I733340

(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 I733340 B**

(45)公告日： 中華民國 110 (2021) 年 07 月 11 日

(21)申請案號：109105290　(22)申請日： 中華民國 109 (2020) 年 02 月 19 日

(51)Int. Cl.：　*G06F21/30　(2013.01)*　*H04L9/30　(2006.01)*

(71)申請人：網聯科技股份有限公司 (中華民國) TANGRAM CO., LTD.　(TW)

臺中市大雅區大雅里雅潭路 4 段 837 號 4 樓

(72)發明人：黃士瀅 (TW)；林鼎皓 (TW)

(74)代理人：高玉駿；楊祺雄

(56)參考文獻：

TW	200533138A	CN	108173662A
CN	108471426A	US	2015/0113275A1

審查人員：郭彥鋒

申請專利範圍項數：11 項　　圖式數：2　　共 16 頁

(54)名稱

合法性驗證方法

(57)摘要

一種合法性驗證方法，藉由伺服端及電子裝置的主從式系統實施，該電子裝置持續地接收與時間相關的外部資料，該方法包含：電子裝置根據所儲存的已傳送目標區段產生並傳送第一關鍵值至伺服端；伺服端根據所儲存的已接收目標區段產生第二關鍵值，且判斷第一關鍵值與第二關鍵值是否相同；若相同則傳送傳輸認可回覆給電子裝置；電子裝置在接收到傳輸認可回覆後，傳送外部資料至伺服端；電子裝置根據外部資料產生第一目標區段並以其更新已傳送目標區段；伺服端接收外部資料後，根據所接收之外部資料產生第二目標區段並以其更新已接收目標區段。

