



(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 I536285 B

(45)公告日：中華民國 105 (2016) 年 06 月 01 日

(21)申請案號：100139923

(22)申請日：中華民國 100 (2011) 年 11 月 02 日

(51)Int. Cl. : G06Q10/00 (2012.01)

G06F9/44 (2006.01)

G06F21/00 (2013.01)

H04L9/28 (2006.01)

(30)優先權：2010/11/04 美國

12/939,702

(71)申請人：銀泉網路公司 (美國) SILVER SPRING NETWORKS, INC. (US)

美國

(72)發明人：維斯瓦尼 瑞傑 VASWANI, RAJ (US)；楊俊耀 YEUNG, WILSON CHUEN YEOW (CA)；賽伯特 克莉絲堤娜 SEIBERT, CRISTINA (US)；波葉爾德 尼爾森 布魯斯 BOLYARD, NELSON BRUCE (US)；丹姆 班哲明 N DAMM, BENJAMIN N. (CA)；聖約翰 麥可 C STJOHNS, MICHAEL C. (US)

(74)代理人：閻啟泰；林景郁

(56)參考文獻：

TW 552757

CN 201118607Y

US 5943656

US 2005/0144437A1

US 2006/0125421A1

審查人員：沈佳瑾

申請專利範圍項數：45 項 圖式數：8 共 40 頁

(54)名稱

用於公共事業應用程式之實體安全授權的控制方法，及用於公共事業網路的認證系統

CONTROLLING METHOD OF PHYSICALLY SECURED AUTHORIZATION FOR UTILITY APPLICATIONS, AND AUTHENTICATION SYSTEM FOR UTILITY NETWORK

(57)摘要

為了對一個公共事業管理系統提供整體安全性，對此系統之多個構件所發出的關鍵命令和控制信息係明確地由一個保全權限機構進行核准。此明確核准係認證所請求行動且授權在一個信息中所指示之具體指定行動的實行。與存取控制相關聯之公共事業管理和控制系統的金鑰構件係被置放在一個實體掩體件中。藉著此方式，變得僅需要將對於負責核准多個網路行動之多個子系統進行掩護。其它的管理模組係能保持在該掩體件外側，藉此避開予以劃分成經掩護構件和非經掩護構件的需要。對於非經掩護子系統中各者之多個關鍵構件的存取係透過經掩護核准系統的控制。

To provide overall security to a utility management system, critical command and control messages that are issued to components of the system are explicitly approved by a secure authority. The explicit approval authenticates the requested action and authorizes the performance of the specific action indicated in a message. Key components of the utility management and control system that are associated with access control are placed in a physical bunker. With this approach, it only becomes necessary to bunker those subsystems that are responsible for approving network actions. Other management modules can remain outside the bunker, thereby avoiding the need to partition them into bunkered and non-bunkered components. Access to critical components of each of the non-bunkered subsystems is controlled through the bunkered approval system.

指定代表圖：

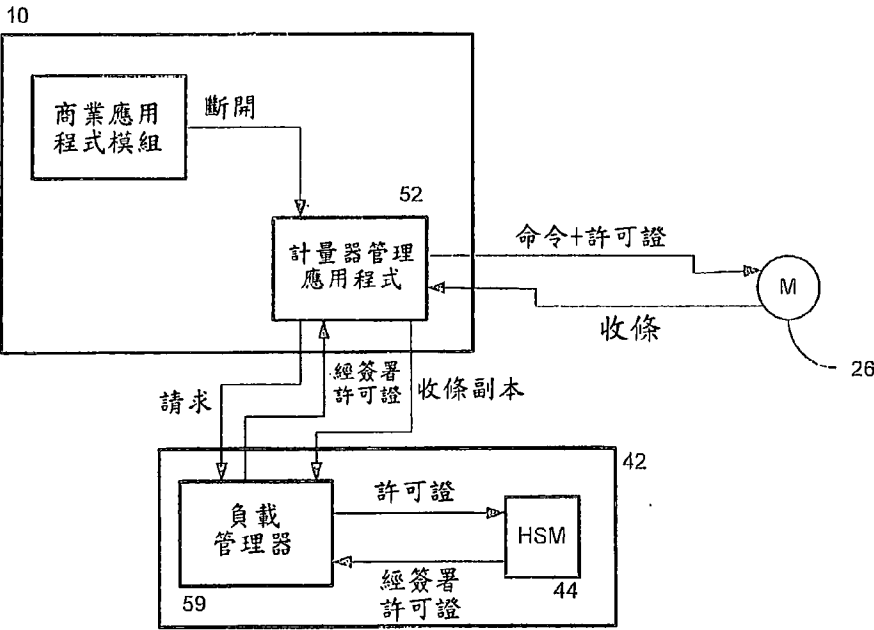


圖6

符號簡單說明：

- 10 . . . 後端支援部門
- 26 . . . 計量器/(末端)節點
- 42 . . . 實體掩體件
- 44 . . . 硬體安全性模組(HSM)
- 52 . . . 計量器管理應用程式
- 59 . . . 負載管理器(模組)

發明專利說明書

公告本

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：100139923

※ 申請日：100.11.2

※IPC 分類：G060 10/00 (2012.01)

G06F 9/44 (2006.01)

一、發明名稱：(中文/英文)

G06F 21/00 (2013.01)

H04L 9/28 (2006.01)

用於公共事業應用程式之實體安全授權的控制方法，及用於
公共事業網路的認證系統

CONTROLLING METHOD OF PHYSICALLY SECURED
AUTHORIZATION FOR UTILITY APPLICATIONS, AND
AUTHENTICATION SYSTEM FOR UTILITY NETWORK

二、中文發明摘要：

為了對一個公共事業管理系統提供整體安全性，對此系統之多個構件所發出的關鍵命令和控制信息係明確地由一個保全權限機構進行核准。此明確核准係認證所請求行動且授權在一個信息中所指示之具體指定行動的實行。與存取控制相關聯之公共事業管理和控制系統的金鑰構件係被置放在一個實體掩體件中。藉著此方式，變得僅需要將對於負責核准多個網路行動之多個子系統進行掩護。其它的管理模組係能保持在該掩體件外側，藉此避開予以劃分成經掩護構件和非經掩護構件的需要。對於非經掩護子系統中各者之多個關鍵構件的存取係透過經掩護核准系統的控制。

三、英文發明摘要：

To provide overall security to a utility management system, critical command and control messages that are issued to components of the system are explicitly approved by a secure authority. The explicit approval authenticates the requested action and authorizes the performance of the specific action indicated in a message. Key components of the utility management and control system that are associated with access control are placed in a physical bunker. With this approach, it only becomes necessary to bunker those subsystems that are responsible for approving network actions. Other management modules can remain outside the bunker, thereby avoiding the need to partition them into bunkered and non-bunkered components. Access to critical components of each of the non-bunkered subsystems is controlled through the bunkered approval system.

四、指定代表圖：

(一)本案指定代表圖為：圖 6。

(二)本代表圖之元件符號簡單說明：

10：後端支援部門

26：計量器 / (末端) 節點

42：實體掩體件

44：硬體安全性模組 (HSM)

52：計量器管理應用程式

59：負載管理器 (模組)

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

六、發明說明：

【發明所屬之技術領域】

此揭示內容係關於與多個公共事業營運公司相關聯之操作的管理和控制，且更特別是關於用以管理和控制此等操作之系統的安全性。

【先前技術】

公共事業營運公司係具有複雜且高度互連的系統，其係在用以運作一群相關軟體模組以供管理且控制此公共事業營運公司之多個操作的實體伺服器上作執行。圖 1 係可以在用於一個公共事業營運公司之一個典型管理和控制系統中所發現構件中的一些構件之一個通用方塊圖，該公共事業營運公司係對多個客戶供應電力，和諸如天然氣、用水等可行的其他商品。此系統之後端支援部門 10 係包括數個與此公共事業之各種操作相關聯的各別子系統，例如一個客戶資訊系統 (CIS) 12、一個客戶關係模組 (CRM) 14、一個服務中斷管理系統 (OMS) 16、一個 GPS 資訊系統 18、一個計費系統 20、一個電網穩定模組 22、和一個使用者介面 24。儘管並非如圖 1 所例示，額外的功能性模組係能出現在該後端支援部門 10 中。該些子系統中的一些子系統係可具有與分佈式網路中之多個裝置進行通訊的能力，以用於所供應的商品和與該些裝置相關聯之遠端控制操作。例如：此後端支援伺服器係可與位於客戶住處之個別計量器 26 進行通訊，以取得用於計費目的之消耗資料且命令該等

計量器將該客戶斷開自/將該客戶重新連接至由該公共事業營運公司所提供之一個或更多商品的供應。從該後端支援伺服器到個別計量器之其它命令係可包含用以接收來自該等客戶之外送能量流的命令。

