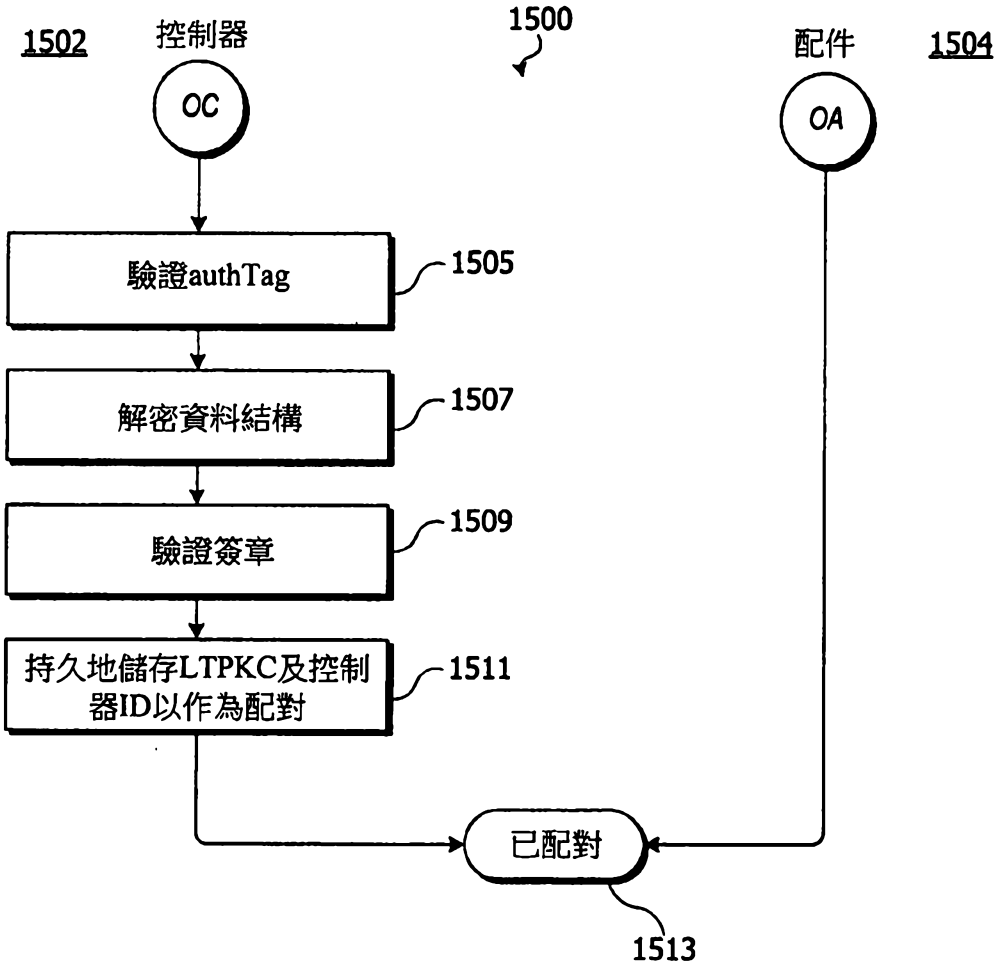

1502
控制器
1500
配件
1504
OC
OA
驗證authTag
1505
解密資料結構
1507
驗證簽章
1509
持久地儲存LTPKC及控制器ID以作為配對
1511
已配對
1513

圖15F

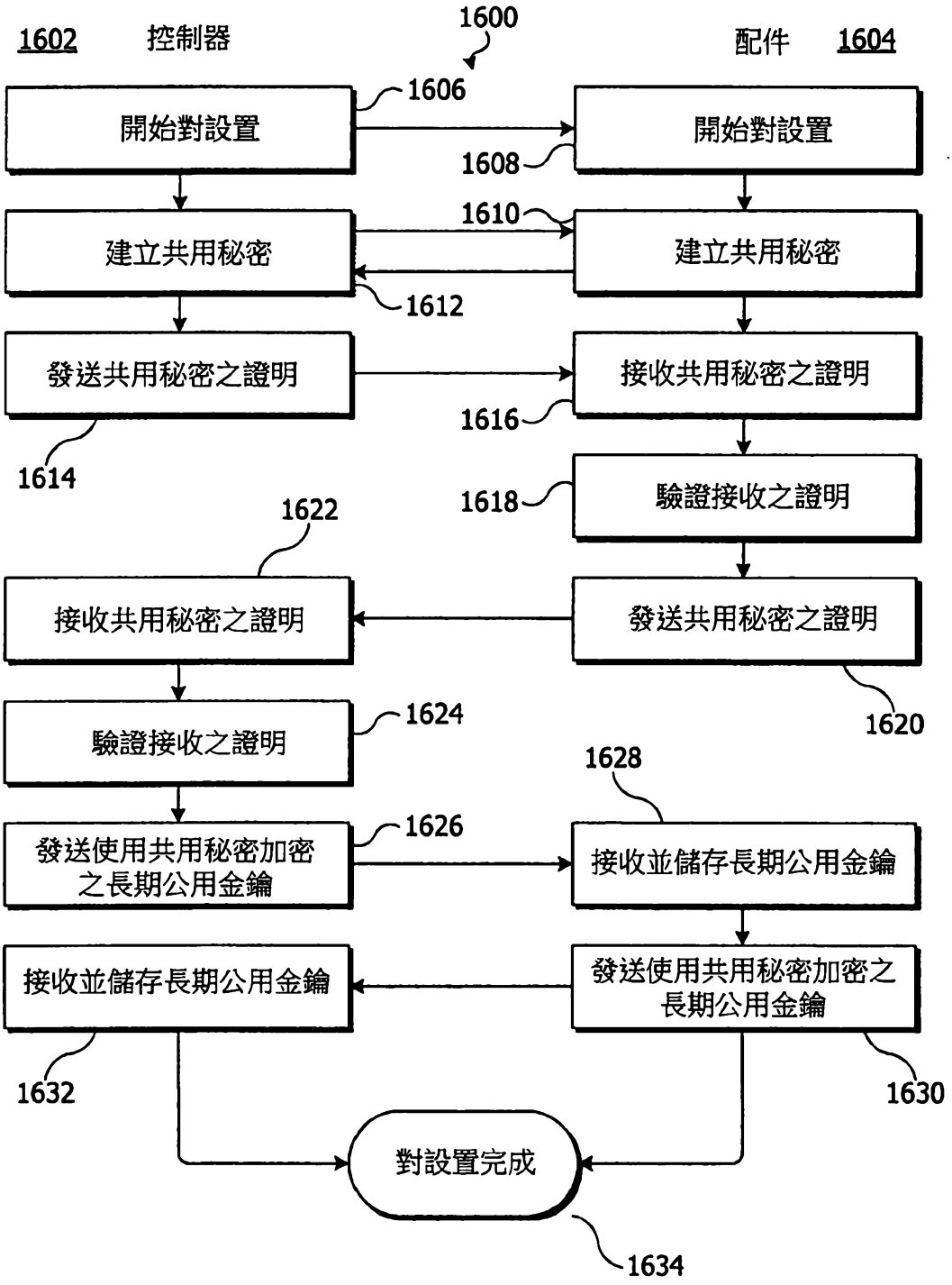

1602
控制器
1600
配件
1604
1606
開始對設置
開始對設置
1608
1610
建立共用秘密
建立共用秘密
1612
發送共用秘密之證明
接收共用秘密之證明
1616
1614
1618
驗證接收之證明
1622
接收共用秘密之證明
發送共用秘密之證明
1620
驗證接收之證明
1624
1628
發送使用共用秘密加密之長期公用金鑰
1626
接收並儲存長期公用金鑰
接收並儲存長期公用金鑰
發送使用共用秘密加密之長期公用金鑰
1632
1630
對設置完成
1634

圖16

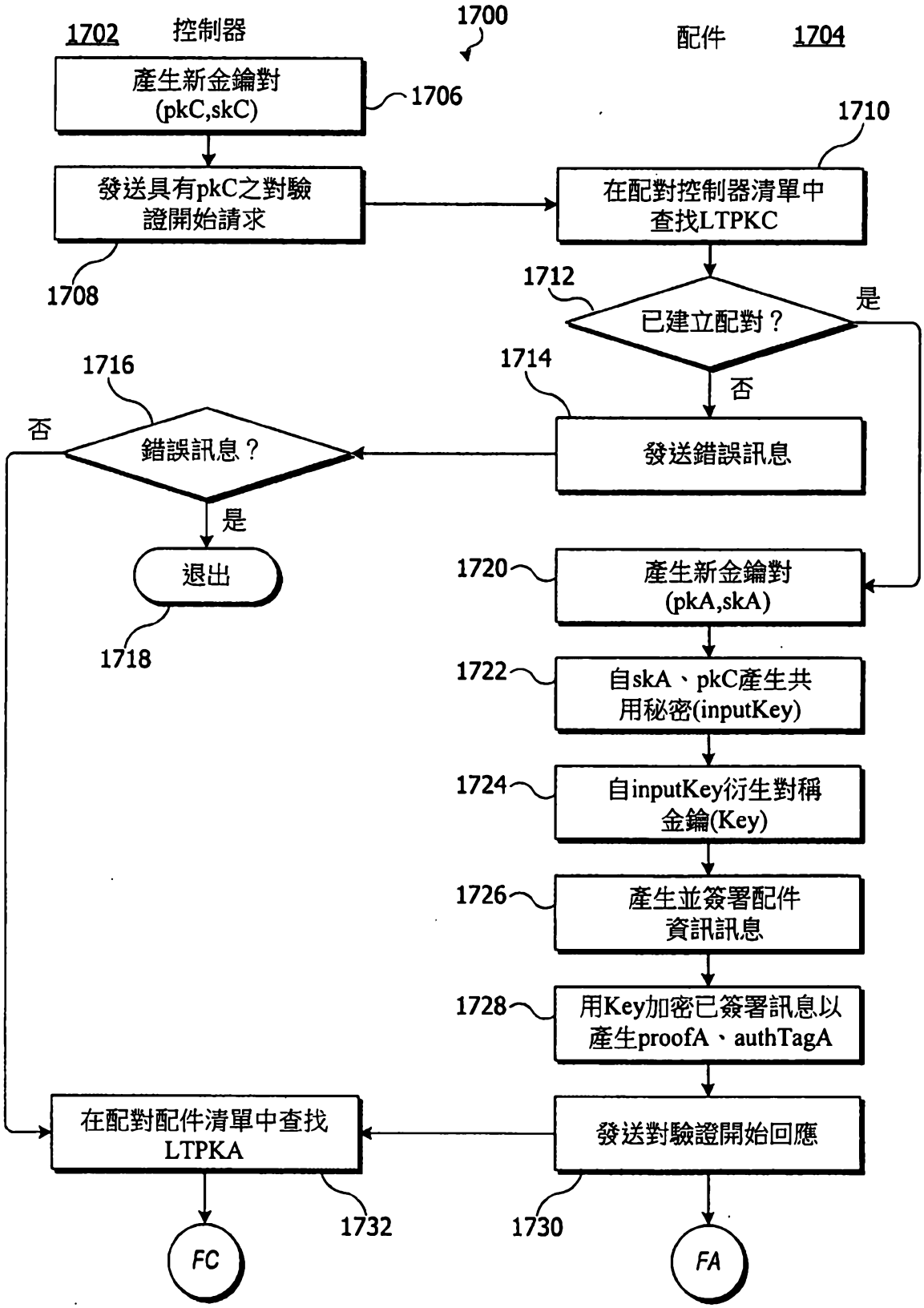

1700
1702 控制器
配件 1704
產生新金鑰對 (pkC,skC)
1706
發送具有pkC之對驗證開始請求
1708
在配對控制器清單中查找LTPKC
1710
已建立配對？
1712
是
否
發送錯誤訊息
1714
錯誤訊息？
1716
否
是
退出
1718
產生新金鑰對 (pkA,skA)
1720
自skA、pkC產生共用秘密(inputKey)
1722
自inputKey衍生對稱金鑰(Key)
1724
產生並簽署配件資訊訊息
1726
用Key加密已簽署訊息以產生proofA、authTagA
1728
發送對驗證開始回應
1730
在配對配件清單中查找LTPKA
1732
FC
FA