指定代表圖：

符號簡單說明：

50~61:步驟

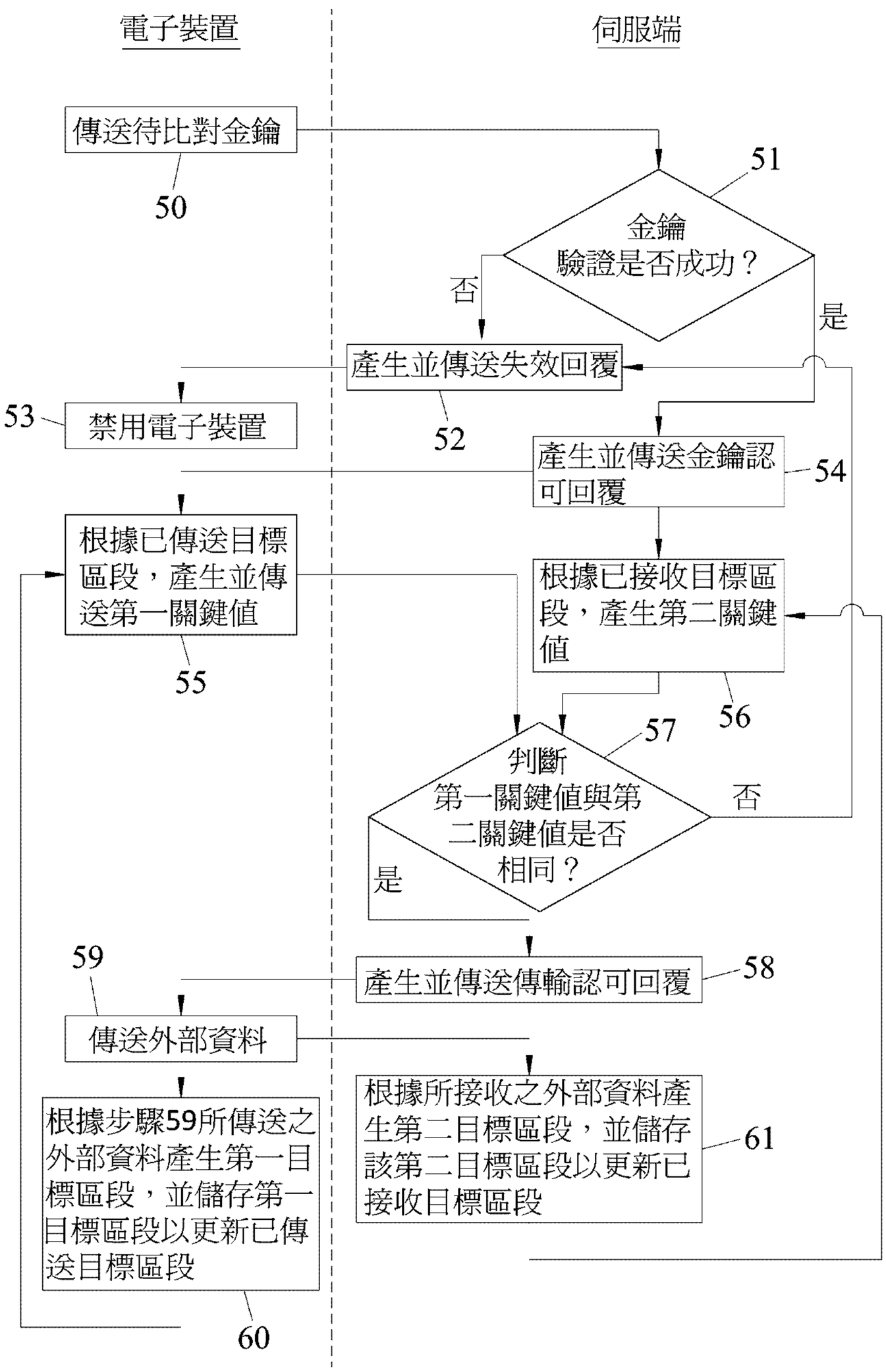

圖2

專利案號：109105290

公告本

I733340

【發明摘要】

【中文發明名稱】　合法性驗證方法

【中文】

一種合法性驗證方法，藉由伺服端及電子裝置的主從式系統實施，該電子裝置持續地接收與時間相關的外部資料，該方法包含：電子裝置根據所儲存的已傳送目標區段產生並傳送第一關鍵值至伺服端；伺服端根據所儲存的已接收目標區段產生第二關鍵值，且判斷第一關鍵值與第二關鍵值是否相同；若相同則傳送傳輸認可回覆給電子裝置；電子裝置在接收到傳輸認可回覆後，傳送外部資料至伺服端；電子裝置根據外部資料產生第一目標區段並以其更新已傳送目標區段；伺服端接收外部資料後，根據所接收之外部資料產生第二目標區段並以其更新已接收目標區段。

【指定代表圖】：圖（2）。

【代表圖之符號簡單說明】

50~61:步驟

【發明說明書】

【中文發明名稱】　合法性驗證方法

【技術領域】

【0001】本發明是有關於一種系統驗證方法，特別是指一種可確保所連接之電子裝置為安全合法且可信任的驗證方法。

【先前技術】

【0002】現有的一電子裝置在與一伺服端初次建立連線並連接時，該電子裝置會向該伺服端索取一金鑰，並將其永久儲存至該電子裝置中，日後當電子裝置欲再次連接至該伺服端時，便會將該金鑰傳送至該伺服端，並由該伺服端對金鑰驗證成功後，才能確定與該電子裝置的連接。

【0003】然而，當有不肖人士直接採用「硬拷貝」的方式製造出該電子裝置（連同所儲存之該金鑰也拷貝）時，該伺服端則無法辨識出該電子裝置的真偽。

【0004】有鑑於此，勢必須提出一種全新解決方案，以驗證該電子裝置的合法性，並克服傳統技術所面臨之問題。

【發明內容】

【0005】因此，本發明的目的，即在提供一種以一主從式系統來實施的合法性驗證方法，該主從式系統包含一伺服端，及通訊連接該伺服端之一電子裝置，該電子裝置持續地接收其周邊的複數外部資料，該合法性驗證方法用於驗證該電子裝置之合法性，並包含下列步驟：