在圖 1 之實例中，該等計量器係組成用以經由一個區域網路 30 與該後端支援部門進行通訊之多個末端節點，該區域網路 30 係具有用以對進出此網路提供出口之多個存取點 32。該等存取點 32 係經由一個廣域網路 34 或一個專用通訊鏈路以與該後端支援部門 10 之多個伺服器進行通訊。

在此類型之一個系統中，憂慮的一個議題係遠端斷開和重新連接之保全管理，其可能分別發生在一個客戶搬離一個住處或拖欠款項的時候、或者是發生在一個新客戶佔有此住處的時候。所惡意及/或錯誤發送之命令以在遠端斷開及/或重新連接住處係可具有使電力分佈網格不穩定的可能性。未經授權之重新連接同樣可能造成分散式電力的竊取。為限制此等可能性，必須致力於確保命令和多個控制操作以一個安全方式且僅藉由經過授權以從事此等操作之實體所發生。然而，因為一個典型公共事業之後端支援部門是由各種互連系統所組成，所以一個保全存取之強制執行係變為困難。在此公共事業內之許多不同群組係需要存取所有或是部份的軟體系統，其係使用以限制邏輯及/或實體存取個別子系統的能力複雜化。

對此議題之一個可行解決方案係將某些系統或此等系統之部分置放在一個實體安全環境（在本文中稱為一個掩

體件)內。一個掩體件之多個實例係包含一個限制存取的空間或容器(例如:一個上鎖空間)、和圍繞一個經保護系統之一個防竄改殼體或圍體。該掩體件係嚴格地限制對該等系統或該等系統之保護部分所執行的硬體裝置進行存取。此外,在該掩體件內之系統係輸出非常有限的邏輯存取。然而,此解決方案係仍然呈現一個挑戰性問題,其在於對公共事業之軟體系統進行重構(refactor)以決定那些部分需要在該掩體件內而那些部分則能保持在該掩體件外側以對需要的部分提供更有彈性之存取係有其困難性。

【發明內容】

為了對一個公共事業管理系統提供整體安全性,對此系統之多個構件所發出的關鍵命令和控制信息係必須明確地由一個保全權限機構所核准。此明確核准係認證所請求行動且授權在一個信息中所指示之具體指定行動的實行。與存取控制相關聯之公共事業管理和控制系統的金鑰構件係被置放在一個實體安全性環境中。藉著此方式,變得僅需要將對於負責核准多個網路行動之多個子系統進行實體保全,例如經由一個掩體件。換言之,諸如該客戶資訊系統、該客戶關係模組、該服務中斷管理系統、該計費系統等之大部分的管理模組係能保持在該掩體件外側,藉此避開將該些子系統劃分成經掩護構件和非經掩護構件的需要。對於非經掩護子系統中各者之多個關鍵構件的存取係透過經掩護核准系統的控制。

【實施方式】

為促進對本發明所基於多個原理的了解，茲在後文中參考在一個電力分佈式系統中之遠端連接和斷開命令的安全性控制作出敘述。然而將理解到：此一實例並非僅僅是該些原理之實際應用。反之，該些原理係能搭配任何類型之關鍵命令來運用，此關鍵命令假如被不當或錯誤地發出則可能具有嚴重干擾或損壞一個系統的可能性。同樣，該些原理係併同所發送至在所有時間下適當運作為重要之系統的一個關鍵構件之所有命令和控制信息來使用。

圖 2 係例示其中實施有本發明多個觀念之一個資料中心 40 的一個實例。傳統上，該資料中心係含有數個上執行各種應用程式 12、14、16 之實體伺服器。儘管在圖式中僅僅例示些許代表性的應用程式，然而將理解到：大量的此等應用程式係能被實施在該資料中心內。反過來說，由該等應用程式中之兩者或更多所實行之功能係可被整合成一個單一且詳盡的程式。

同樣定位於該資料中心內的是一個實體掩體件 42，其係具有有限的實體存取，諸如具有鋼筋牆之一個上鎖空間。作為另一個實例，除了或是取代上鎖，該掩體件可以是一個使用多部保全攝像機、運動偵測器等而受到嚴密看管或保護之區域。作為另一個實例，該掩體件係可在實體上被分佈，而安全性關係業已建立在多個經分佈部件之間。作為另一個實例，該掩體件係可在邏輯上受到保全，諸如藉由安全地使用執行軟體及/或韌體，其功能性係保全

而免除諸如實體竄改之自毀性封裝。該掩體件並非必定是一個空間，不過例如可以是一個實體保全隔間。

具有一個相關的硬體安全性模組 44 之一個或更多額外伺服器係定位於該掩體件內以用於實施一個授權引擎 46，其係具有用以實行諸如授權、認證和稽核之安全性相關操作的軟體模組。該硬體安全性模組係含有用以鏈結到多個私人金鑰之公開憑證。該硬體安全性模組較佳係使用一個強固安全性演算法以實行多個密碼編譯操作，諸如橢圓曲線密碼學或另一具高度安全之密碼編譯方法。多個硬體安全性模組中適合用於本文中所述之多個應用程式的一個實例係來自德國公司 Utimaco Safeware 之產品線 SafeGuard CryptoServer 的硬體安全性模組。

對於該掩體件或者是對位在該掩體件內之多個伺服器裝置的存取係能以生物感測器技術所強化，例如指紋偵測、實體金鑰或符記及/或密碼防護。在一個實施例中，一個具有階層之分層安全性系統係能被運用以最大化防護。假如一個分層的安全性無效（例如：密碼意外地被洩漏或遭到偷竊），則諸如一個金鑰或符記所致動之多段式門栓鎖之一個較高層級的安全性機制係能被啟動以維持整體系統的實體安全性。

來自非經掩護後端支援應用程式 12 到 16 等之某些類型的命令係受到約束，使得除非各自得到授權否則將不予執行。例如：遠端斷開和重新連接命令係該些受約束命令之一個範疇，其在於對電力分佈網格之穩定性存在嚴重干

擾的可能性。為強制執行關於該些類型之操作的安全性，落實該些操作之應用程式係可僅僅在源自於該掩體件 42 內之一個控制台或另外受到自該掩體件 42 內所發出之一允許所授權時接受多個命令而加以進行。因此，僅僅在具有權限以發出該些命令和擁有諸如密碼、金鑰、指紋等之用於對該掩體件進行存取的必要手段之人員係將能夠對該應用程式發出該等受約束命令。

當初使化一操作而引起一個命令的產生時，可以藉由該授權引擎 46 進行簽署或另外授權，且接著被轉送到與該掩體件 42 外部之適當應用程式相關聯的一個應用程式設計介面（API）。例如：該命令係可由儲存在該硬體安全性模組 44 內之一個私人金鑰進行簽署。一旦在一個外部應用程式處收到經簽署命令（例如：該等應用程式 12 到 16 中之一個應用程式或在該等計量器 26 中的一個計量器所運行之一個應用程式），則經由該應用程式存取之一個公開金鑰進行驗證。一旦經驗證為源自於該掩體件內，則該命令係由該外部應用程式加以執行。

在一些情況中，由一個實體發出實體上將存在於該掩體件內之遠端斷開命令可能不實際。假如支援此命令之遠端產生，然而此等命令係能由冒充經授權實體之使用者所惡意地發出。為限制此等發生的可能性，依據本發明之一個決策模組 48 係被實施於該掩體件內。該決策模組如圖 2 所描述係可為一個分開的軟體或韌體構件，或者邏輯上如下文所述係可被納入該硬體安全性模組內。該決策模組 48

係以一個安全方式進行重新組態或重新程式規劃，諸如藉由自該掩體件內部所輸入之命令。此模組係含有用以檢驗一個經請求行動且決定是否允許被落實的商業邏輯。例如：假如依照可能干擾該電力分佈網格之穩定性的一個順序或相對時序來發出重新連接命令，此等命令係能被決策所阻隔且不會被傳遞到該授權引擎進行簽署。此外，當偵測到前述狀況時，決策旗標係能被升起且採取適當行動，諸如斷開發出命令之一個實體。例如，該些狀況係能包含：

1. 一次（例如：在一個預定時間間隔內）發出大量的遠端斷開命令，用以指出惡意地將多個此使用者自該電力分佈網格斷開的一個可能意圖；

2. 以一個可疑次序所發出的命令，諸如：與同一客戶相關聯之一系列重複的斷開和重新連接命令，或者是與一個用戶之當前狀態不一致的命令，例如：對已經沒有連接到電力網格之一個使用者發出一個斷開命令；