圖17A

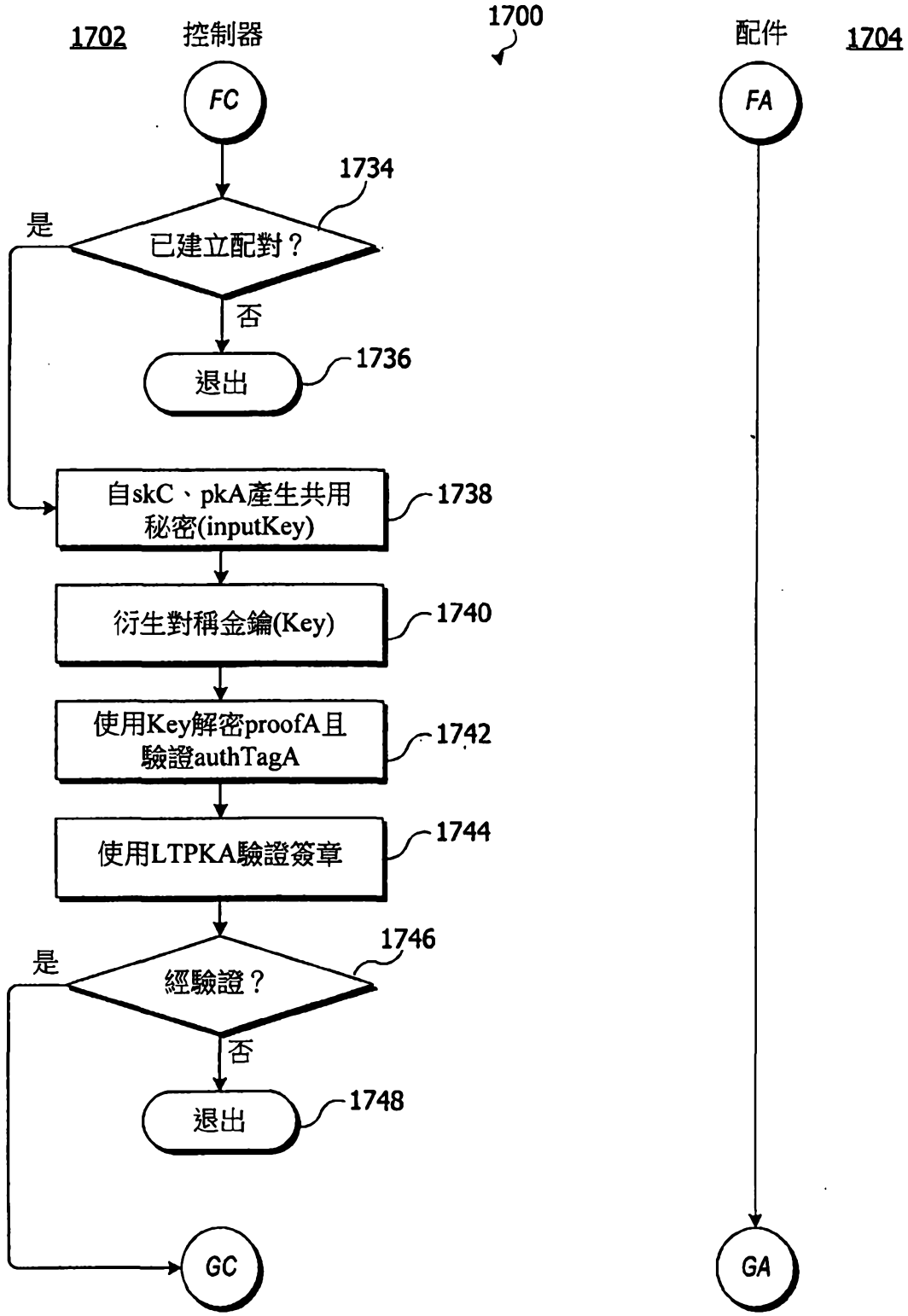

1700
1702
控制器
配件
1704
FC
FA
1734
是
已建立配對？
否
退出
1736
自skC、pkA產生共用秘密(inputKey)
1738
衍生對稱金鑰(Key)
1740
使用Key解密proofA且驗證authTagA
1742
使用LTPKA驗證簽章
1744
1746
是
經驗證？
否
退出
1748
GC
GA

圖17B

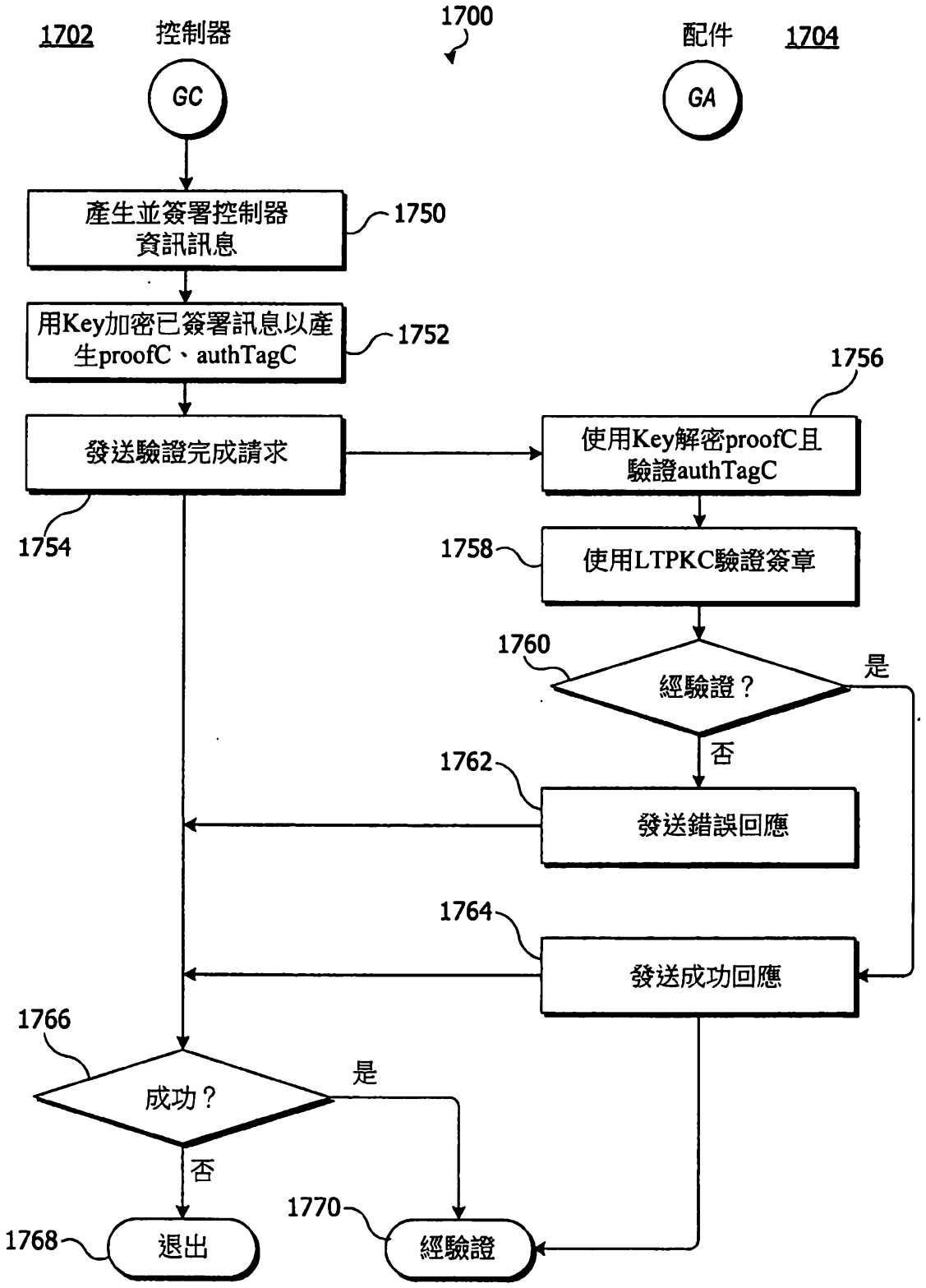

1700
1702
控制器
GC
配件
1704
GA
產生並簽署控制器資訊訊息
1750
用Key加密已簽署訊息以產生proofC、authTagC
1752
發送驗證完成請求
1754
1756
使用Key解密proofC且驗證authTagC
1758
使用LTPKC驗證簽章
1760
經驗證？
是
否
1762
發送錯誤回應
1764
發送成功回應
1766
成功？
是
否
1768
退出
1770
經驗證

圖17C

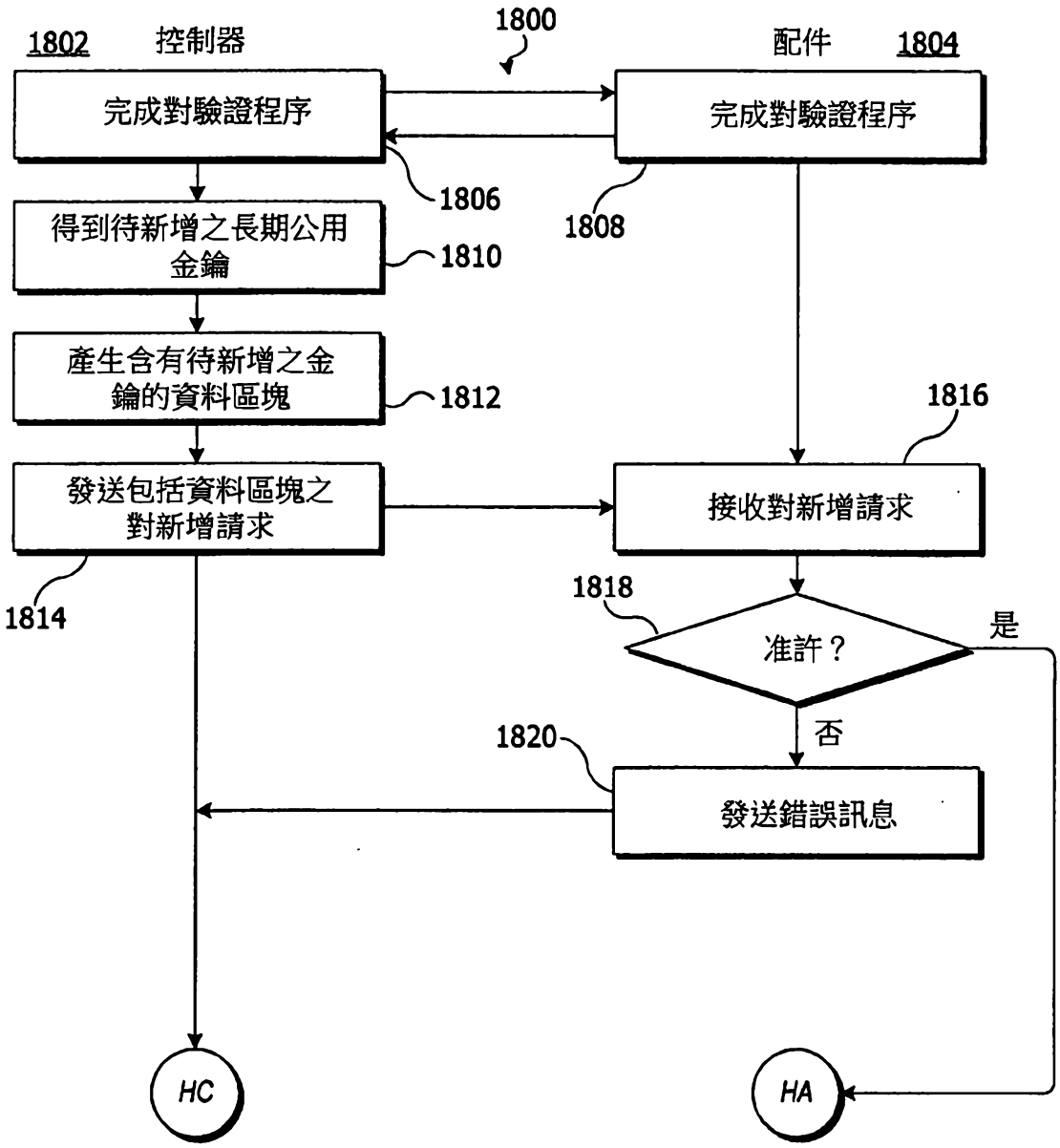

1800
1802
控制器
配件
1804
完成對驗證程序
完成對驗證程序
1806
1808
得到待新增之長期公用金鑰
1810
產生含有待新增之金鑰的資料區塊
1812
1816
發送包括資料區塊之對新增請求
接收對新增請求
1814
1818
准許？
是
否
1820
發送錯誤訊息
HC
HA