【0006】(A)藉由該電子裝置，根據其所儲存的一已傳送目標區段產生一第一關鍵值，並傳送該第一關鍵值至該伺服端；

【0007】(B)藉由該伺服端，根據其所儲存的一已接收目標區段產生一第二關鍵值；

【0008】(C)藉由該伺服端，接收該第一關鍵值，並判斷該第一關鍵值與該第二關鍵值是否相同；

【0009】(D)若步驟(C)判斷出該第一關鍵值等於該第二關鍵值，則藉由該伺服端，傳送一傳輸認可回覆給該電子裝置，否則，傳送一失效回覆給該電子裝置；

【0010】(E)藉由該電子裝置，在接收到該傳輸認可回覆後，傳送該等外部資料至該伺服端，其中，該等外部資料係與時間相關；

【0011】(F)藉由該電子裝置，根據步驟(E)所傳送之該等外部資料產生一第一目標區段，並儲存該第一目標區段以更新該已傳送目標區段；及

【0012】(G)藉由該伺服端，在接收該等外部資料後，根據其所接

收之該等外部資料產生一第二目標區段，並儲存該第二目標區段以更新該已接收目標區段。

【0013】本發明之另一目的，即在提供一種以一電子裝置來實施的合法性驗證方法，該電子裝置通訊連接一伺服端，且該電子裝置持續地接收其周邊的複數外部資料，該合法性驗證方法用於驗證該電子裝置之合法性，並包含下列步驟：

【0014】(A)藉由該電子裝置，根據其所儲存的至少一已傳送目標區段產生一第一關鍵值；

【0015】(B)藉由該電子裝置，傳送該第一關鍵值至該伺服端，以使該伺服端根據該第一關鍵值，及其所產生的一第二關鍵值，決定傳送一失效回覆或一傳輸認可回覆給該電子裝置；

【0016】(C)藉由該電子裝置，在接收到該傳輸認可回覆後，傳送該等外部資料至該伺服端，其中，該等外部資料係與時間相關；及

【0017】(D)藉由該電子裝置，根據步驟(C)所傳送之該等外部資料產生一第一目標區段，並儲存該第一目標區段以更新該已傳送目標區段。

【0018】由於該等外部資料與時間相關，若該電子裝置被更換，其傳送的外部資料與該伺服端所接收的外部資料不同步，便無法通過驗證，更進一步來說，即使以「硬拷貝」的方式製造出多個電子裝置，當其中一電子裝置重新與該伺服端連接，開始接受與時間相

關的外部資料並與該伺服器進行合法性驗證後，其餘「硬拷貝」製造出的電子裝置，即無法通過驗證，故可克服傳統技術所面臨之問題。

【圖式簡單說明】

【0019】本發明的其他的特徵及功效，將於參照圖式的實施方式中清楚地呈現，其中：

圖 1 是一方塊圖，說明一執行本發明合法性驗證方法的一較佳實施例的一主從式系統；及

圖 2 是一流程圖，說明該較佳實施例的步驟 50~61。

【實施方式】

【0020】在本發明被詳細描述之前，應當注意在以下的說明內容中，類似的元件是以相同的編號來表示。

【0021】參閱圖1，本發明合法性驗證方法之一較佳實施例，係藉由一主從式系統100來實施，該主從式系統100包含一伺服端1，以及一通訊連接該伺服端1的電子裝置2。

【0022】該伺服端1包括一連接至通訊網路(圖未示)的伺服端通訊模組11、一伺服端儲存模組12，以及一電連接該伺服端通訊模組11與該伺服端儲存模組12的伺服端處理模組13。

【0023】該電子裝置2用於持續地接收其周邊之複數外部資料，其中，該等外部資料係與時間相關。該電子裝置2包括一連接至通訊網路的電子端通訊模組21、一電子端儲存模組22、一用於接收該等外部資料的電子端輸入/輸出(以下簡稱I/O)模組23，以及一電連接該電子端通訊模組21、該電子端儲存模組22與該電子端I/O模組23的電子端處理模組24。在本較佳實施例中，每一外部資料可為該電子裝置2周邊的感測資料、ON/OFF訊號、Counter資料等，但不以此為限。

【0024】其中，該電子裝置2可設置於各種需要收集外部資料的設備上，舉例來說，該電子裝置2可設置於加工機之主軸或刀庫，以收集加工機使用過程中的溫度、震動、音量、濕度等外部資料。

【0025】參閱圖1與2，本發明合法性驗證方法之較佳實施例包含下列步驟。

【0026】在步驟50中，該電子端處理模組24透過該電子端通訊模組21將該電子端儲存模組22預先儲存之一待比對金鑰傳送至該伺服端1。

【0027】在步驟51中，該伺服端處理模組13在透過該伺服端通訊模組11接收到該待比對金鑰後，根據其預先儲存之一伺服端金鑰對該待比對金鑰進行驗證；若金鑰驗證失敗，代表該電子裝置2並非合法之裝置，則進行步驟52之處理，若金鑰驗證成功，則進行步驟