3. 一個請求應用程式無法提供必要的憑據或者是另外得到授權；

4. 一個請求應用程式不在一組具有許可以發出某些操作之經核准應用程式中；以及

5. 分佈網路的狀態，其係基於實際的功率負載和預計規劃的功率需求。

為實施此功能性，該掩體件係可含有用於其外部之多個應用程式的應用程式設計介面（API）之一個代理伺服器50。操作上，當對該些「外部」應用程式中一個應用程式

的應用程式設計介面作出一個呼叫時，該呼叫係被導引到該掩體件內之代理伺服器 50。該代理伺服器係對該決策模組 48 中的公共事業商業邏輯作諮詢而可能需要授權此請求，且具有由適當商業邏輯所簽署之請求。該請求接著被傳遞到該授權引擎 46 以進行簽署。一但經過授權，該代理伺服器係調用處在該掩體件外部之經呼叫應用程式的常規應用程式設計介面，且傳遞經授權呼叫。

在一個替代性實施方式中，該掩體件 142 係可不包含一個代理伺服器。在此案例中，一個請求係可直接對一個外部應用程式之應用程式設計介面作出。依此，該外部應用程式係呼叫該掩體件內之授權引擎，以決定經請求操作是否需要一個簽章。作為一個預設條件，所有請求係能被傳遞到該掩體件內以進行授權，而避免由該外部應用程式作任何決定的需要。提交給該掩體件之請求首先係經過該決策模組加以檢驗和簽署，且接著被傳遞到該授權引擎 46。一旦一個請求得到授權，則經呼叫應用程式係根據該請求進行動作。

被包含在該掩體件 42 中之硬體安全性模組 44 係能以兩個層級來操作。後文實例係搭配在該等計量器 26 處所實行之操作進行敘述。於第一操作層級處，該公共事業營運公司係可設立一個決策，使在後端支援部門處的一個應用程式和一個計量器 26 或是該區域網路 30 的任何其他構件之間的所有通訊必須予以加密和簽署。此決策之實施方式係被描述在圖 3 的實例中。在此實例中，一個計量器管理

應用程式 52 係使例如一個命令之一個信息發送到該等計量器 26 中的一者或更多。此信息係被係建構在此應用程式之一個計量器命令和介面模組 54 中，且被轉送到該掩體件 42 中的硬體安全性模組 44，該信息係具有一個請求以實行本身適當的加密和簽署。該決策模組 48 首先係可進行檢驗以證實該請求源自於一個經授權來源。若是如此，則予以傳遞到該硬體安全性模組。該硬體安全性模組 44 係使用與該應用程式相關聯之適當金鑰以在該信息上實行所請求的操作，且回傳經加密且簽署的資料。該計量器管理應用程式 52 之命令和介面模組 54 接著係產生一個合併有經加密且簽署信息之資料封包，且經由該網路 30 予以傳送到該計量器。

對於由該應用程式 52 自該網路中之節點所接收的信息來說，該等信息首先係被轉送到該硬體安全性模組以進行解密。此模組 48 係亦能對所接收信息之發送端的真實性和資料的整體性實行適當驗證。經驗證且解密的信息接著係被回傳到該應用程式 52。

對於諸如遠端連接和斷開之關鍵操作來說，該硬體安全性模組係能以一個第二層級進行操作以強化在此等操作上的一個速率限制。圖 4 係描述一個硬體安全性模組之內部組態配置的一個實例。此模組係以數個分槽進行組態。各個分槽係含有私人金鑰、憑證、機密金鑰和存取特權之一個集合，以實行諸如簽署、加密、解密等之密碼編譯服務。不同的分槽係關聯於不同的安全性背景，且含有與其各自背景相關之金鑰、憑證和其它資訊。藉由該硬體安全

性模組在一個命令上實行一個密碼編譯服務（諸如以一個私人金鑰對該命令進行簽署）係使該命令的接收端（例如；一個節點 26）能夠使用一個相關聯的公開金鑰以認證該命令之來源。該決策模組 48 係作出一個經請求命令是否允許被呈現到該硬體安全性模組以進行一個或更多密碼編譯服務的初步裁定。

各個分槽係能以一個或更多速率限制而選擇性地進行組態（例如經由一個命令行系統管理工具），以強化所欲的商業邏輯。對一個分槽進行組態之一個命令的一個實例係如下述：

```
HSM_configure slot=2 rate-name="rate1" window=24h
count=10000
```

此一命令以每 24 小時滑動視窗具有 10000 密碼編譯操作之一個最大速率限制對分槽 2 進行組態。假如在先前 24 小時內出現超此密碼編譯操作之分配數量，則該分槽係停止所有進一步的密碼編譯操作。其後，一位系統管理者係將需要藉由發送一個重設命令來重設該分槽。

一個分槽係能以超過一個之速率進行組態，其如下述：

```
HSM_configure slot=2 rate-name="rate1" window=
24h count=40000
```

```
HSM_configure slot=2 rate-name="rate2" window=
60m count=2000
```

該些兩個命令係以兩個速率限制視窗對分槽 2 進行組態：其中一個是在一個 24 小時滑動視窗上具有 40000 個密

碼編譯操作，而另一個則是在一個 60 分鐘滑動視窗上具有 2000 個密碼編譯操作。

假如以一個速率限制對一個分槽進行組態，則在該分槽中所執行之所有密碼編譯操作係在一個滑動視窗上相對經分配限制加以計數。在上文所給定實例中，假如在過去 24 小時中存有超過 40000 個密碼編譯操作、或在最後 60 分鐘中存有超過 2000 個密碼編譯操作，則該分槽係停止任何進一步的密碼編譯操作。

在一個實施例中，對於臨界值違例之稽核係能以每 5 分鐘的增量來實行。圖 5 係例示其中一個分槽業已在一個 25 分鐘滑動視窗中具有 800 個密碼編譯操作之一限制進行組態的一個實例。該滑動視窗係能被實施作為一個多階緩衝器 56。所例示的緩衝器係包含 5 階 58，而每一階係代表一個 5 分鐘的時間間隔。每一階係含有在其相對應的時間間隔期間由該分槽所實行之密碼編譯操作的數量之一個計數。下述表格係提供在一個給定時點處該緩衝器中所含有之資料的一個快照。

階	時間訊框	計數
1	-25 到 -20 分鐘	15
2	-20 到 -15 分鐘	0
3	-15 到 -10 分鐘	7
4	-10 到 -5 分鐘	1
5	-5 到 0 分鐘	6

假如所有該等計數之總和（在此案例中為 15 加 0 加 7

加 1 加 6 等於 29) 超過該臨界值，則該分槽係停止所有進一步的密碼編譯操作直到系統管理者予以重設。一個警告機制係能被實施以在停止操作的時間之前通知系統管理相關人員。例如：一個第一警告係可在總計數超過一個速率限制的 80% 時加以產生，而一個第二警告則是假如總計數達到此限制的 90% 時加以被產生。

與最近間隔相關聯之階（在此案例中為階 5）係保持各個新密碼編譯操作的一個持續計數。在各個 5 分中間個之結束處，所儲存的計數係被轉移到下一個最舊的階。最新的階係被重設為 0，且開始計數下一個 5 分鐘間隔所另行的密碼編譯操作。

由於各個分槽能以其自有的速率限制而選擇性地進行組態，所以對該事業邏輯之實施方式係提供適應性。例如：在下文所述，某些關鍵命令在能被執行之前可能需要一個明確類型的認證，下文被稱作為一個「許可證」。該些命令係可被映射到與用以落實此許可程序之一個分槽相關聯的一個安全性背景，且具有特別嚴格的速率限制。其它類型的命令係可被映射到不同的安全性背景，且可經由具有較不嚴格之速率限制的一個不同分槽進行加密及/或簽署。

對於諸如遠端斷開和重新連接之關鍵操作來說，諸如由多個所核准之一個叫高層級的安全性可能是適當的，而各個係必須在接收節點處受到認證。然而從網路效率的觀點來看，假如該命令所導引到之節點僅僅需要被聯繫一次即可執行該命令係理想的。在本發明的一個觀點中，前述

目標係能藉由用以提供所有所需資訊而使該節點能夠認證一個命令之一個許可系統所達成。本質上，被發送至一個應用程式（諸如到一個計量器的一個斷開命令）之每一個關鍵命令係可被要求要伴隨一個許可證。如上文所註記，不同類行之命令係能被映射到不同的安全性背景。當不論是自動地由一個應用程式還是透過一個使用者介面來發出一個命令時，發出的應用程式係檢驗該命令的安全性背景。假如需要加密，則該命令係被轉送到該硬體安全性模組之一個適當分槽以進行此一操作。假如作出該安全性背景需要一個許可證之一裁定，則該命令係被轉送到該掩體件中用以發出許可證之一個許可伺服器。在一個實施例中，該許可伺服器之功能係可藉由該硬體安全性模組中的一個分槽來實施。