圖18A

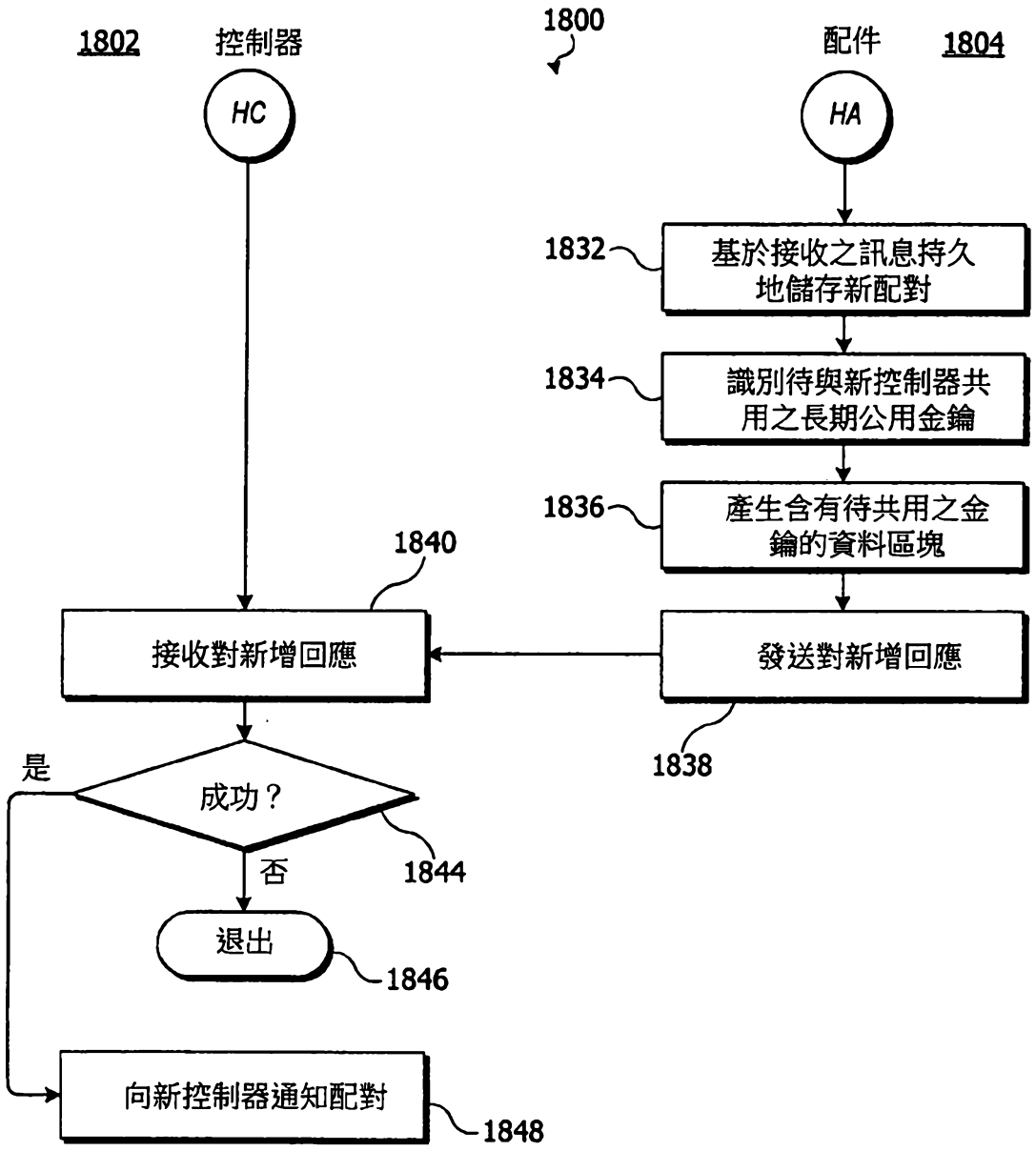

1802
控制器
1800
配件
1804
HC
HA
1832
基於接收之訊息持久地儲存新配對
1834
識別待與新控制器共用之長期公用金鑰
1836
產生含有待共用之金鑰的資料區塊
1840
接收對新增回應
發送對新增回應
1838
是
成功？
1844
否
退出
1846
向新控制器通知配對
1848

圖18B

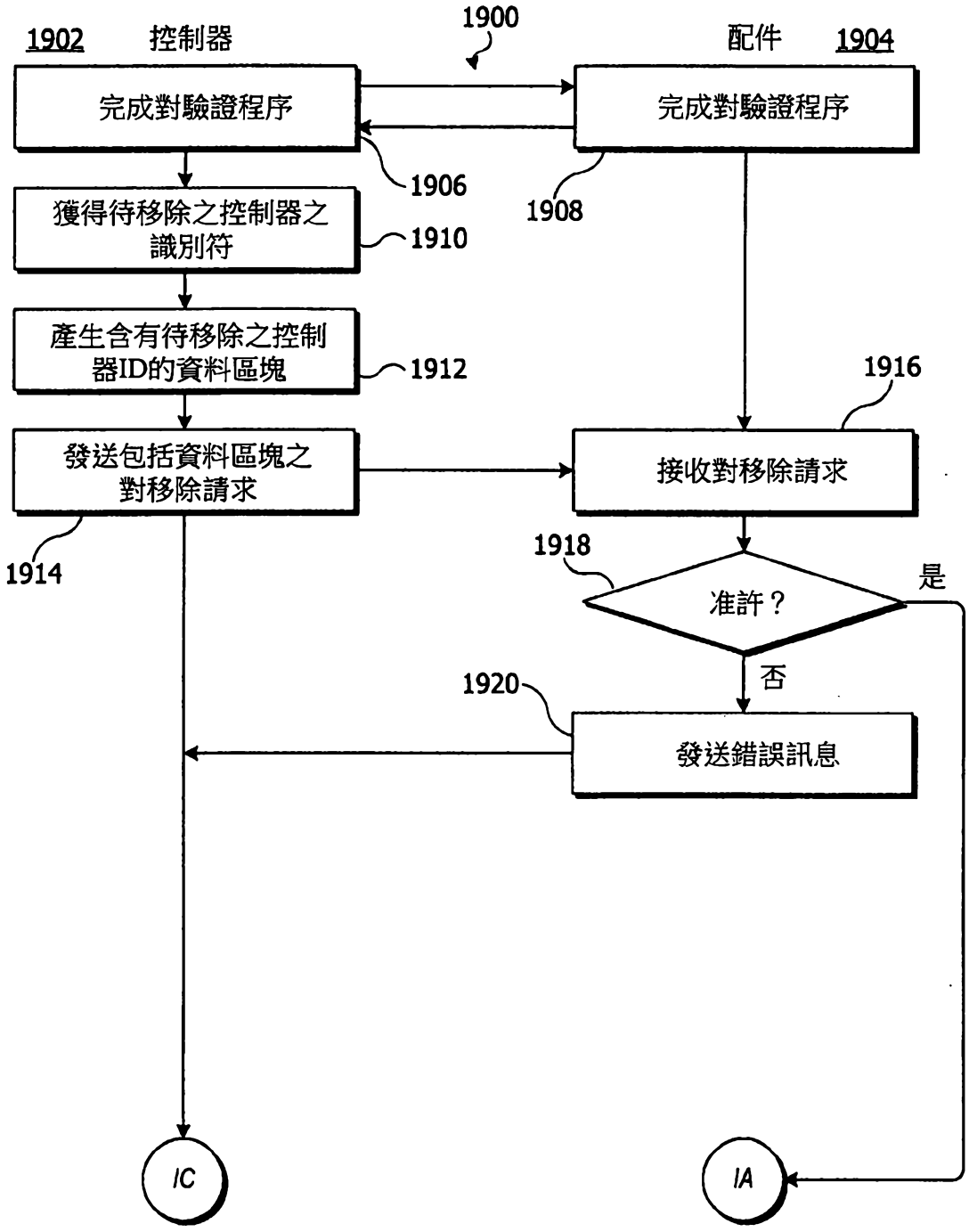

1900
1902
控制器
配件
1904
完成對驗證程序
完成對驗證程序
1906
1908
獲得待移除之控制器之識別符
1910
產生含有待移除之控制器ID的資料區塊
1912
1916
發送包括資料區塊之對移除請求
接收對移除請求
1914
1918
准許？
是
否
1920
發送錯誤訊息
IC
IA

圖19A

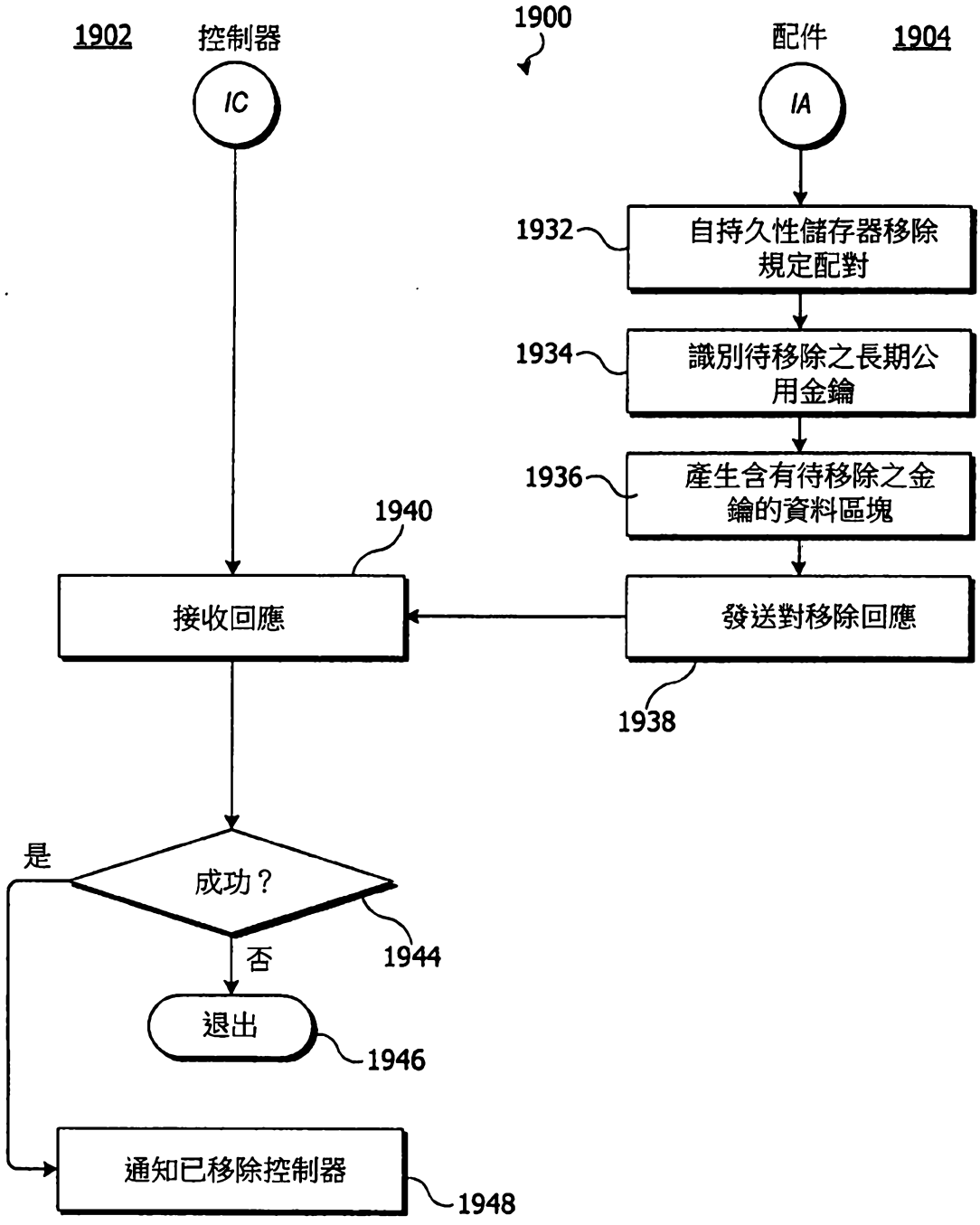

1902
控制器
IC
1900
配件
1904
IA
1932
自持久性儲存器移除規定配對
1934
識別待移除之長期公用金鑰
1936
產生含有待移除之金鑰的資料區塊
1940
接收回應
發送對移除回應
1938
是
成功？
1944
否
退出
1946
通知已移除控制器
1948