54之處理。

【0028】其中，所述金鑰驗證方式係為習知技術，且非本發明之重點，故不在此贅述其細節。

【0029】在步驟52中，該伺服端處理模組13產生一失效回覆，並透過該伺服端通訊模組11將該失效回覆傳送至該電子裝置2。

【0030】在步驟53中，該電子端處理模組24在透過該電子端通訊模組21接收到該失效回覆後，使該電子裝置2本身失效，即，禁用（Disable）該電子裝置2。

【0031】在步驟54中，該伺服端處理模組13產生一金鑰認可回覆，並透過該伺服端通訊模組11將該金鑰認可回覆傳送至該電子裝置2。

【0032】在步驟55中，該電子端處理模組24根據儲存於該電子端儲存模組22的一已傳送目標區段，產生一第一關鍵值，並透過該電子端通訊模組21將該第一關鍵值傳送至該伺服端1。

【0033】在步驟56中，該伺服端處理模組13根據儲存於該伺服端儲存模組11的一已接收目標區段產生一第二關鍵值。

【0034】在步驟57中，該伺服端處理模組13在透過該伺服端通訊模組11接收該第一關鍵值後，判斷該第一關鍵值與該第二關鍵值是否相同；若是，則進行步驟58之處理，否則，代表該電子裝置2並非合法之裝置，回到步驟52之處理。

【0035】在步驟58中，該伺服端處理模組13產生一傳輸認可回覆，並透過該伺服端通訊模組11將該傳輸認可回覆至該電子裝置2。

【0036】在步驟59中，該電子端處理模組24在透過該電子端通訊模組21接收到該傳輸認可回覆後，傳送該等外部資料至該伺服端1，其中，該等外部資料係由該電子端I/O模組23持續接收，每一外部資料包括複數資料段，及分別對應該等資料段的複數時間戳記（Timestamp）。

【0037】在步驟60中，該電子端處理模組24根據步驟59所傳送之該等外部資料產生一第一目標區段，並儲存該第一目標區段以更新該已傳送目標區段，並回到流程步驟55。其中，該第一目標區段係選自於步驟59所傳送之該等外部資料，且該第一目標區段具有至少一選自於該等外部資料之時間戳記。

【0038】在步驟61中，該伺服端處理模組13在透過該伺服端通訊模組11接收該等外部資料後，根據所接收之該等外部資料產生一第二目標區段，並儲存該第二目標區段以更新該已接收目標區段，並回到流程步驟56。其中，該第二目標區段係選自於該伺服端1所接收之該等外部資料，且該第二目標區段具有至少一選自於該等外部資料之時間戳記。

【0039】值得一提的是，該電子裝置2與該伺服端1係以相同的規則，分別自所傳送及所接收的該等外部資料選出該第一目標區段及

該第二目標區段，且該電子裝置2與該伺服端1亦是以相同的演算法，例如，以相同的雜湊（hash）函式，分別根據該已傳送目標區段及該已接收目標區段產生該第一關鍵值及該第二關鍵值。

【0040】綜上所述，若該電子裝置2被更換，其傳送的外部資料與該伺服端1所接收的外部資料不同步，自然無法計算出相同的該第一關鍵值及該第二關鍵值，故無法通過驗證；更進一步來說，若以「硬拷貝」的方式製造出多個電子裝置(圖未示)，當其中任一電子裝置與該伺服端1連線，該等外部資料的時間戳記會繼續更新，若此時再有其餘「硬拷貝」製造的電子裝置試圖連上，這些電子裝置皆會被禁用，且該伺服端1發現此種異常狀況時，亦可進一步發出異常訊息供使用者知悉。因此，確實能達成本發明的目的。

【0041】惟以上所述者，僅為本發明的實施例而已，當不能以此限定本發明實施的範圍，凡是依本發明申請專利範圍及專利說明書內容所作的簡單的等效變化與修飾，皆仍屬本發明專利涵蓋的範圍內。