用於發出許可證之一個佈置和程序的一個實例係被例示在圖 6 中，其參照一個用以將一個住處自該電力分佈網格斷開的命令。在此實例中，該後端支援部門 10 之多個商業模組中諸如一個稽核系統的一個商業模組係發出一個命令到該計量器管理應用程式 52，以斷開與一個帳戶相關聯之住處。在收到此命令時，該計量器管理應用程式係可排程一個特定時間的斷開操作。且接著經過一個保全鏈路以將一個信息發送到一個負載管理器模組 59，以請求用以發出該命令的許可。此負載管理器係位於該掩體件 42 內之商業邏輯的一個構件，且決定對於該分佈網格之負載改變是否可能有害。在此實例中，該負載管理器係作用為一個許

可伺服器之一個實施方式。該負載管理器係拒絕該請求（假如作出所請求的改變可能有害之一個裁定），將該請求延緩一段時間（例如：假如目前有太多未完成的請求），或者是核准該請求。對該負載管理器之請求係包含諸如目標節點、排程之操作時間、和所需完成執行該命令之時間視窗大小的資訊。

假如該請求得到核准，則該負載管理器係產生一個該命令待導引到之節點所辨認的許可證。在將該許可證回傳到該計量器管理應用程式 52 之前，該許可證係以與該負載管理器相關聯之一個金鑰進行簽署。在所例示實例中，該許可伺服器（亦即負載管理器 59）係與該硬體安全性模組 44 分開。因此在此案例中，該許可證係被發送到該硬體安全性模組，以被該負載管理器之私人金鑰進行簽署。經簽署許可證接著被回傳到該負載管理器，以被轉送至該計量器管理應用程式 52。

在收到該經簽署許可證時，該計量器管理應用程式係將該經授權命令搭配該經簽署許可證一起發送到與待斷開之住處相關聯的節點 26。該節點接著係能例如藉由依照一系列憑證來驗證該許可證：從該許可證經過該負載管理器之憑據到與該電力分佈網格之系統操作者相關聯的一個總管權限機構。該節點亦驗證該許可證內之時間數值與當前時間的一致性。假如所有資訊為正確且經過驗證，則該節點係執行該命令且將一個經簽署收條發送到該計量器管理應用程式 52，以指出該命令的完成。此收條的一個副本係

可被發送至該負載管理器 59，以使得該負載管理器能夠持續追蹤未完成的請求。

該計量器管理應用程式 52 係亦能對被發送到該節點之封包的酬載進行簽署，以對由不同控制實體（也就是該計量器管理應用程式和該負載管理器）所發出的命令提供兩個分開的授權。兩個形式的授權皆需要在該節點執行該命令之前先得到該節點的驗證。在此實例中，該許可伺服器（例如：負載管理器）未必佔有與該節點 26 直接通訊所需的憑據。反之，該許可伺服器係將憑據提供到另一控制實體（在此案例中是該計量器管理應用程式 52），以進行該經授權命令的執行。

用於決定是否核准一個命令之商業邏輯可能相對簡單（例如：其中許可一個預定斷開操作數量之一個初始叢集的一個漏桶演算法），而後隨每單位時間一個較少操作數量。在此案例中，該負載管理器之功能係可使用先前所數之速率控制而被實施在該硬體安全性模組的一個分槽內。另一較為複雜的演算法係能基於該電力分佈網格的狀態，例如追蹤實際的功率負載和作出基於預計之功率需求的裁定。此後述實施例係可如圖 6 所描述被實行在該硬體安全性模組的外部，例如在一個專用的實體系統、一個虛擬化伺服器或者是在一個分享系統上之一個應用程式內。

除了遠端斷開和重新連接，其它類型之命令同樣可能需要具有一個許可證，諸如被導引到一個客戶之住處以降低一段具體指定時間內的消耗之負載限制命令。再者，假

如在該系統中一個特定類性之裝置的安全操作對系統穩定性至關重要（諸如一個分佈自動化構件），則對該裝置發出之所有命令可能需要具有一個許可證。每當一個後端支援模組對此一個裝置發出一個命令，該後端支援模組係將該命令轉送到該許可伺服器以取得必要的許可證。

用於在一個信息之酬載內所含有之一個許可證的一個示範性格式係被描述在圖 7 中。此許可酬載之第一欄位 60 係指出一個起始時間，也就是該許可證成為有效之時間。當在一個節點處收到含有一個許可酬載之一個信息時，該節點係比較該起始時間和其當前時間。假如該起始時間晚於該當前時間加上一個預定增量（例如：5 分鐘），則該節點係拒絕該許可證的有效性。

該許可酬載之第二欄位 62 係指出期間該許可證維持有效之一個持續期間視窗。此欄位係含有用以指出在超過該許可證為有效之起始時間的數個預定時間間隔（例如：5 分鐘區間）之一個數值。假如該節點之當前時間大於該許可證之起始時間加上該預設間隔和該視窗數值之乘積，則該節點係拒絕該許可證的有效性。例如：假如該起始時間為 1：00：00，該視窗數值為 2，且當前時間為 1：12：38，則該許可證係視為已過期而被拒絕。

該許可酬載之下一個欄位 64 係指出獲准加以執行之操作。例如：此欄位係可含有用以指出一個電力斷開操作或一個電力重新連接操作之一個數值。多項操作係能聯繫單一個許可證。目標類型欄位 66 係指出用於其後隨之目標欄

位 68 的格式。該目標欄位 68 係指定用以實行獲准操作的節點或裝置。例如：此目標係能為該節點之 MAC 位址。該目標類型欄位 66 係指出其中該位址所表達之格式，例如一個 DER 八位元組字串。

為進一步增加安全性，一個約束係可被強加而使得一次僅能對一個計量器發出一個斷開命令或重新連接命令。在發出一個許可證之前，該負載管理器係可進行檢驗以確保對於該裝置之目標位址聯繫單一裝置，而不是一群組位址或廣播位址。

該許可酬載係能由與對經指示操作具有特權之一個憑證相關聯的私人金鑰進行簽署。在收到含有該許可酬載之資料封包時，該節點首先係進行檢驗以查看該經指示操作是否需要一個許可證。假如需要一個許可證，則該節點係確認被用來簽署該許可證之憑證和私人金鑰具有用以執行所請求操作之必要特權。假如此確認為肯定，則該節點係驗證經簽署許可證之真實性，當業已由經指示憑證對應之私人金鑰所簽署時。該節點接著係驗證該目標之指定識別出該節點本身。最後。該節點係檢查相對其當前時間之起始時間和視窗數值以確認該許可證還未過期。

假如成功地檢驗所有的驗證，則該操作係被執行，且一個回應係被回傳以確認執行的成功。假如前述驗證步驟中任一者無法達成，則該許可證係可被拒絕且一錯誤信息係被回傳。只要是已經完成該資料封包中的所有操作、或者回傳一個錯誤信息，則該許可證係被丟棄且不再保留。

在對該掩體件之存取遭到破壞的事件上，一合適形式之補救行動係可加以實行。此一個解決方案係提供一個與一個掩體件相關聯之邏輯或實體應急按鈕。此應急按鈕係能被啟動以對該管理系統知會與該應急按鈕相關聯之掩體件遭到破壞，且應該不再予以信任。例如：由一個經破壞掩體件所簽署之遠端斷開服務的任何請求係應該被忽略。

此應急按鈕係能以各種方式來實施。適合實例係包含經由一個無線或有線通訊系統、在被連接到一個區域或無線網路之適合位置處之實體按壓鈕（例如：在員工之辦公桌上）、及/或具有音頻命令機能和無線連接性之可配帶裝置所發送的控制訊號。

圖 8 係例示其中能實施一個應急按鈕之功能性的一個系統之一個實例。在此實例中，該公共事業管理和控制系統係被安置在兩個資料中心 70 和 72 內。例如：各個資料中心係可含有用於冗餘之各種管理和控制子系統的一個完整實例。各個資料中心係含有一個相關聯的掩體件，分別被標示為「掩體件 1」和「掩體件 2」。各個掩體件係具有其總管在一個已知的權限機構中之一個憑證系列的一個憑證。對於該兩個掩體件之此等憑證彼此係不相同。