圖19B

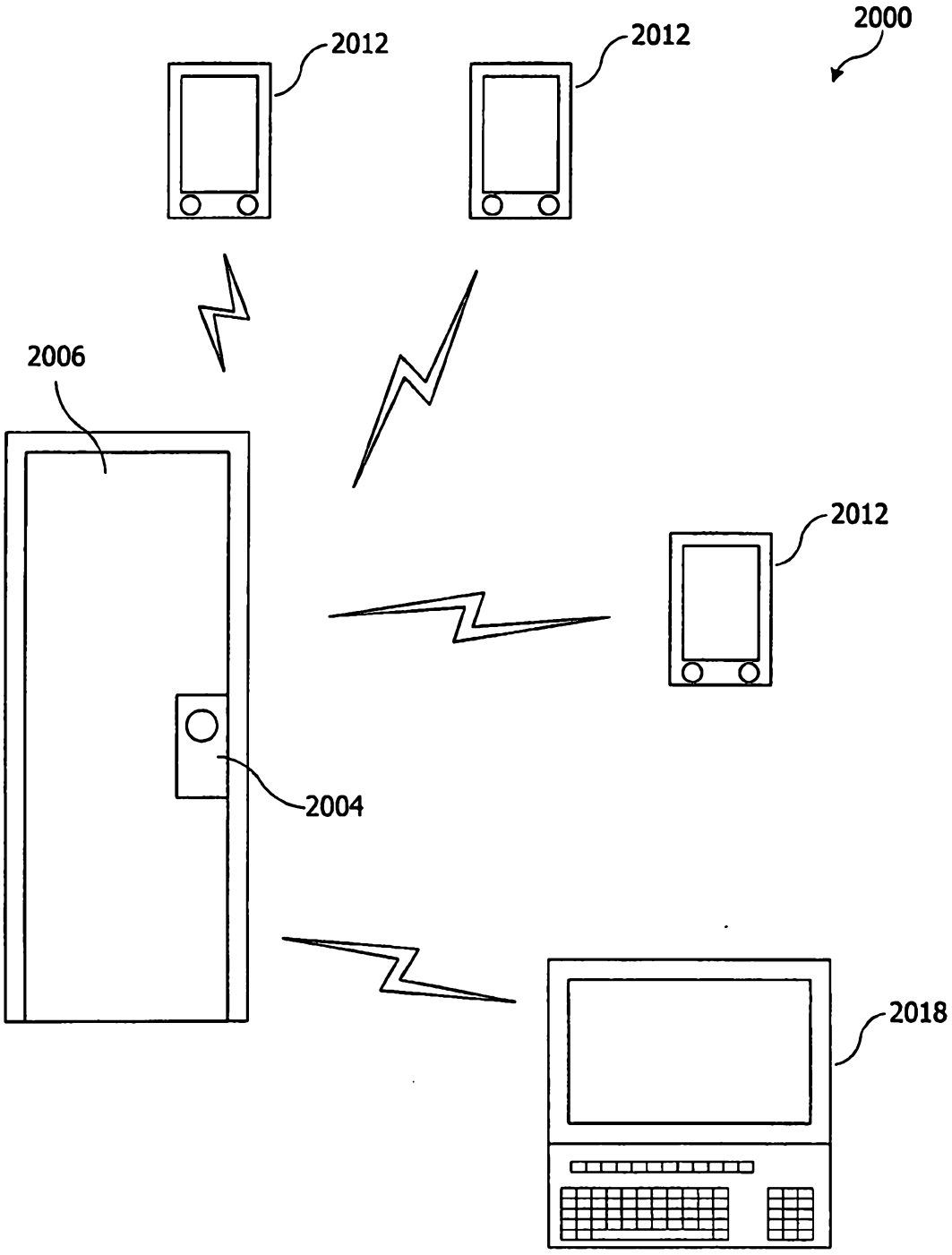


圖20

2100

服務	特性	IID	值
配件資訊(執行個體ID=1) 2102	com.proto.ch.identify	2	空值
	com.proto.ch.manufacturer	3	"Acme"
	com.proto.ch.model	4	"A-Lock"
	com.proto.ch.name	5	"A Name"
	com.proto.ch.serial-number	6	"7353"
鎖機構(執行個體ID=7) 2104	com.proto.ch.lock-mech.current-state 2110	8	解除鎖定
	com.proto.ch.lock-mech.target-state 2112	9	解除鎖定
	com.proto.ch.name	10	"A-Lock-Mech"
鎖管理(執行個體ID=11) 2106	com.proto.ch.lock-mgt.control-point 2114	12	空值
	com.proto.ch.version	13	1.2.3
	com.proto.ch.logs	14	<tlv>
	com.proto.ch.admin-only-access	15	假
	com.proto.ch.lock-mgt.auto-timeout	16	5
	com.proto.ch.lock-mech.last-action	17	6
	com.proto.ch.door-state.current	18	關閉
	com.proto.ch.name	19	"A-Lock-Mgr"

圖21

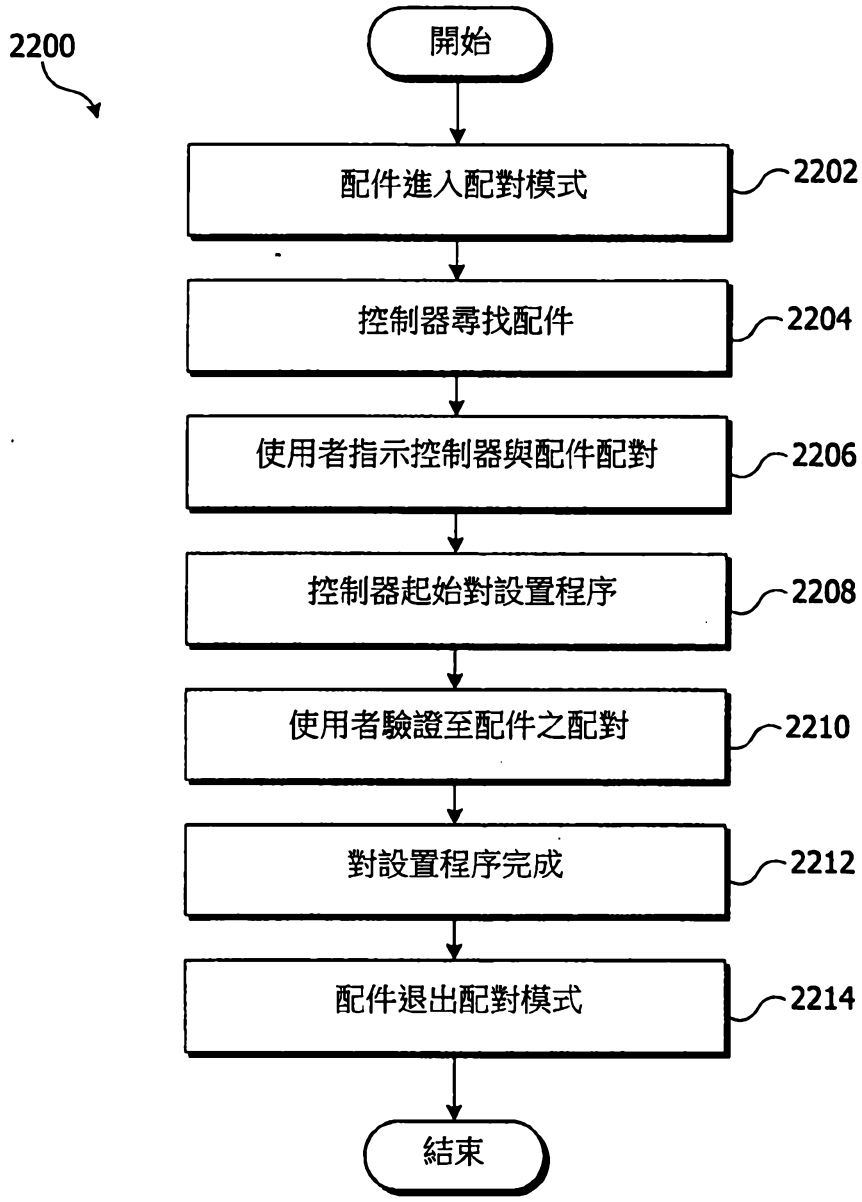

2200
開始
配件進入配對模式
2202
控制器尋找配件
2204
使用者指示控制器與配件配對
2206
控制器起始對設置程序
2208
使用者驗證至配件之配對
2210
對設置程序完成
2212
配件退出配對模式
2214
結束

圖22

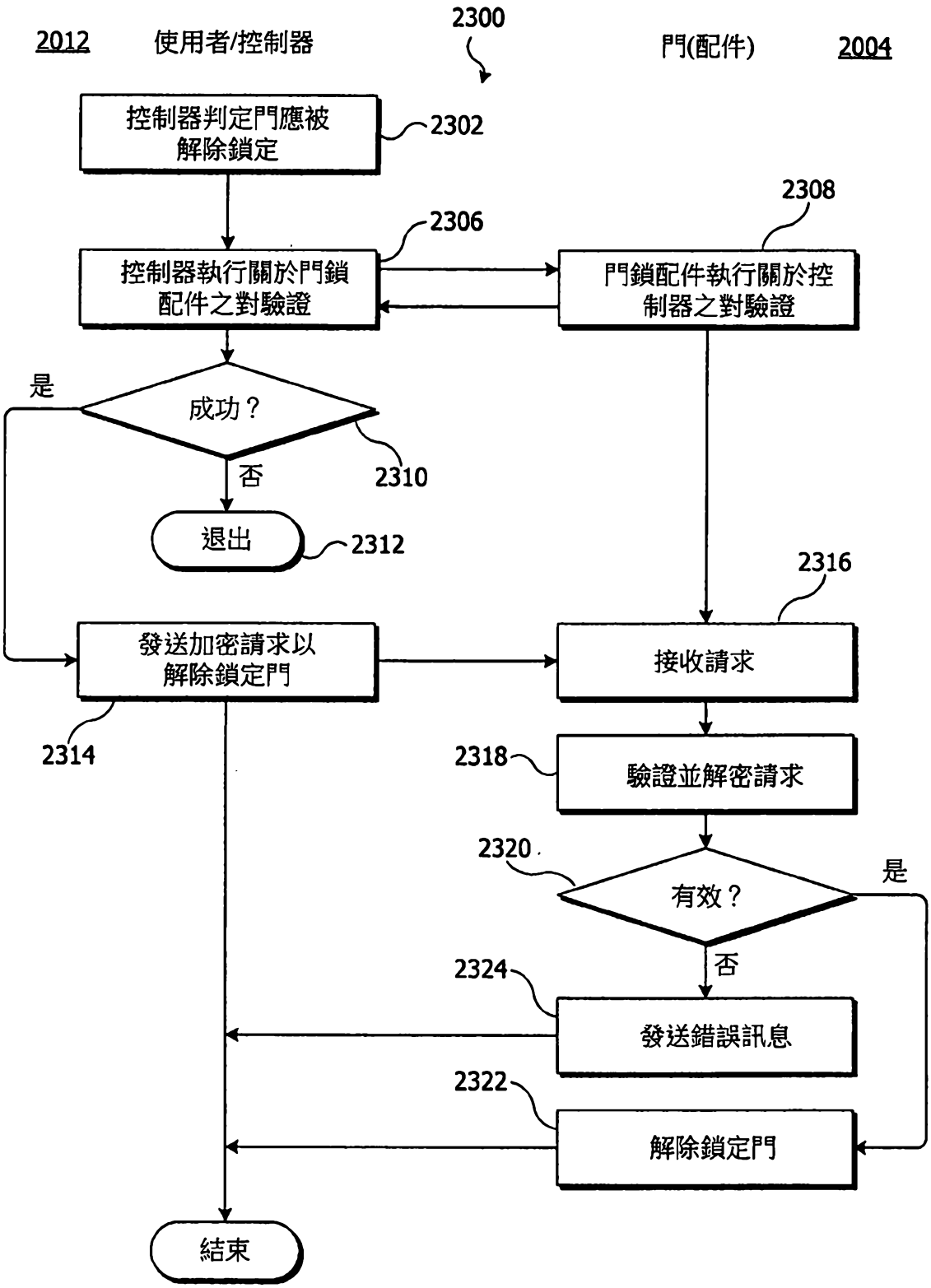

2012
使用者/控制器
2300
門(配件)
2004
控制器判定門應被解除鎖定
2302
2306
控制器執行關於門鎖配件之對驗證
2308
門鎖配件執行關於控制器之對驗證
是
成功？
否
2310
退出
2312
2316
發送加密請求以解除鎖定門
接收請求
2314
2318
驗證並解密請求
2320
有效？
是
否
2324
發送錯誤訊息
2322
解除鎖定門
結束