【符號說明】

【0042】

100:主從式系統

1:伺服端

11:伺服端通訊模組

12:伺服端儲存模組

13:伺服端處理模組

2:電子裝置

21:電子端通訊模組

22:電子端儲存模組

23:電子端 I/O 模組

24:電子端處理模組

50~61:步驟

【發明申請專利範圍】

【第1項】 一種合法性驗證方法，以一主從式系統來實施，該主從式系統包含一伺服端，及通訊連接該伺服端之一電子裝置，該電子裝置持續地接收其周邊的複數外部資料，該合法性驗證方法用於驗證該電子裝置之合法性，並包含以下步驟：

(A) 藉由該電子裝置，根據其所儲存的一已傳送目標區段產生一第一關鍵值，並傳送該第一關鍵值至該伺服端；

(B) 藉由該伺服端，根據其所儲存的一已接收目標區段產生一第二關鍵值；

(C) 藉由該伺服端，接收該第一關鍵值，並判斷該第一關鍵值與該第二關鍵值是否相同；

(D) 若步驟(C)判斷出該第一關鍵值等於該第二關鍵值，則藉由該伺服端，傳送一傳輸認可回覆給該電子裝置，否則，傳送一失效回覆給該電子裝置；

(E) 藉由該電子裝置，在接收到該傳輸認可回覆後，傳送該等外部資料至該伺服端，其中，該等外部資料係與時間相關；

(F) 藉由該電子裝置，根據步驟(E)所傳送之該等外部資料產生一第一目標區段，並儲存該第一目標區段以更新該已傳送目標區段；及

(G) 藉由該伺服端，在接收該等外部資料後，根據其所接收之該等外部資料產生一第二目標區段，並儲存該第

二目標區段以更新該已接收目標區段。

【第2項】 如請求項1所述的合法性驗證方法，還包含步驟(G)之後的下列步驟：

(H) 回到步驟(A)。

【第3項】 如請求項1所述的合法性驗證方法，還包含步驟(D)之後的下列步驟：

(I) 藉由該電子裝置，在接收到該失效回覆後，使該電子裝置失效。

【第4項】 如請求項1所述的合法性驗證方法，其中，每一外部資料包括複數資料段，及分別對應該等資料段的複數時間戳記。

【第5項】 如請求項4所述的合法性驗證方法，其中，在步驟(F)中，該第一目標區段係選自於步驟(E)所傳送之該等外部資料，且該第一目標區段具有至少一選自於該等外部資料之時間戳記。

【第6項】 如請求項5所述的合法性驗證方法，其中，在步驟(G)中，該第二目標區段係選自於該伺服端所接收之該等外部資料，且該第二目標區段具有至少一選自於該等外部資料之時間戳記。

【第7項】 一種合法性驗證方法，藉由通訊連接一伺服端的一電子裝置來實施，該電子裝置持續地接收其周邊的複數外部資料，該合法性驗證方法用於驗證該電子裝置之合法性，並包含下列步驟：

(A) 藉由該電子裝置，根據其所儲存的至少一已傳送

目標區段產生一第一關鍵值；

(B) 藉由該電子裝置，傳送該第一關鍵值至該伺服端，以使該伺服端根據該第一關鍵值，及其所產生的一第二關鍵值，決定傳送一失效回覆或一傳輸認可回覆給該電子裝置；

(C) 藉由該電子裝置，在接收到該傳輸認可回覆後，傳送該等外部資料至該伺服端，其中，該等外部資料係與時間相關；及

(D) 藉由該電子裝置，根據步驟(C)所傳送之該等外部資料產生一第一目標區段，並儲存該第一目標區段以更新該已傳送目標區段。

【第8項】 如請求項7所述的合法性驗證方法，還包含步驟(D)之後的下列步驟：

(E) 回到步驟(A)。

【第9項】 如請求項7所述的合法性驗證方法，還包含步驟(B)之後的下列步驟：

(F) 藉由該電子裝置，在接收到該失效回覆後，使該電子裝置失效。

【第10項】如請求項7所述的合法性驗證方法，其中，每一外部資料包括複數資料段，及分別對應該等資料段的複數時間戳記。

【第11項】如請求項10所述的合法性驗證方法，其中，在步驟(D)中，該第一目標區段係選自於步驟(C)所傳送之該等外部資料，且該第一目標區段具有至少一選自於該等外部資料之