在該控制網路中之各個節點（例如：存取點 32 和末端節點 26）係具有用以儲存和安裝一個憑證撤銷列表的能力。該等存取點 32 同樣具有用以過濾來源位址之能力。

一個示範性操作係將被敘述為對於掩體件 1 之存取業已遭到破壞的一個情況下。與該掩體件 1 相關聯之一個應

急按鈕係被啟動，且產生的應急訊號係被發送到該掩體件 2 中的一個伺服器以實施該應急按鈕的功能。此應急訊號係包含所予以發送之裝置的真實性之一個適當指示。例如：該應急訊號係可包含與該裝置相關聯之一個簽章，或者是伴隨依據一個預定演算法所產生之一個雜湊數值。在收到一個經過認證之應急訊號時，該掩體件 2 中之伺服器係發出多個命令以組態用於所有存取點 32 的一個防火牆規則，來指導該等存取點 32 將源自於資料中心 70 的封包丟棄。該掩體件 2 中之伺服器同樣發出多個命令以組態該等所有存取點 32 上的一個憑證撤銷列表，來指示與該掩體件 1 相關聯之憑證不再有效。該掩體件 2 中之伺服器同樣將一個信息發送到每一個末端節點，以指導每一個末端節點自一個存取點重新載入其憑證撤銷列表。

藉由組態該存取點上之防火牆過濾器以丟棄來自資料中心 70 的封包，一個佯裝的攻擊者係可被減緩一段時間，而足夠使該等憑證撤銷列表能夠被傳播到所有的末端節點。為了在已經發生一個潛在滲透之後回復掩體件 1，一個新憑證係必須被安裝，且與該憑證之新關聯性係加以進行且被傳播到該控制網路中的所有節點。

總結來說，本發明所揭示係提供各種的安全性特性以降低與由公共事業所提供商品之遞送相關聯的惡意行動或者另外不適當行動之風險。對一個公共事業分佈網路之穩定性具有可能性干擾的關鍵命令係透過下述機制而得到保全：用以對後端支援管理系統之敏感構件的存取有所限制

之一個實體掩體件，搭配使用用於認證、簽署和加密此等命令之一個硬體安全性模組。一個基於許可證之授權框架係對一個特定關鍵命令提供一更加精細之安全性層級。該硬體安全性模組同樣能經過組態以限制用以執行命令的速率，而進一步妨礙用以發出不恰當之一連串序列的嘗試。

熟習本項技術人士將理解到：所揭示之觀念係能以其它具體指定形式來體現，而不會悖離其精神和基本特徵。本發明所揭示之實施例在所有方面則被視具有例示性，而不是具有限制性。本發明之範疇係由後附的申請專利範圍所指出而不是前述的發明說明，且落入等效意義和範圍內之所有改變係預期被包含在本文中。

【圖式簡單說明】

圖 1 係一個公共事業管理和控制系統之一個通用方塊圖；

圖 2 係具有經掩護構件之一個公共事業管理後端支援系統的一個方塊圖；

圖 3 係用以示意性描述當一個信息被發送到一個計量器時之資料流的一個方塊圖；

圖 4 係一個硬體安全性模組之組態的一個方塊圖；

圖 5 係用以在一個滑動視窗中計數多個密碼編譯操作之一個多級緩衝器的一個方塊圖；

圖 6 係例示用於對多個命令發出許可證之一個系統和程序的一個實例；

圖 7 係一個許可酬載之一個示範性格式的一個方塊圖；

圖 8 係在多重資料中心中所實施之一個公共事業控制和管理系統的一個方塊圖。

【主要元件符號說明】

- 10：後端支援部門
- 12：客戶資訊系統（CIS）
- 14：客戶關係模組（CRM）
- 16：服務中斷管理系統（OMS）
- 18：GPS 資訊系統
- 20：計費系統
- 22：電網穩定模組
- 24：使用者介面
- 26：計量器 / （末端）節點
- 30：區域網路
- 32：存取點
- 34：廣域網路
- 40：資料中心
- 42：實體掩體件
- 44：硬體安全性模組（HSM）
- 46：授權引擎
- 48：決策模組
- 50：代理伺服器
- 52：計量器管理應用程式

54：（計量器）命令和介面模組

56：多階緩衝器

58：階

59：負載管理器（模組）

60：第一欄位

62：第二欄位

64：下一個欄位

66：目標類型欄位

68：目標欄位

70：資料中心

72：資料中心

七、申請專利範圍：

1.一種用於控制在一個公共事業網路中之多個裝置的方法，其係包括：

在該公共事業網路的一個後端支援部門系統中，對待以被該公共事業網路中之一個裝置所落實之一個操作產生一個命令；

在該後端支援部門系統中，決定該產生的命令是否請求一個密碼編譯服務被實行，以使該產生的命令被實行；

假如該產生的命令請求該密碼編譯服務被實行，則將該命令轉送到一個硬體安全性模組，其係該後端支援部門系統的一個保全構件，並且具有權限以授權該命令是否能被轉送到該裝置；

在該硬體安全性模組內執行下述功能：

在該命令上實行該密碼編譯服務，以在業已實行該密碼編譯服務時，使該命令之接收端能夠將該命令認證為該接收端獲准執行的命令；

計數在一個具體指定時段中藉由該硬體安全性模組所實行之多個密碼編譯服務的數量；及

假如在該具體指定時段內所實行之密碼編譯服務的經計數數量超過一個臨界限制，則終止在經接收命令上進一步密碼編譯服務的實行；以及

在業已實行該密碼編譯服務時，將該命令傳送到該公共事業網路中之該裝置以落實該操作。

2.如申請專利範圍第 1 項之方法，其中該計數該等密碼

編譯服務之數量係被實行在該具體指定時段之一個滑動時間視窗上。

3.如申請專利範圍第 2 項之方法，其中該計數該等密碼編譯服務之數量係針對複數個滑動時間視窗來實行，該等滑動時間視窗各者係與各自不同之時間長度和臨界限制相關聯。

4.如申請專利範圍第 1 項之方法，其中該密碼編譯服務係對該命令的加密。

5.如申請專利範圍第 1 項之方法，其中該密碼編譯服務係簽署該命令。

6.如申請專利範圍第 1 項之方法，其係進一步包括下述步驟：在該等密碼編譯服務之經計數數量達到低於該臨界限制之一個預定數值時產生一個警告。

7.如申請專利範圍第 1 項之方法，其中該硬體安全性模組係包括複數個分槽，且其中該等功能係被執行在該等分槽中的一個分槽。

8.如申請專利範圍第 7 項之方法，其中該等功能係使用各自不同的臨界限制以同樣被執行在一個第二分槽中。

9.如申請專利範圍第 1 項之方法，其中該裝置係經組態以決定一個經接收命令是否藉由使用與該密碼編譯服務相關聯之一個公開金鑰進行授權。

10.一種用於控制在一個公共事業網路中之多個裝置的方法，其係包括：

在該公共事業網路的一個後端支援部門系統中，對於

待以被該公共事業網路中之一個裝置所落實之一個操作產生一個命令；

在該後端支援部門系統中，決定產生的命令是否請求一個許可證以使該產生的命令被實行；

假如該產生的命令請求一個許可證，則將該命令轉送到一個許可伺服器，其係該後端支援部門系統的一個保全構件，並且具有權限以授權該命令是否能被轉送到該裝置；

在該許可伺服器內產生該許可證以具體指定 (i) 該許可證為有效之一個時段，(ii) 待以實行之操作，和 (iii) 實行該操作之裝置；

將含有該許可證之一個資料封包傳送到該公共事業網路中之裝置；

在該裝置處收到該資料封包時，決定具體指定的操作是否需要該許可證，且假如是如此，則決定該許可證目前是否有效；以及

假如該許可證目前為有效，則實行該具體指定的操作。

11.如申請專利範圍第 10 項之方法，其中該許可證係含有一個啟始數值和一個持續時間數值，該啟始數值係指出該許可證何時變為有效，且該持續時間數值係指出該許可證從該啟始數值開始保持有效的時間長度。

12.如申請專利範圍第 10 項之方法，其中該許可證係包含一個第一欄位和一個第二欄位，該第一欄位係含有要實行該操作之裝置的一個識別，且該第二欄位係指出該第一欄位之格式。

13.如申請專利範圍第 12 項之方法，其中在該第一欄位中所含有之識別係包括該裝置的一個 MAC 位址。

14.如申請專利範圍第 12 項之方法，其中該格式係一個 DER 八位元組字串。

15.如申請專利範圍第 10 項之方法，其中該許可證係藉由與該許可伺服器相關聯之一個金鑰進行簽署，且該裝置係驗證該許可證之簽章。

16.如申請專利範圍第 10 項之方法，其中該許可伺服器係被實施在一個硬體安全性模組內。

17.如申請專利範圍第 16 項之方法，其中該硬體安全性模組係執行下述功能：

計數在一個具體指定時段中藉由該硬體安全性模組所產生之多個許可證的數量；以及

假如在該具體指定時段內所產生之許可證的經計數數量超過一個臨界限制，則終止對於經接收命令之進一步許可證的產生。

18.如申請專利範圍第 17 項之方法，其中該計數經產生許可證之數量係被實行在該具體指定時段之一個滑動時間視窗上。

19.如申請專利範圍第 18 項之方法，其中該計數經產生許可證之數量係針對複數個滑動時間視窗來實行，該等滑動時間視窗各者係與各自不同之時間長度和臨界限制相關聯。

20.一種用於一個公共事業網路之認證系統，其係包括：

一個後端支援部門系統，其係經組態為對待以被該公共事業網路中之一個裝置所落實之一個操作產生一個命令，並且決定產生的命令是否請求一個許可證以使該產生的命令被實行；

一個許可伺服器，其係該後端支援部門系統的一個保全構件，該許可伺服器係經組態以在該後端支援部門系統決定該產生的命令請求該許可證時，從該後端支援部門系統接收該產生的命令，且產生該許可證以具體指定 (i) 該許可證為有效之一個時段，(ii) 待以實行之操作，和 (iii) 實行該操作之裝置；以及