圖23

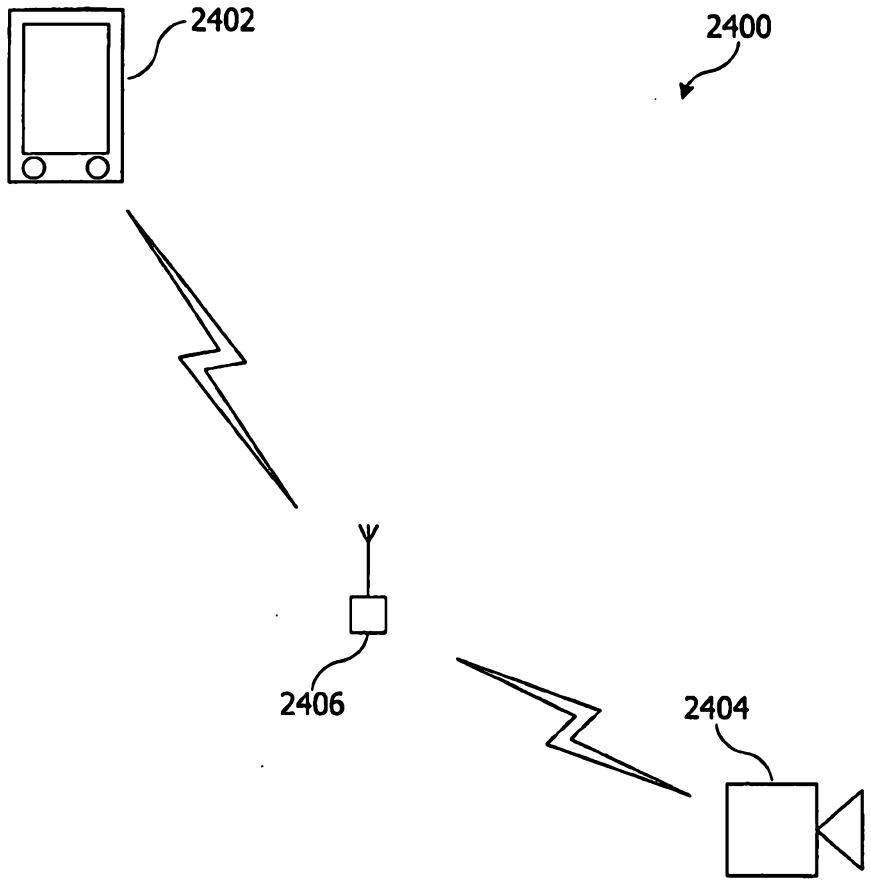


圖24

服務	性質	值
IP攝影機串流 2501	類型	com.proto.svc.ip-camera-streaming
	必需特性	com.proto.ch.on
		com.proto.ch.ip-cam-mgt.session.start
		com.proto.ch.ip-cam-mgt.session.end
		com.proto.ch.video.codec.name
		com.proto.ch.video.codec.parameters
		com.proto.ch.video.attributes
		com.proto.ch.rtp.video-payload-type
		com.proto.ch.rtp.protocol
		com.proto.ch.rtcp.extensions
		com.proto.ch.srtp.crytpo-suite
	選用之特性	com.proto.ch.audio.codec.name
		com.proto.ch.audio.codec.parameters
		com.proto.ch.audio.codec.channels
		com.proto.ch.audio.attributes
		com.proto.ch.rtp.audio.clock-rate
		com.proto.ch.rtp.audio.payload-type
記錄 2502	類型	com.proto.svc.recording
	必需特性	com.proto.ch.recording.control
		com.proto.ch.recording.status
播放 2503	類型	com.proto.svc.playback
	必需特性	com.proto.ch.playback.control
		com.proto.ch.playback.status
	選用之特性	com.proto.ch.playback.speed

圖25A

服務	性質	值
攝影機 2504	類型	com.proto.svc.camera
	必需特性	com.ch.proto.on
	選用之特性	com.ch.proto.pan
		com.ch.proto.tilt
		com.ch.proto.zoom
		com.ch.proto.rotate
		com.ch.proto.night-vision
		com.ch.proto.mirror
麥克風 2505	類型	com.proto.svc.microphone
	必需特性	com.proto.ch.on
		com.proto.ch.volume
揚聲器 2506	類型	com.proto.svc.speaker
	必需特性	com.proto.ch.on
		com.proto.ch.volume

圖25B

特性	性質	值
工作階段開始 2601	類型	com.proto.ch.ip-cam-mgt.session.start
	權限	配對寫入
	格式	<object> [參見圖22B]
工作階段結束 2602	類型	com.proto.ch.ip-cam-mgt.session.end
	權限	配對寫入
	格式	<object>
視訊轉碼器名稱 2603	類型	com.proto.ch.video.codec.name
	權限	配對讀取
	格式	<string>
視訊轉碼器參數 2604	類型	com.proto.ch.video.codec.parameters
	權限	配對讀取
	格式	<object>
視訊屬性 2605	類型	com.proto.ch.video.attributes
	權限	配對讀取
	格式	<object>
RTP視訊有效負載類型 2606	類型	com.proto.ch.rtp.video.payload-type
	權限	配對讀取
	格式	<int>
RTP協定 2607	類型	com.proto.ch.rtp.protocol
	權限	配對讀取
	格式	<string>
RTCP延伸 2608	類型	com.proto.ch.rtp.extensions
	權限	配對讀取
	格式	Array of <string>
SRTP密碼編譯套件 2609	類型	com.proto.ch.srtp.crypto-suite
	權限	配對讀取
	格式	<string>

圖26A

特性	性質	值
音訊轉碼器名稱 2610	類型	com.proto.ch.audio.codec.name
	權限	配對讀取
	格式	<string>
音訊轉碼器參數 2611	類型	com.proto.ch.audio.codec.parameters
	權限	配對讀取
	格式	<object>
音訊轉碼器頻道 2612	類型	com.proto.ch.audio.codec.channels
	權限	配對讀取
	格式	<int>
音訊屬性 2613	類型	com.proto.ch.audio.attributes
	權限	配對讀取
	格式	<object>
RTP音訊時脈速率 2614	類型	com.proto.ch.rtp.audio.clock-rate
	權限	配對讀取
	格式	<int>
RTP音訊有效負載類型 2615	類型	com.proto.ch.rtp.audio.payload-type
	權限	配對讀取
	格式	<int>

圖26B

金鑰名稱	值類型	描述
「工作階段ID」 2631	UUID	用於串流工作階段之UUID
「控制器IP」 2632	字串	控制器用以接收視訊串流之IP位址
「控制器埠」 2633	整數	控制器用以接收視訊串流之埠
「控制器SRTP主控金鑰」 2634	字串	自控制器發送至攝影機的用於RTCP之SRTP主控金鑰
「控制器SRTP主控salt」 2635	字串	自控制器發送至攝影機的用於RTCP之SRTP主控salt
「視訊最大頻寬」 2636	整數	用於視訊之最大頻寬(kbps)
「音訊最大頻寬」 2637	整數	用於音訊之最大頻寬(kbps)

圖26C

特性	性質	值
夜視 2651	類型	com.proto.ch.ip-camera-night-vision
	格式	<int>
	權限	配對讀取，配對寫入
平移 2652	類型	com.proto.ch.pan
	格式	<int>
	權限	配對讀取，配對寫入
傾斜 2653	類型	com.proto.ch.tilt
	格式	<int>
	權限	配對讀取，配對寫入
旋轉 2654	類型	com.proto.ch.rotation
	格式	<int>
	權限	配對讀取，配對寫入
變焦 2655	類型	com.proto.ch.zoom
	格式	<float>
	權限	讀取/寫入/更新
鏡像 2656	類型	com.proto.ch.ip-camera-mirror
	格式	<boolean>
	權限	讀取/寫入/更新

圖26D

特性	性質	值
記錄控制 2661	類型	com.proto.ch.recording.control
	格式	<object>
	權限	配對寫入
記錄狀態 2662	類型	com.proto.ch.recording.status
	格式	<object>
	權限	配對讀取
播放控制 2663	類型	com.proto.ch.playback.control
	格式	<object>
	權限	配對寫入
播放狀態 2664	類型	com.proto.ch.playback.status
	格式	<object>
	權限	配對讀取
播放速度 2665	類型	com.proto.ch.playback.speed
	格式	<float>
	權限	配對讀取，配對寫入

圖26E

2700

```
{
   "services" : [
      {
         "type" : "com.proto.svc.accessory-info",
         "instanceID" : 1,
         "characteristics" : [
            {
               "type" : "com.proto.ch.id",
               "value" : "55:44:33:22:11:00",
               "perms" : [ "PR" ],
               "instanceID" : 2
            },
            {
               "type" : "com.proto.ch.name",
               "value" : "Acme IP Camera",
               "perms" : [ "PR" ],
               "instanceID" : 3
            },
            {
               "type" : "com.proto.ch.manufacturer",
               "value" : "Acme",
               "perms" : [ "PR" ],
               "instanceID" : 4
            },
            {
               "type" : "com.proto.ch.model",
               "value" : "Q5678",
               "perms" : [ "PR" ],
               "instanceID" : 5
            },
            {
               "type" : "com.proto.ch.serial-number",
               "value" : "9Z8Y7X6W5V4U",
               "perms" : [ "PR" ],
               "instanceID" : 6
            }
         ]
      },
// 繼續下一頁
```

2702

圖27A

// 自前一頁繼續

2700

```
{
   "type" : "com.proto.svc.ip-camera-streaming",
   "instanceID" : 7,
   "characteristics" : [
      {
         "type" : "com.proto.ch.on",
         "value" : true,
         "perms" : [ "PR", "PW" ],
         "instanceID" : 8
      },
      {
         "type" : "com.proto.ch.ip-cam-mgt-session.start",
         "value" : null,
         "perms" : [ "PW" ],
         "instanceID" : 9
      },
      {
         "type" : "com.proto.ch.ip-cam-mgt.session.end",
         "value" : null,
         "perms" : [ "PW" ],
         "instanceID" : 10
      },
      {
         "type" : "com.proto.ch.video.codec.name",
         "value" : "H264",
         "perms" : [ "PR" ],
         "instanceID" : 11
      },
      {
         "type" : "com.proto.ch.video.codec.name",
         "value" : "H264",
         "perms" : [ "PR" ],
         "instanceID" : 11
      },
      {
         "type" : "com.proto.ch.video.codec.parameters",
         "value" : {
            "profile-level-id" : "64001f",
            "packetization-mode" : 0
         }
         "perms" : [ "PR" ],
         "instanceID" : 12
      },
```

2704

// 繼續下一頁

圖27B

2700

// 自前一頁繼續

2704

```
        {
            "type" : "com.proto.ch.video.attributes",
            "value" : {
               "imgattr" : "send [x=1280,y=720]"
            },
            "perms" : [ "PR" ],
            "instanceID" : 13
        },
        {
            "type" : "com.proto.ch.video.payload-type",
            "value" : 99,
            "perms" : [ "PR" ],
            "instanceID" : 14
        },
        {
            "type" : "com.proto.ch.rtp.protocol",
            "value" : "RTP/SAVPF",
            "perms" : [ "PR" ],
            "instanceID" : 15
        },
        {
            "type" : "com.proto.ch.rtp.extensions",
            "value" : [ "tstr", "tmmbr" ],
            "perms" : [ "PR" ],
            "instanceID" : 16
        },
        {
            "type" : "com.proto.ch.srtp.crypto-suite",
            "value" : "AES_256_CM_HMAC_SHA1_80",
            "perms" : [ "PR" ],
            "instanceID" : 17
        }
    ]
},
```