時間戳記。

【發明圖式】

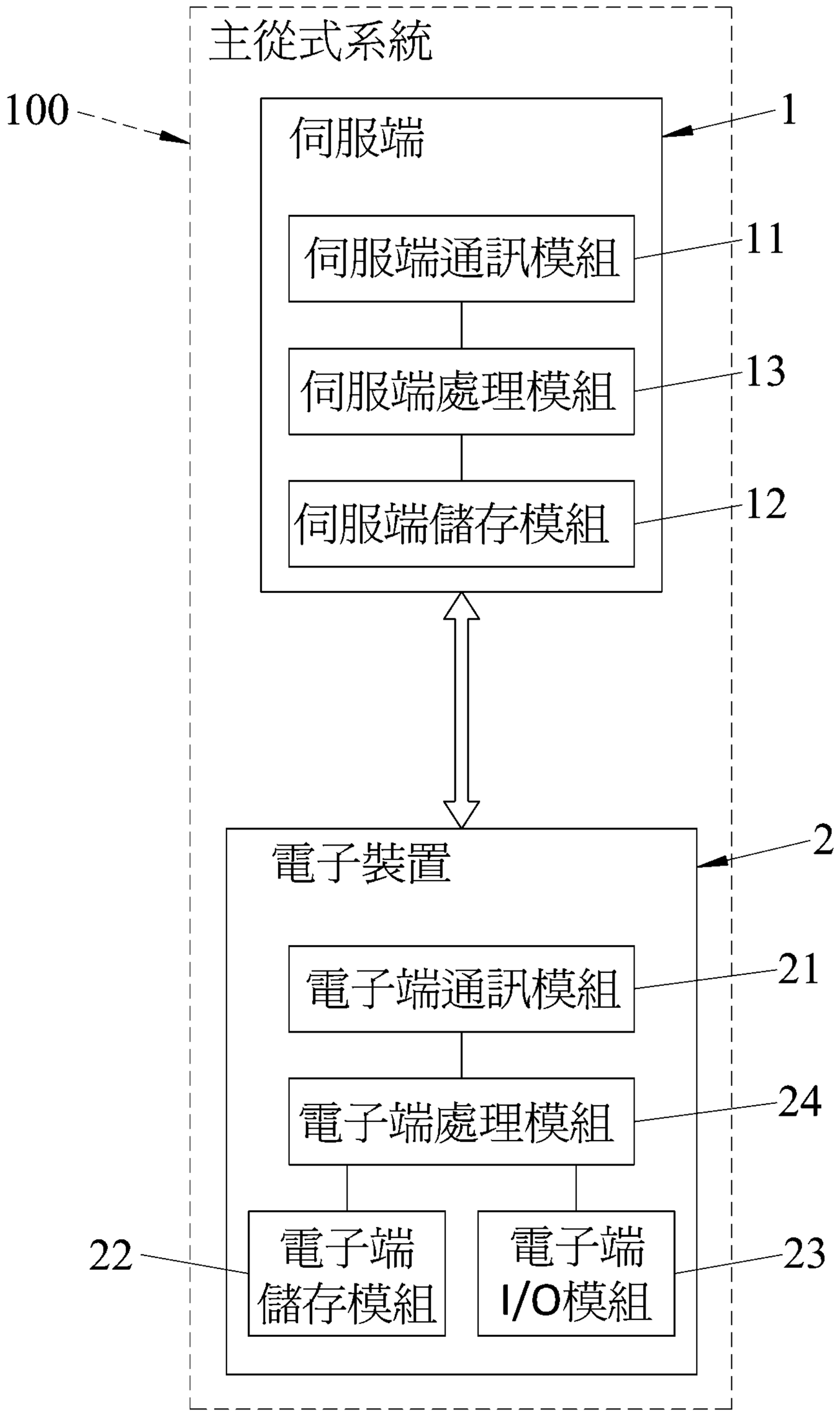
主從式系統
100
伺服端
1
伺服端通訊模組
11
伺服端處理模組
13
伺服端儲存模組
12
電子裝置
2
電子端通訊模組
21
電子端處理模組
24
22
電子端
儲存模組
電子端
I/O模組
23