一個通訊介面，其係經組態以將含有該許可證之一個資料封包傳送到該公共事業網路中之裝置。

21.如申請專利範圍第 20 項之認證系統，其中該許可證係含有一個啟始數值和一個持續時間數值，該啟始數值係指出該許可證何時變為有效，且該持續時間數值係指出該許可證從該啟始數值開始保持有效的時間長度。

22.如申請專利範圍第 20 項之認證系統，其中該許可伺服器係被實施在一個硬體安全性模組內。

23.如申請專利範圍第 22 項之認證系統，其中該硬體安全性模組係經組態以執行下述功能：

計數在一個具體指定時段中藉由該硬體安全性模組所產生之多個許可證的數量；以及

假如在該具體指定時段內所產生之許可證的經計數數量超過一個臨界限制，則終止對於經接收命令之進一步許

可證的產生。

24.如申請專利範圍第 23 項之認證系統，其中該計數經產生許可證之數量係被實行在該具體指定時段之一個滑動時間視窗上。

25.如申請專利範圍第 24 項之認證系統，其中該計數經產生許可證之數量係針對複數個滑動時間視窗來實行，該等滑動時間視窗各者係與各自不同之時間長度和臨界限制相關聯。

26.如申請專利範圍第 20 項之認證系統，其係進一步包括其中安置有該許可伺服器之一個實體保全環境。

27.如申請專利範圍第 20 項之認證系統，其係包括：

一個實體保全環境，該許可伺服器係被包括在該實體保全環境中；以及

至少一個伺服器，其係在該實體保全環境外部，該至少一個伺服器係經組態以響應於由該後端支援部門系統產生的命令，來執行與一個公共事業之操作相關聯的一個或更多應用程式，該等應用程式中之至少一些應用程式係具有用於接收來自該公共事業網路中之多個裝置的多個遠端請求之介面，以用於實行與該公共事業之操作相關的多個功能；

其中該許可伺服器係包括：

一個硬體安全性模組，其係位於該實體保全環境內部且儲存一個機密金鑰；

一個授權引擎，其係位於該實體保全環境內部，

該授權引擎係經組態以接收指向該等應用程式之多個遠端請求，且提供依據該機密金鑰所簽署之經授權請求；及

一個決策模組，其係位於該實體保全環境內部，該決策模組係經組態以依據與該等應用程式相關聯之商業邏輯來處理該等遠端請求，且選擇性地使該等請求能夠被該授權引擎所授權。

28.如申請專利範圍第 27 項之認證系統，其係進一步包括用於該介面之一個代理伺服器，其係位於該實體保全環境內部，該代理伺服器操作上係接收用在該等應用程式之多個遠端請求，以及將該等經接收請求轉送到該決策模組。

29.如申請專利範圍第 27 項之認證系統，其中該等應用程式係經組態以將由該等應用程式所接收的遠端請求重新指向該決策模組。

30.如申請專利範圍第 27 項之認證系統，其中該決策模組係經組態以決定在一個預定時段內所發出之含有多個命令以斷開電力的遠端請求之數量是否超過一個限制數值，且假如該等遠端請求之數量超過該限制數值則阻擋該等命令的執行。

31.如申請專利範圍第 27 項之認證系統，其中該決策模組係經組態以決定含有多個命令以斷開且重新連接電力之一個遠端請求序列是否與相同客戶相關聯，且假如符合此一條件則阻擋該等命令的執行。

32.如申請專利範圍第 27 項之認證系統，其中該決策模

組係經組態以決定含有一個命令以斷開或重新連接電力之一個遠端請求是否與一個客戶之當前狀態不一致，且假如不一致則阻擋該命令的執行。

33.如申請專利範圍第 27 項之認證系統，其中該決策模組係經組態以決定一個遠端請求是否接收自一個經認證來源，且假如該來源未經認證則阻擋該遠端請求的處理。

34.如申請專利範圍第 27 項之認證系統，其中該決策模組係經組態以決定用以實行一個操作之一個遠端請求是否接收自具有許可以請求此操作的一個應用程式，且假如作出請求的應用程式不具有此許可則阻擋該遠端請求的處理。

35.如申請專利範圍第 27 項之認證系統，其中該決策模組係藉由自該實體保全環境內所輸入之命令而可重新組態。

36.如申請專利範圍第 20 項之認證系統，其係包括：

一個實體保全環境，其係具有一個相關聯的認證憑證，該許可伺服器係被包括在該實體保全環境中；以及

至少一個存取點，該通訊介面係經由該至少一個存取點以與該公共事業網路中之多個裝置進行通訊；

其中響應於該實體保全環境的安全性業已遭到破壞的一個指示，該許可伺服器係經組態以發出一個憑證撤銷列表，進而指出與安全性遭到破壞之實體保全環境相關聯的憑證為無效，並且對該等裝置發出一個命令以自一個存取點載入該憑證撤銷列表。

37.如申請專利範圍第 36 項之認證系統，其中響應於該實體保全環境的安全性業已遭到破壞的一個指示，該許可伺服器係進一步對該至少一個存取點發出一個命令以丟棄源自於所在的實體保全環境業已遭到破壞之許可伺服器的通訊。

38.如申請專利範圍第 36 項之認證系統，其中該等裝置係經組態以決定一個經接收命令是否藉由使用與該許可伺服器中所儲存的一個密碼編譯金鑰相關聯之一個公開金鑰進行授權。

39.一種公共事業網路，其係包括：

一個後端支援部門系統，其係經組態為對待以被該公共事業網路中之一個裝置所落實之一個操作產生一個命令，並且決定產生的命令是否請求一個許可證以使該產生的命令被實行；

一個許可伺服器，其係該後端支援部門系統的一個保全構件，該許可伺服器係經組態以在該後端支援部門系統決定該產生的命令請求該許可證時，從該後端支援部門系統接收該產生的命令，且產生該許可證以具體指定 (i) 該許可證為有效之一個時段，(ii) 待以實行之操作，和 (iii) 實行該操作之裝置；

一個通訊介面，其係經組態以經由該公共事業網路來傳送含有該許可證之一個資料封包；以及

複數個裝置，其係經連接到該公共事業網路以用於接收資料封包，該等裝置中各者係經組態以：

決定在一個經接收資料封包中所具體指定之操作是否需要該許可證；

假如是如此，則決定該許可證目前是否有效；且

假如該許可證目前為有效，則實行該具體指定的操作。

40.如申請專利範圍第 39 項之公共事業網路，其中該許可證係含有一個啟始數值和一個持續時間數值，該啟始數值係指出該許可證何時變為有效，且該持續時間數值係指出該許可證從該啟始數值開始保持有效的時間長度。

41.如申請專利範圍第 39 項之公共事業網路，其中該許可伺服器係經組態以使用一個金鑰來簽署該許可證，且該裝置係經組態以驗證該許可證之簽章。

42.如申請專利範圍第 39 項之公共事業網路，其中該許可伺服器係被實施在一個硬體安全性模組內。

43.如申請專利範圍第 42 項之公共事業網路，其中該硬體安全性模組係經組態以執行下述功能：

計數在一個具體指定時段中藉由該硬體安全性模組所產生之多個許可證的數量；以及

假如在該具體指定時段內所產生之許可證的經計數數量超過一個臨界限制，則終止對於經接收命令之進一步許可證的產生。

44.如申請專利範圍第 43 項之公共事業網路，其中該計數經產生許可證之數量係被實行在該具體指定時段之一個滑動時間視窗上。

45.如申請專利範圍第 44 項之公共事業網路，其中該計數經產生許可證之數量係針對複數個滑動時間視窗來實行，該等滑動時間視窗各者係與各自不同之時間長度和臨界限制相關聯。

八、圖式：

(如次頁)