// 繼續下一頁

圖27C

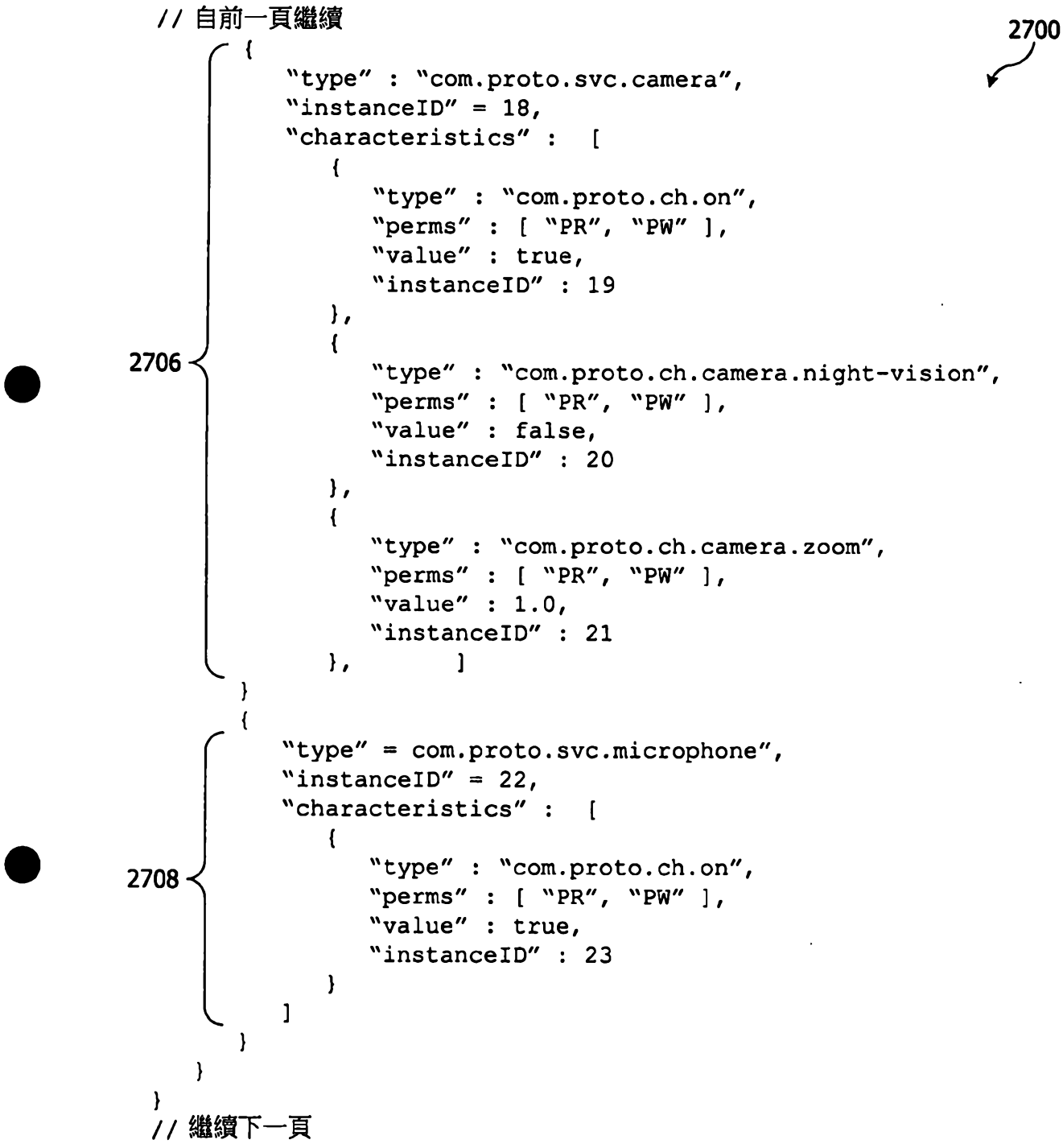

// 自前一頁繼續
2700
{
"type" : "com.proto.svc.camera",
"instanceID" = 18,
"characteristics" : [
{
"type" : "com.proto.ch.on",
"perms" : ["PR", "PW"],
"value" : true,
"instanceID" : 19
},
{
"type" : "com.proto.ch.camera.night-vision",
"perms" : ["PR", "PW"],
"value" : false,
"instanceID" : 20
},
{
"type" : "com.proto.ch.camera.zoom",
"perms" : ["PR", "PW"],
"value" : 1.0,
"instanceID" : 21
},
]
2706
}
{
"type" = com.proto.svc.microphone",
"instanceID" = 22,
"characteristics" : [
{
"type" : "com.proto.ch.on",
"perms" : ["PR", "PW"],
"value" : true,
"instanceID" : 23
}
]
2708
}
}
}
// 繼續下一頁

圖27D


2800
設置配件
2802
控制器探索配件
2804
建立配件與控制器之間的對驗證工作階段
2806
使用控制器為攝影機通電
2808
使用者指示控制器開始串流來自攝影機之視訊
2810
控制器產生並發送開始媒體工作階段請求至配件
2812
配件發送對請求之回應
2814
配件串流媒體至控制器
2816
使用者指示控制器停止串流來自攝影機之媒體
2818
控制器將結束媒體工作階段請求發送至配件
2820
配件發送對請求之回應
2822
配件停止串流媒體至控制器
2824

圖28

```
PUT /characteristics HTTP/1.1
Host: ipcamera.local:12345
Content-Type: application/uap+json                    2900
Content-Length: <length>
{
   "characteristics" : [
     {
       "accessory ID" : 1,
       "instance ID" : 9,                              2904
       "value" : {
          "session-id" : "1DDD2EEE",
          "controller-ip" : 10.0.1.23",
          "controller-port" : 32032,
          "controller-srtp-master-key" : <string1>,
          "controller-srtp-master-salt" : <string2>
       }
     }
   ]
}
```

2902 2906

圖29

```
                                                      3000
HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>
{
     "value" :
          {
          "error-code" : 0,
          "accessory-ip" : 10.0.1.101",
          "accessory-port" : 13000,
          "accessory-srtp-master-key" : <string1>,
          "accessory-srtp-master-salt" : <string2>
          }
}
```

3002 3004

圖30

```
PUT /characteristics HTTP/1.1                                    3100
Host: ipcamera.local:12345
Content-Type: application/uap+json
Content-Length: <length>
{
   "characteristics" : [
     {
       "accessory ID" : 1,
       "instance ID" : 10,                                       3104
       "value" : {
          "session-id" : "1DDD2EEE",
       }
     }
   ]
}
```

3102 3106

圖31

```
                                                                 3200
HTTP/1.1 200 OK
Content-Type: application/uap+json
Content-Length: <length>
{
     "value" :
          {
          "error-code" : 0
          }
}
```

3202

圖32

服務	性質	值
IP串流 3301	類型	com.proto.svc.stream
	特性	com.proto.ch.stream.capability
		com.proto.ch.stream.control.input
		com.proto.ch.stream.control.result

圖33

特性	性質	值
串流能力 3401	類型	com.proto.ch.stream.capabilities
	權限	配對讀取
	資料物件	協定: 1=TCP, 2=UDP 協定資訊: <object>
串流控制輸入 3402	類型	com.proto.ch.stream.control.input
	權限	配對寫入
	資料物件	請求類型: 1=開啟 2=關閉 串流ID: <string> 協定資訊: <object>
串流控制結果 3403	類型	com.proto.ch.stream.control.result
	權限	配對讀取，事件
	資料物件	串流ID: <string> 埠: <integer> 異動ID: <string> 狀態碼: <integer> 協定資訊: <object>

圖34

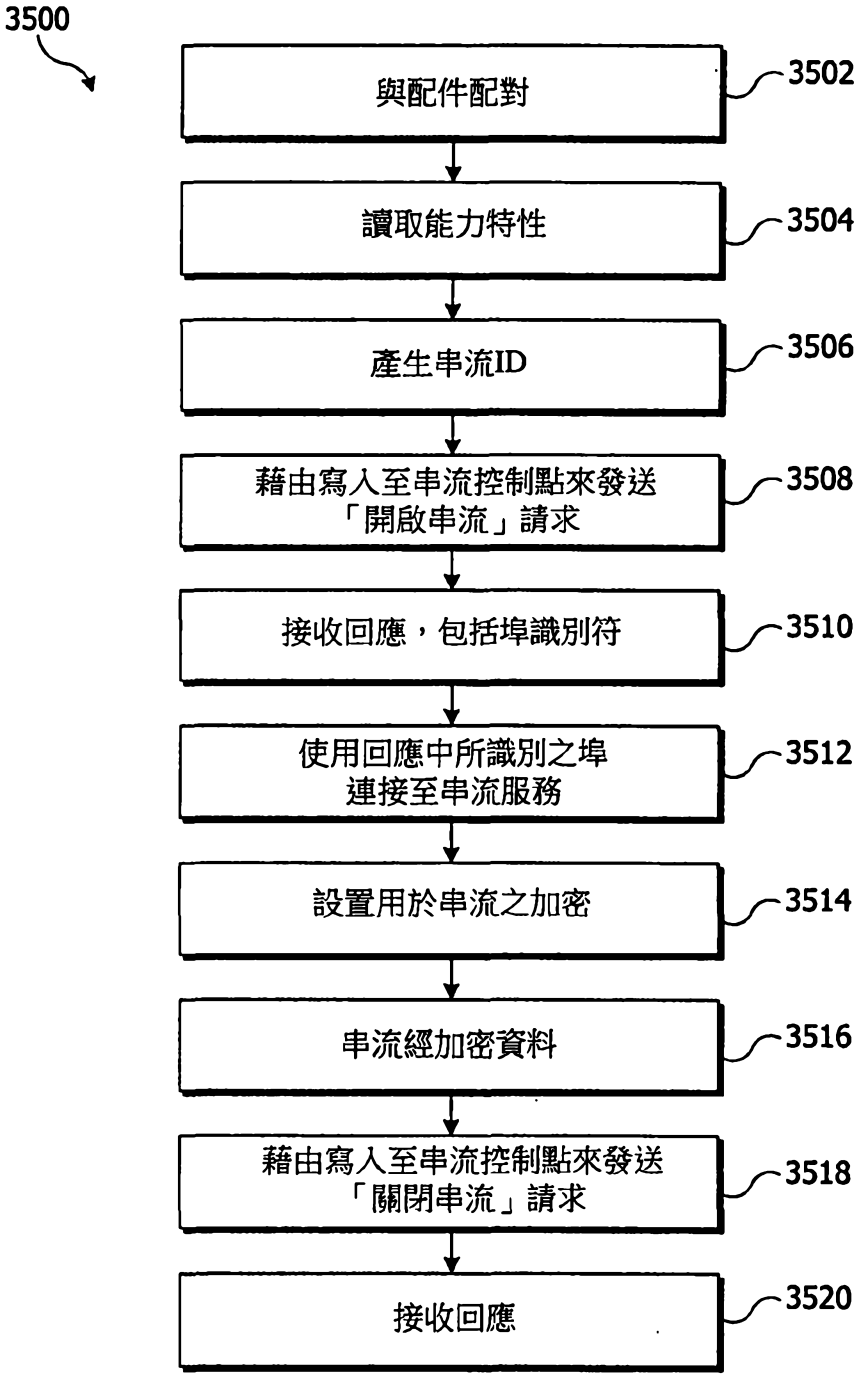

3500
與配件配對
3502
讀取能力特性
3504
產生串流ID
3506
藉由寫入至串流控制點來發送「開啟串流」請求
3508
接收回應，包括埠識別符
3510
使用回應中所識別之埠連接至串流服務
3512
設置用於串流之加密
3514
串流經加密資料
3516
藉由寫入至串流控制點來發送「關閉串流」請求
3518
接收回應
3520