圖1

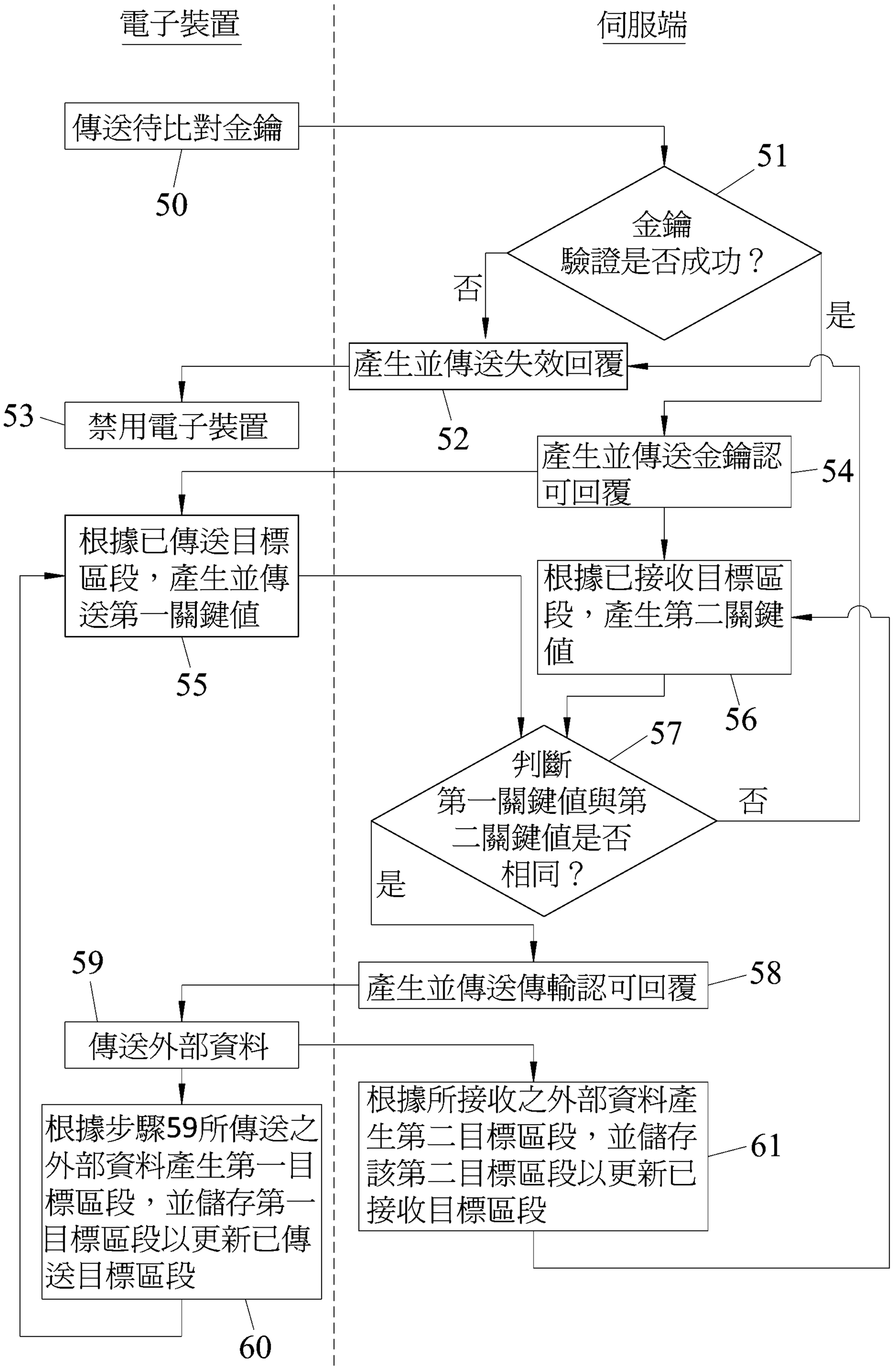
電子裝置
伺服端
傳送待比對金鑰
50
51
金鑰
驗證是否成功？
否
是
產生並傳送失效回覆
52
53
禁用電子裝置
產生並傳送金鑰認可回覆
54
根據已傳送目標區段，產生並傳送第一關鍵值
55
根據已接收目標區段，產生第二關鍵值
56
57
判斷
第一關鍵值與第二關鍵值是否相同？
否
是
59
產生並傳送傳輸認可回覆
58
傳送外部資料
根據步驟59所傳送之外部資料產生第一目標區段，並儲存第一目標區段以更新已傳送目標區段
60
根據所接收之外部資料產生第二目標區段，並儲存該第二目標區段以更新已接收目標區段
61

圖2