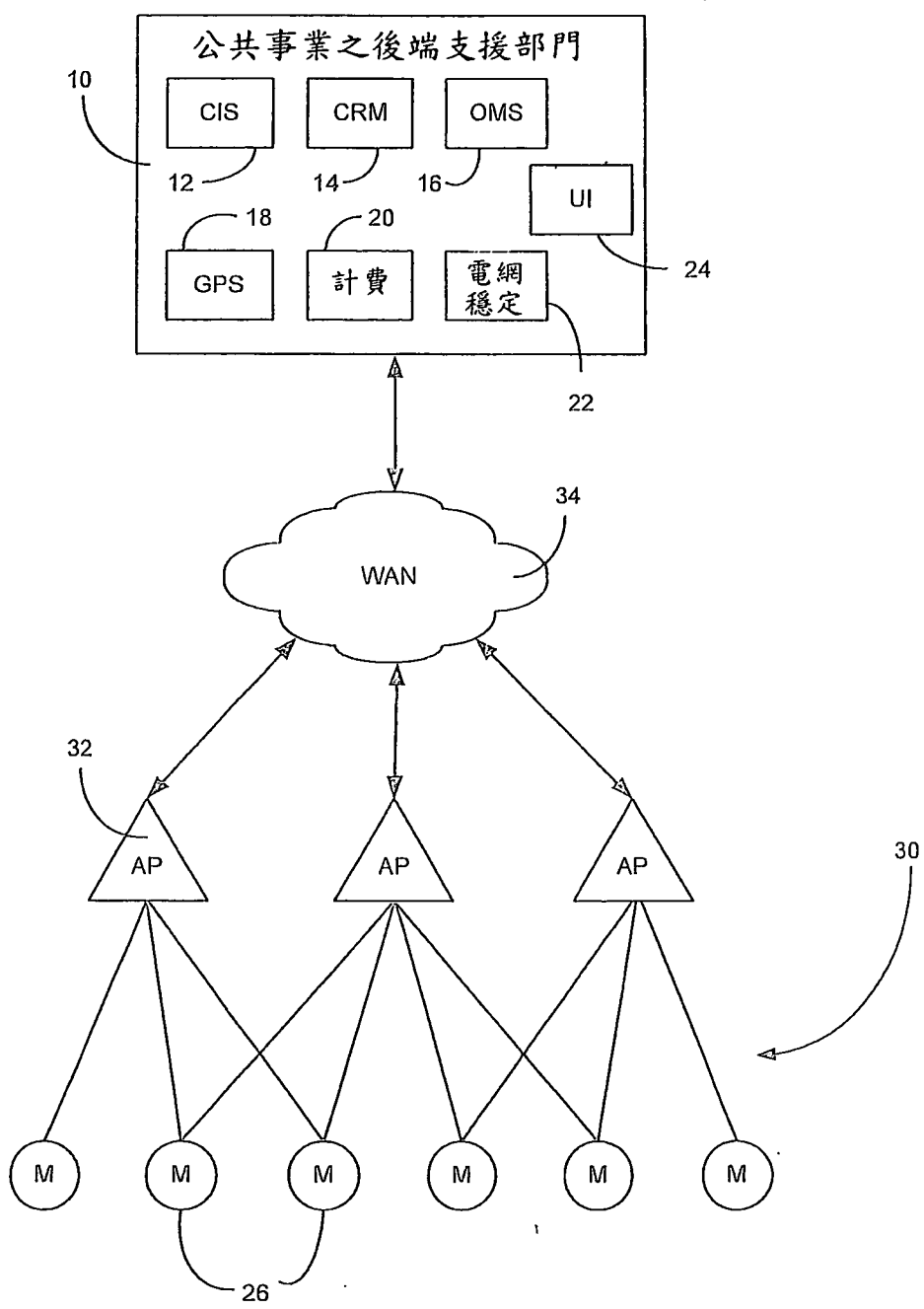


圖 1

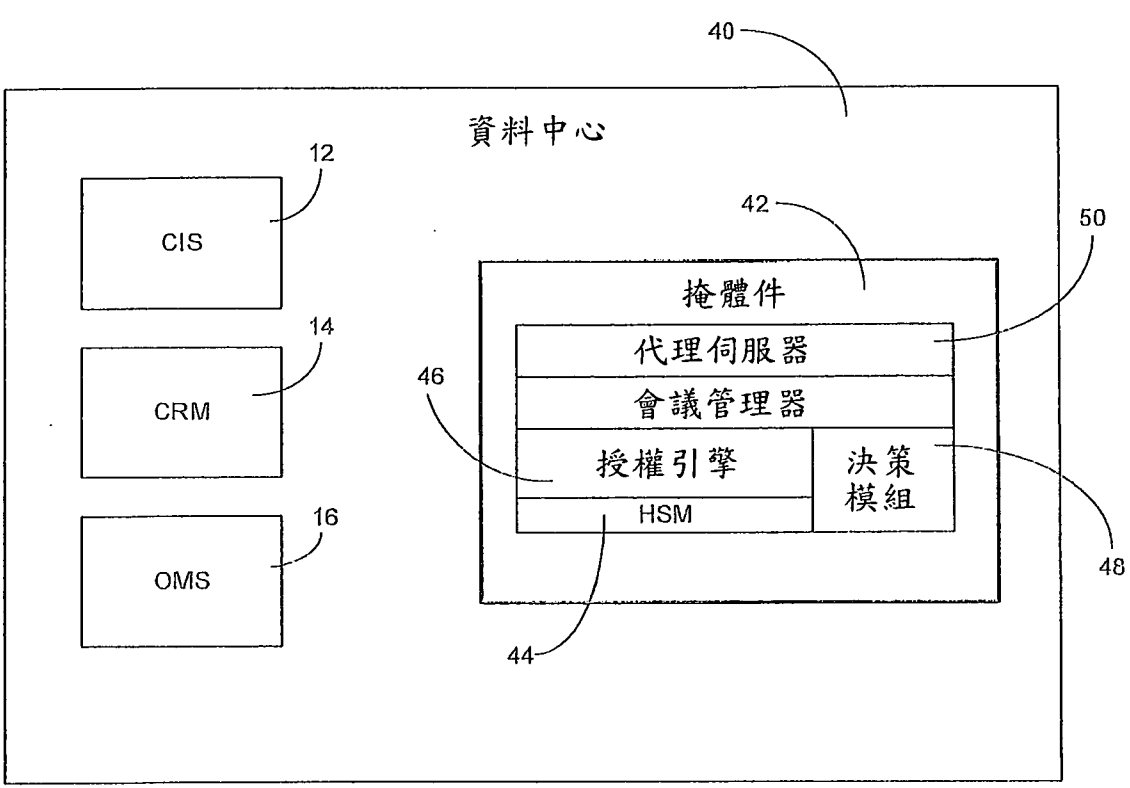


圖2

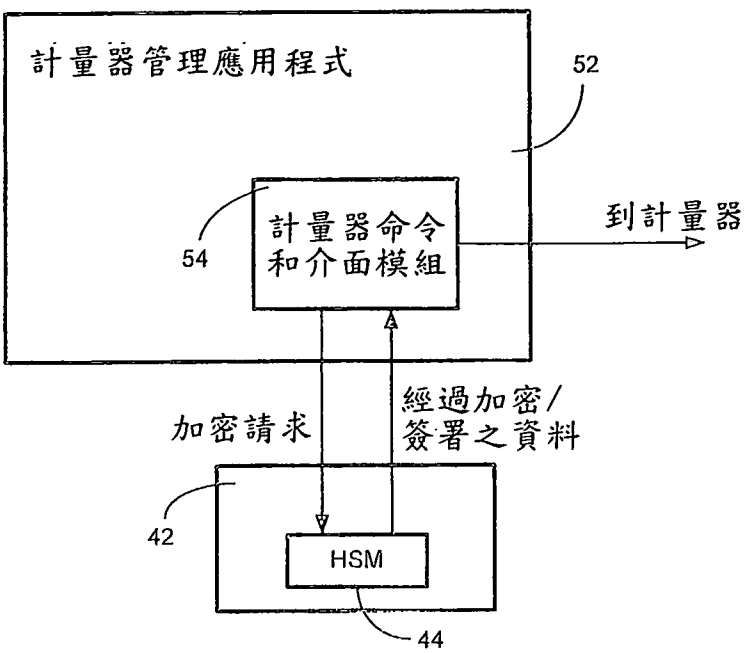


圖3

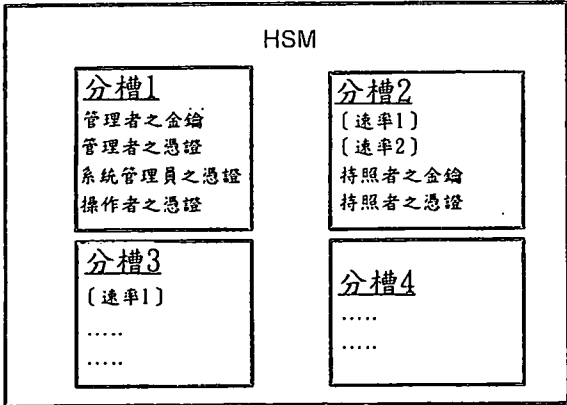


圖4