圖35

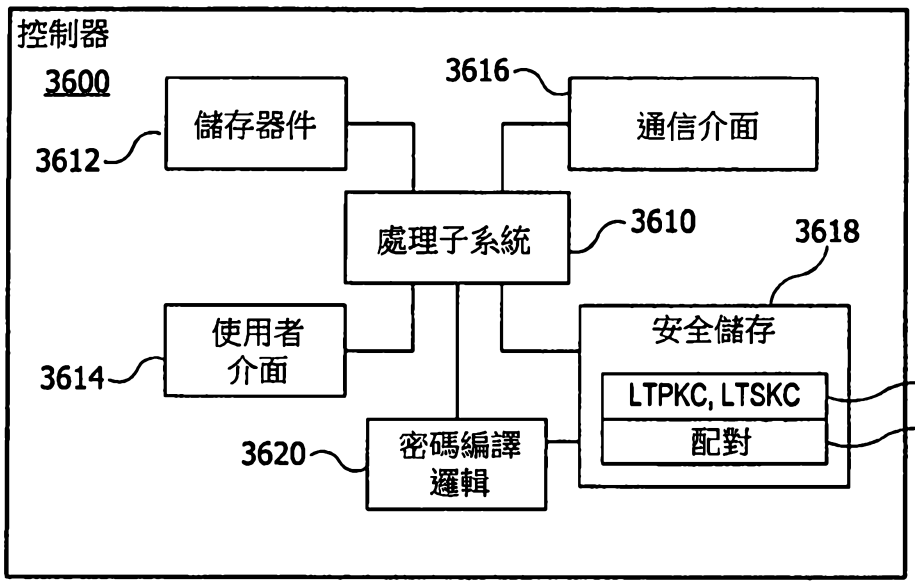

控制器
3600
3612
儲存器件
3616
通信介面
處理子系統
3610
3618
安全儲存
使用者
介面
3614
LTPKC, LTSKC
3622
配對
3624
3620
密碼編譯
邏輯

圖36

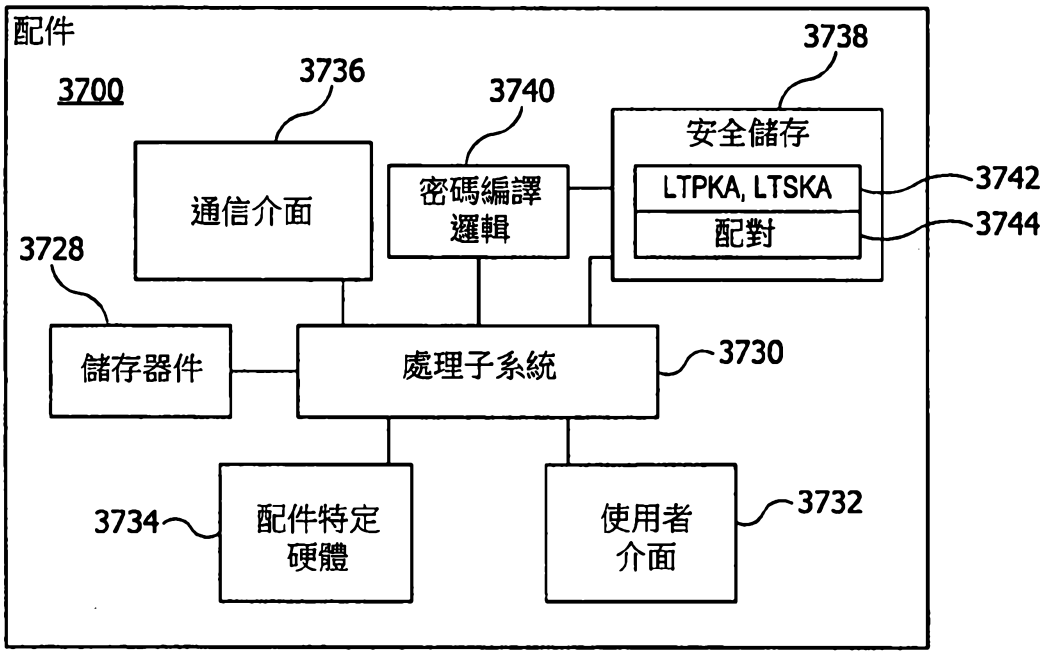

配件
3700
3736
3738
3740
安全儲存
通信介面
密碼編譯
邏輯
LTPKA, LTSKA
3742
配對
3744
3728
儲存器件
處理子系統
3730
3734
配件特定
硬體
使用者
介面
3732

圖37

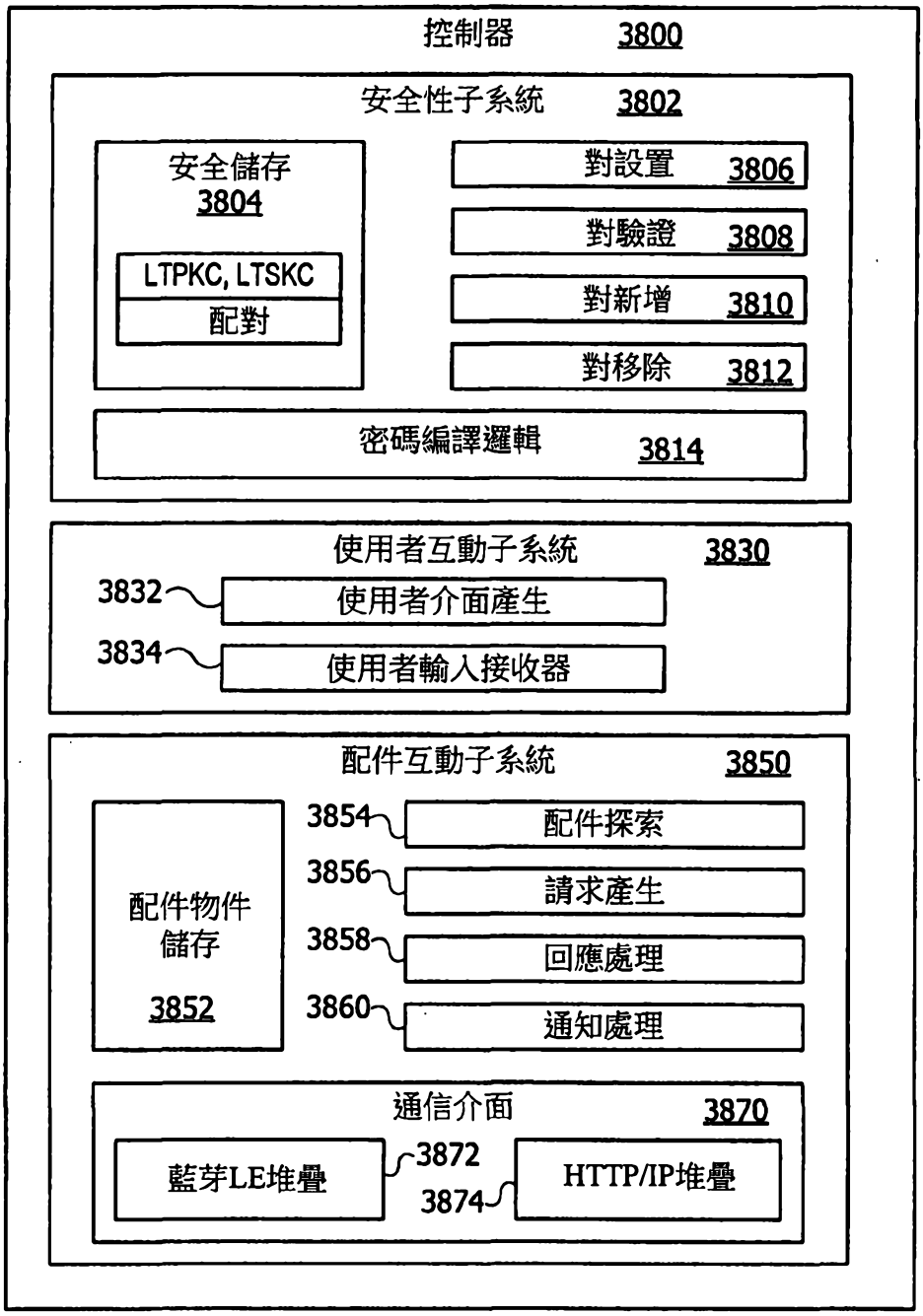

控制器 3800
安全性子系統 3802
安全儲存 3804
LTPKC, LTSKC
配對
對設置 3806
對驗證 3808
對新增 3810
對移除 3812
密碼編譯邏輯 3814
使用者互動子系統 3830
3832
使用者介面產生
3834
使用者輸入接收器
配件互動子系統 3850
配件物件儲存 3852
3854
配件探索
3856
請求產生
3858
回應處理
3860
通知處理
通信介面 3870
藍芽LE堆疊
3872
3874
HTTP/IP堆疊

圖38

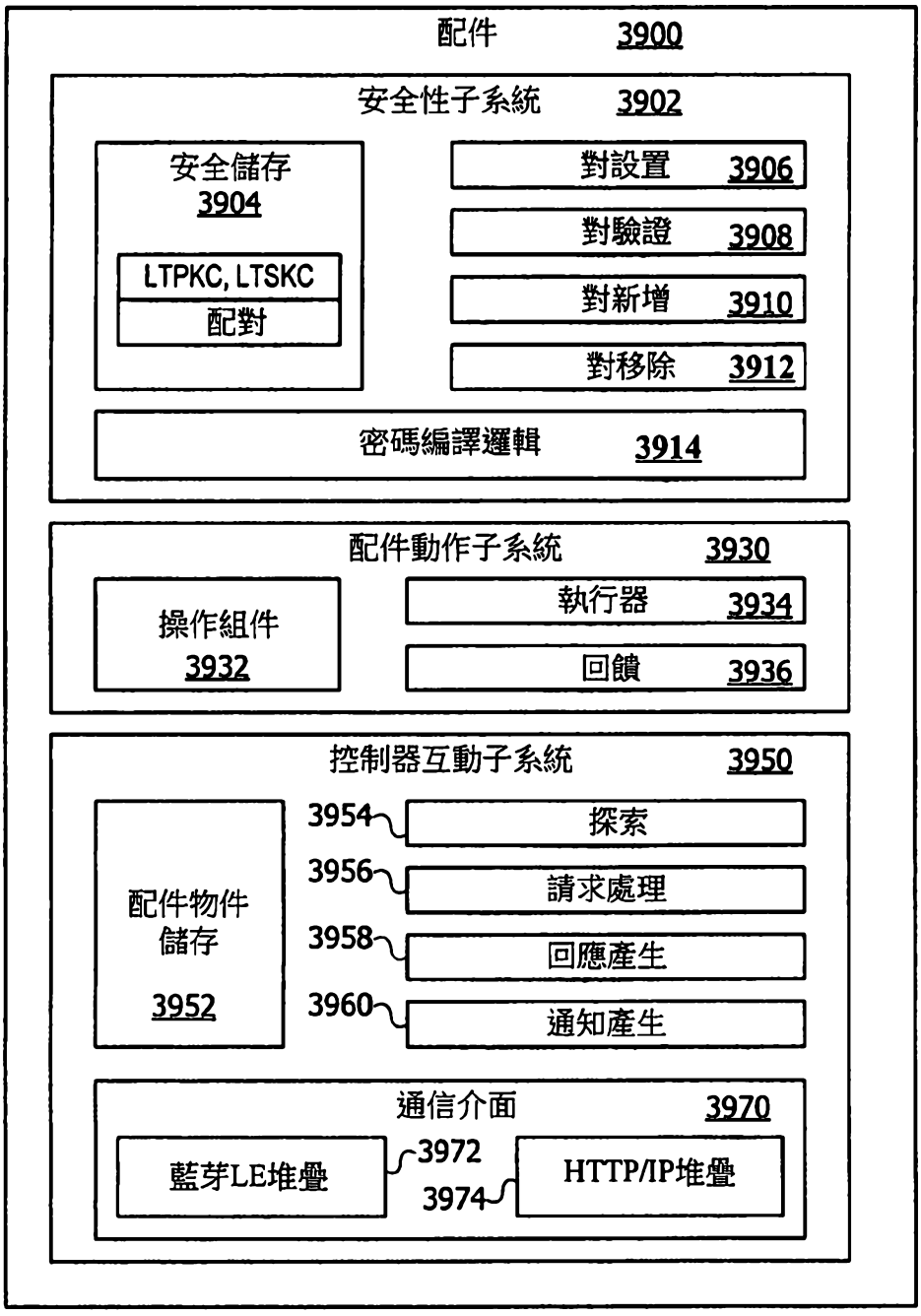

配件 3900
安全性子系統 3902
安全儲存 3904
LTPKC, LTSKC
配對
對設置 3906
對驗證 3908
對新增 3910
對移除 3912
密碼編譯邏輯 3914
配件動作子系統 3930
操作組件 3932
執行器 3934
回饋 3936
控制器互動子系統 3950
配件物件儲存 3952
3954
探索
3956
請求處理
3958
回應產生
3960
通知產生
通信介面 3970
藍芽LE堆疊
3972
3974
HTTP/IP堆疊