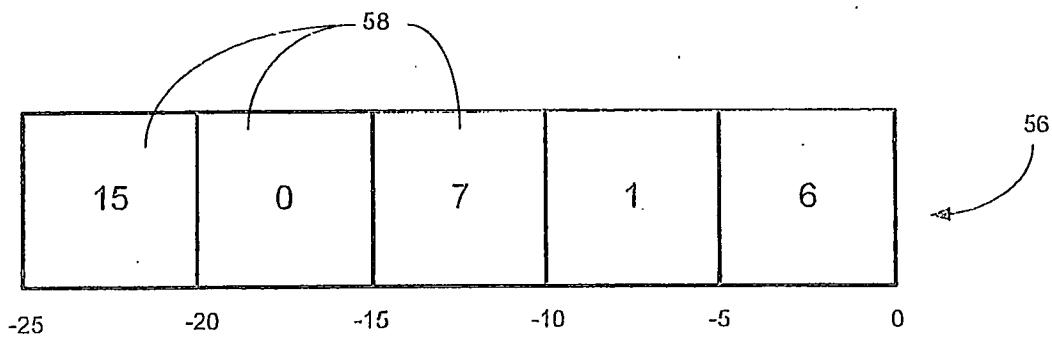


圖5

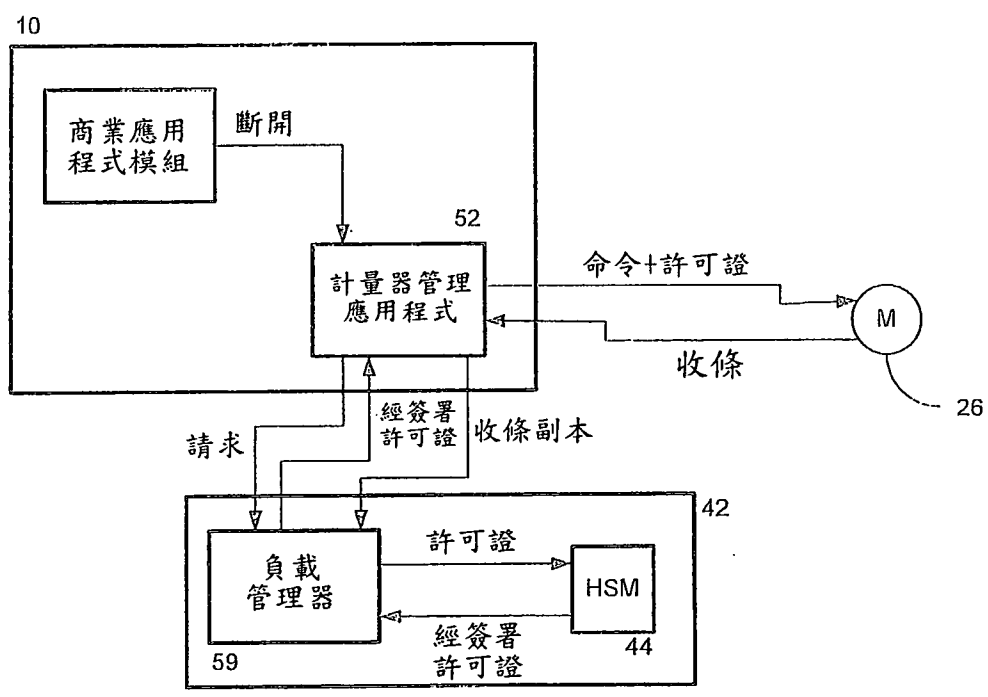


圖6

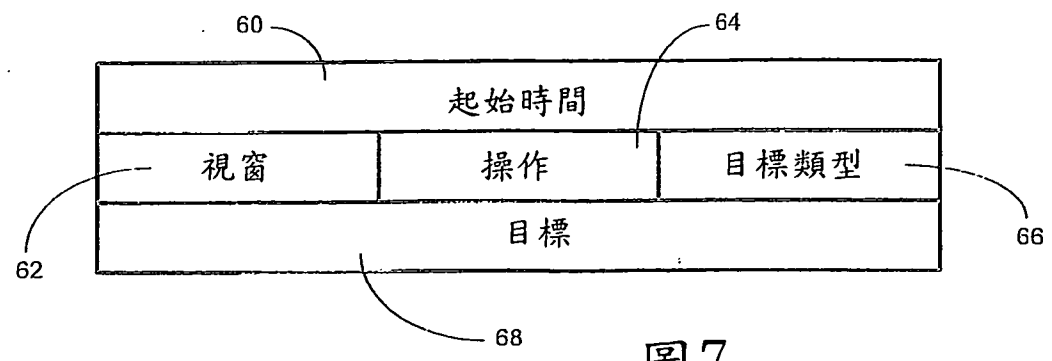


圖7

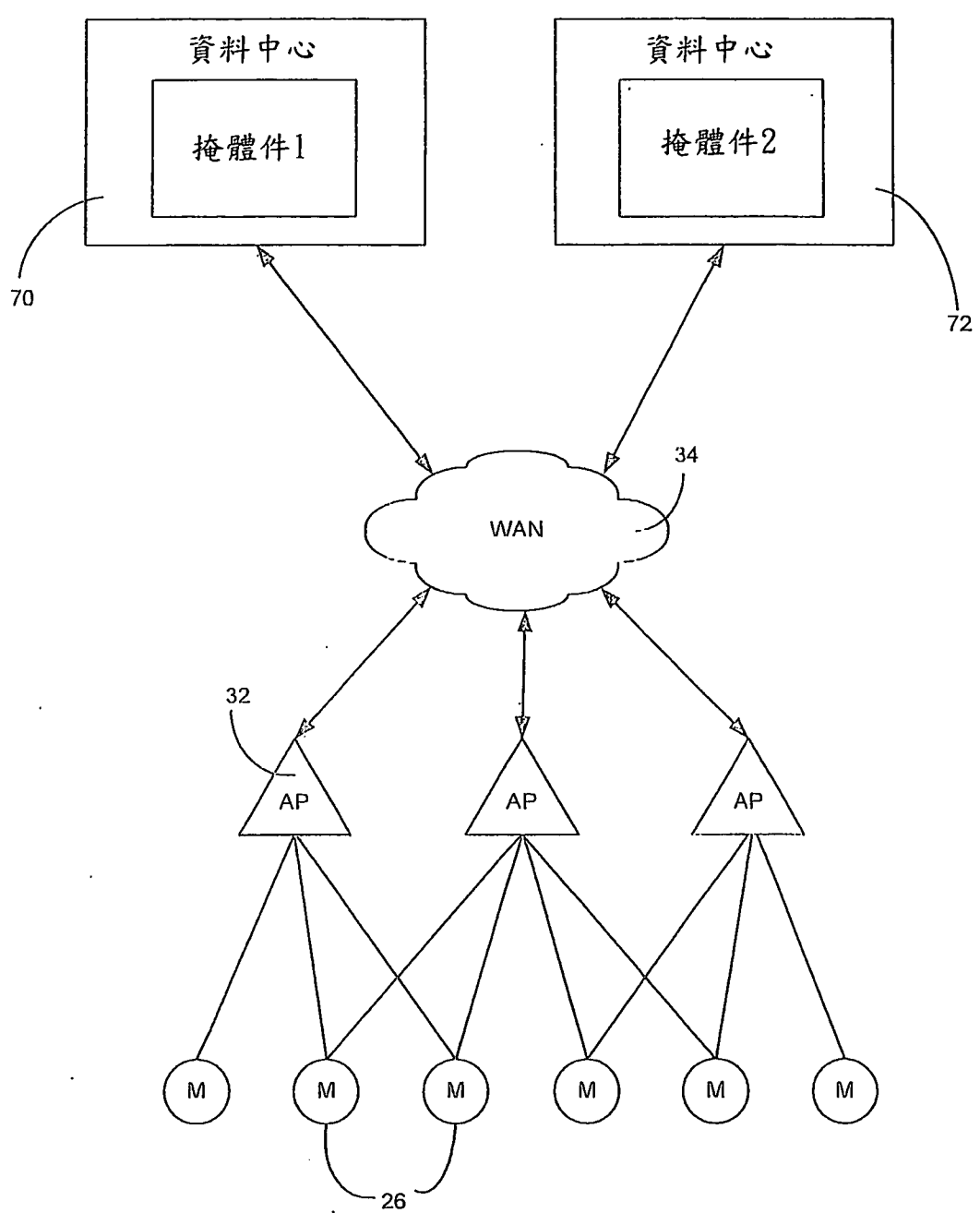


圖8