圖39

【代表圖】

【本案指定代表圖】：第（4）圖。

【本代表圖之符號簡單說明】：

400　用於藉由控制器來探索配件的程序

402　配件

404　控制器

410　區塊

412　區塊

414　區塊

416　區塊

418　區塊

422　區塊

424　區塊

426　區塊

428　區塊

430　區塊

431　區塊

432　區塊

434　區塊

436　區塊

438　區塊

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

申請專利範圍

1. 一種用於電子器件之間通信的方法，其包含：

藉由一控制器偵測可用於配對之一配件；

藉由該控制器執行一對設置操作以與該配件建立一配對，該對設置操作包括：

使用在該配件與該控制器之間交換的一頻帶外資訊項目建立一共用秘密；

使用該共用秘密來安全地交換該配件之一長期公用金鑰與該控制器之一長期公用金鑰；及

藉由該控制器安全且持久地儲存與該配件之一識別符相關聯的該配件之該長期公用金鑰；

藉由該控制器自該配對配件獲得一配件定義記錄，該配件定義記錄包括一組服務，每一服務具有一組特性，每一特性表示配件狀態之一態樣；及

藉由該控制器將一請求傳達至該配對配件以修改該配件定義記錄中所規定之該等特性中之一或多者，該請求可由該配對配件解譯為用以調用該配對配件之一操作之一指令。

2. 如請求項1之方法，其進一步包含，在調用該配件之該操作之前：

藉由該控制器執行關於該配對配件之一對驗證操作，該對驗證操作包括：

將該控制器具有該配對配件之該長期公用金鑰之一證明及對應於該控制器之該長期公用金鑰之一長期秘密金鑰發送至該配對配件；及

自該配對配件接收該配對配件具有該控制器之該長期公用金鑰之一證明及對應於該配對配件之該長期公用金鑰之一長

期秘密金鑰，

其中該控制器僅在該對驗證操作成功之情況下調用該配對配件之該操作。

3. 如請求項2之方法，其中執行該對驗證操作進一步包括：產生一工作階段金鑰，且其中該工作階段金鑰係用以加密該請求以修改該配件定義記錄中所規定之該特性中之一或多者。

4. 如請求項1之方法，其進一步包含：

藉由該控制器將一請求發送至該配對配件以訂用來自定義於該配件定義記錄中之該組特性之一特定特性之一改變的通知，其中該訂用請求規定該特定特性且進一步規定一通知模式。

5. 如請求項4之方法，其中該規定通知模式為一事件訊息通知模式，該方法進一步包含：

在發送該訂用請求之後，藉由該控制器自該配件接收一非請求型回應訊息，該非請求型回應訊息包括由該控制器規定之該特性之一改變之一通知。

6. 如請求項1之方法，其中該頻帶外資訊項目包括以下各者中之一或多者：

由該配件提供至一使用者及由該使用者提供至該控制器之一設置碼；或

藉由該控制器自除該配件以外之一源獲得之數位憑證驗證資訊，該數位憑證驗證資訊可用以驗證由該控制器自該配件接收之一數位憑證及簽章。

7. 如請求項1之方法，其進一步包含：

藉由該控制器執行代表另一控制器的關於該配對配件之一對新增操作，其中該對新增操作包括藉由該控制器將該另一控制器之一長期公用金鑰或可由該配件使用以驗證該另一控制器之一

憑證中之一者或兩者提供至該配件。

8. 一種控制器，其包含：

用以與一或多個配件通信之一通信介面；

用以安全地儲存用於一或多個配對配件之配對記錄之一安全儲存元件；

經組態以儲存用於一或多個配對配件之配件定義記錄之一資料儲存元件；及

耦接至該通信介面、該安全儲存元件及該資料儲存元件之一處理子系統，該處理子系統經組態以：

與一或多個配件建立一配對，其中與一配件建立一配對包括：

獲得一頻帶外資訊項目；

自該配件安全地獲得該配件之一長期公用金鑰及該配件具有該頻帶外資訊項目之一證明；

將該控制器之一長期公用金鑰安全地提供至該配件；及

建立用於該配件之一配對記錄且將該配對記錄持久地儲存於該安全儲存元件中，該配對記錄包括該配件之一長期公用金鑰；

在與一配件建立一配對之後，自該配對配件獲得一配件定義記錄，該配件定義記錄包括一組服務，每一服務具有一組特性，每一特性表示配件狀態之一態樣；及

藉由將一請求傳達至該配件以修改該配件定義記錄中所規定之該等特性中之一或多者來調用該配對配件之一操作。

9. 如請求項8之控制器，其中該通信介面包括至少兩個不同傳輸協定堆疊，且其中該通信介面選擇該等傳輸協定堆疊中之一者以用於與一特定配件通信。

10. 如請求項9之控制器，其中該至少兩個不同傳輸協定堆疊包括一藍芽LE協定堆疊及一HTTP/IP協定堆疊。

11. 如請求項8之控制器，其中該處理子系統經進一步組態以與一配對配件建立一對驗證工作階段，其中建立該對驗證工作階段包括：

將該控制器具有該配對配件之該長期公用金鑰之一證明及對應於該控制器之該長期公用金鑰之一長期秘密金鑰發送至該配對配件；

自該配對配件接收該配對配件具有該控制器之該長期公用金鑰之一證明及對應於該配對配件之該安全儲存的長期公用金鑰之一長期秘密金鑰；及

建立可用以加密在該控制器與該配對配件之間交換的後續訊息之一或多個工作階段金鑰。

12. 如請求項11之控制器，其中該處理子系統經進一步組態以在一已建立之對驗證工作階段內執行一對新增操作，其中執行該對新增操作包括將另一控制器之一長期公用金鑰發送至該配對配件，該配對配件將與該另一控制器建立一配對。

13. 一種用於電子器件之間通信的方法，其包含：

藉由一配件廣告該配件可用於配對；

藉由該配件執行一對設置操作以與一控制器建立一配對，該對設置操作包括：

使用在該配件與該控制器之間交換的一頻帶外資訊項目建立一共用秘密；

使用該共用秘密來安全地交換該配件之一長期公用金鑰與該控制器之一長期公用金鑰；及

藉由該配件安全且持久地儲存與該控制器之一識別符相關

聯的該控制器之該長期公用金鑰；

藉由該配件將用於該配對配件之一配件定義記錄提供至該配對控制器，該配件定義記錄包括一組服務，每一服務具有一組特性，每一特性對應於配件狀態之一態樣；

藉由該配件自該配對控制器接收一請求以修改該配件定義記錄中所規定之該等特性中之一或多者；及

藉由該配件回應於該接收之請求而執行一調用操作。

14. 如請求項13之方法，其進一步包含：

在該配件處偵測指示該配件應進入一配對模式之一使用者動作，

其中廣告該配件可用於配對係回應於偵測該使用者動作而執行。

15. 如請求項13之方法，其中，在執行關於一個控制器之該對設置操作之後，該配件隨後拒絕執行關於任何其他控制器之該對設置操作，只要該配對控制器之該長期公用金鑰保持安全且持久地儲存即可。

16. 如請求項13之方法，其進一步包含，在自該控制器接收該請求以修改該等特性中之一或多者之前：

藉由該配件執行關於該配對控制器之一對驗證操作，該對驗證操作包括：

自該配對控制器接收該配對控制器具有該配件之該長期公用金鑰之一證明及對應於該配對控制器之該長期公用金鑰之一長期秘密金鑰；及

將該配件具有該配對控制器之該長期公用金鑰之一證明及對應於該配件之該長期公用金鑰之一長期秘密金鑰發送至該配對控制器，

其中該配件僅在該對驗證操作成功之情況下回應於該請求而執行該調用操作。

17. 如請求項16之方法，其中執行該對驗證操作進一步包括：產生一工作階段金鑰，且其中該工作階段金鑰係用以解密該接收之請求以修改該配件定義記錄中所規定之該特性中之一或多者，

其中該配件僅在該接收之請求經成功解密之情況下執行該調用操作。

18. 如請求項13之方法，其進一步包含：

藉由該配件自一配對控制器接收一請求以訂用來自定義於該配件定義記錄中之該組特性之一特定特性之一改變的通知，其中該訂用請求規定該特定特性且進一步規定一通知模式；及

在該規定特性改變之情況下，藉由該配件基於該規定通知模式而產生用於該配對控制器之一更新通知。

19. 如請求項18之方法，其中該規定通知模式為一事件訊息通知模式，且其中產生該更新包括將一非請求型回應訊息發送至該配對控制器，該非請求型回應訊息包括該規定特性之該改變之一通知。

20. 如請求項13之方法，其中該頻帶外資訊項目包括一設置碼，該設置碼由該配件儲存於本機且使用一頻帶外通信頻道傳達至該控制器。

21. 如請求項13之方法，其進一步包含：

藉由該配件執行代表另一控制器的關於該配對控制器之一對新增操作，其中該對新增操作包括：

藉由該配件自該配對控制器接收該另一控制器之一長期公用金鑰；及

藉由該配件安全且持久地儲存與該另一控制器之一識別符

相關聯的該另一控制器之該長期公用金鑰，

其中，在該對新增操作之後，該另一控制器被該配件視為一第二配對控制器。

22. 一種用於電子器件之間通信的配件，其包含：

一通信介面，其用以與一或多個控制器通信；

一操作組件；

一安全儲存元件，其用以安全地儲存配對記錄；

一配件資料儲存元件，其經組態以儲存一配件定義記錄，該配件定義記錄包括一組服務，每一服務具有一組特性，每一特性表示包括該操作組件之一狀態之配件狀態之一態樣；及

一處理子系統，其耦接至該通信介面、該操作組件、該安全儲存元件及該配件資料儲存元件，該處理子系統經組態以：

與一或多個控制器建立一配對，其中與一控制器建立一配對包括：

獲得一頻帶外資訊項目；

自該控制器安全地獲得該控制器之一長期公用金鑰及該控制器具有該頻帶外資訊項目之一證明；

將該配件之一長期公用金鑰安全地提供至該控制器；及

建立用於該控制器之一配對記錄且將該配對記錄持久地儲存於該安全儲存元件中，該配對記錄包括該控制器之一長期公用金鑰；

在與一控制器建立一配對之後，將該儲存之配件定義記錄提供至該配對控制器；及

自該配對控制器接收一請求以修改該配件定義記錄中所規定之該等特性中之一或多者；及

回應於該請求而實現該至少一個操作組件之一操作。

23. 如請求項22之配件，其中該處理子系統經進一步組態以與一配對控制器建立一對驗證工作階段，其中建立該對驗證工作階段包括：

自該配對控制器接收該配對控制器具有該配件之該長期公用金鑰之一證明及對應於該配對控制器之該安全儲存的長期公用金鑰之一長期秘密金鑰；

將該配件具有該配對控制器之該長期公用金鑰之一證明及對應於該配件之該長期公用金鑰之一長期秘密金鑰發送至該配對控制器；及

建立可用以加密在該配對控制器與該配件之間交換的後續訊息之一或多個工作階段金鑰。

24. 如請求項23之配件，其中該處理子系統經進一步組態以在一已建立之對驗證工作階段內執行一對新增操作，其中執行該對新增操作包括：

自該配對控制器接收另一控制器之一長期公用金鑰，該配件將與該另一控制器建立一配對；及

建立用於該另一控制器之一配對記錄且將該配對記錄持久地儲存於該安全儲存元件中，該配對記錄包括該另一控制器之該接收之長期公用金鑰。

25. 如請求項22之配件，其中該至少一個操作組件包括以下各者中之一或多者：

一鎖機構；

一燈泡；

一開門器；或

一攝影機。