201719476

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201719476 A

(43)公開日： 中華民國 106 (2017) 年 06 月 01 日

(21)申請案號：105137495 (22)申請日： 中華民國 105 (2016) 年 11 月 16 日

(51)Int. Cl.： *G06F21/30 (2013.01)* *H04L9/32 (2006.01)*

(30)優先權：2015/11/16 中國大陸 201510785827.2

(71)申請人：中國銀聯股份有限公司 (中國大陸) (CN)
中國大陸

(72)發明人：李定洲 (CN)；周鈺 (CN)；郭偉 (CN)；陳成錢 (CN)；嚴翔翔 (CN)；曾望年 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：18 項 圖式數：3 共 20 頁

(54)名稱

一種在設備之間進行授權的方法和裝置

(57)摘要

在設備之間進行授權的方法的裝置。方法包括授權過程，該授權過程包括：在第一設備的 TEE 端生成並加密授權信息，在第一設備的 REE 端將經加密的授權信息傳輸到第二設備，在第二設備的 REE 端接收經加密的授權信息，在第二設備的 TEE 端解密並驗證經加密的授權信息，在第二設備存儲該授權信息。

指定代表圖：

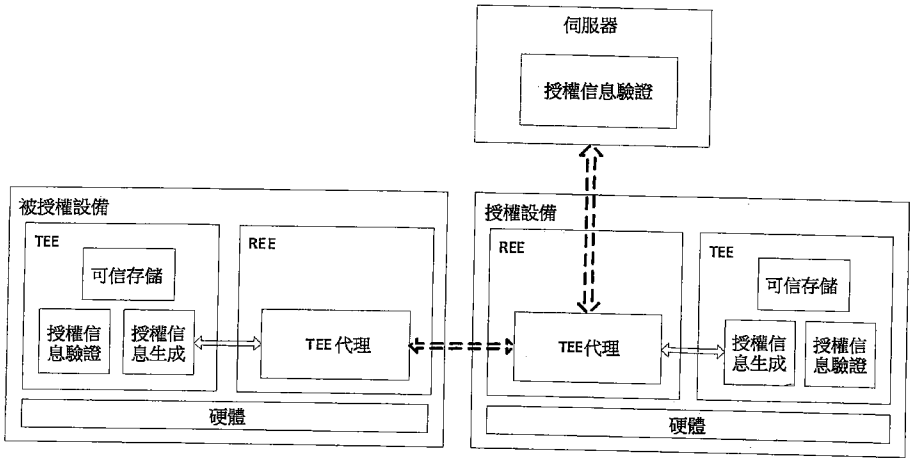

圖 1

201719476

發明摘要

※申請案號：105137495

※申請日：105 年 11 月 16 日　　※IPC 分類：*G06F 21/30* (2013.01)
H04L 9/32 (2006.01)

【發明名稱】(中文/英文)

一種在設備之間進行授權的方法和裝置

【中文】

在設備之間進行授權的方法的裝置。方法包括授權過程，該授權過程包括：在第一設備的 TEE 端生成並加密授權信息，在第一設備的 REE 端將經加密的授權信息傳輸到第二設備，在第二設備的 REE 端接收經加密的授權信息，在第二設備的 TEE 端解密並驗證經加密的授權信息，在第二設備存儲該授權信息。

【英文】

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

發明專利說明書

(本申請書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

一種在設備之間進行授權的方法和裝置

【技術領域】

本發明的實施例涉及在設備之間進行授權的方法和裝置。

【先前技術】

授權設備向被授權設備進行授權，從而被授權設備可以代理授權設備進行授權的操作，例如執行授權設備指定的功能、獲取授權設備指定的資源。

目前，授權設備通過伺服器向被授權設備進行授權。由於授權過程涉及伺服器，授權設備在進行授權前需要向伺服器發送申請，然後由伺服器向被授權設備推送授權信息。這會降低授權效率，導致較高成本。另一方面，由於授權過程涉及伺服器，授權信息必須經過網路傳輸，這將降低授權的安全性，而且這還要求被授權設備線上才能接收推送的授權信息。另外，授權設備的不安全的作業系統也會導致授權信息處於風險。

【發明內容】

一種在設備之間進行授權的方法，該方法包括授權過

程，該授權過程包括：在第一設備的 TEE 端生成並加密授權信息，在第一設備的 REE 端將經加密的授權信息傳輸到第二設備，在第二設備的 REE 端接收經加密的授權信息，在第二設備的 TEE 端解密並驗證經加密的授權信息，在第二設備存儲該授權信息。

在設備之間進行授權的裝置，其包括授權過程裝置，該授權裝置包括：用於在第一設備的 TEE 端生成並加密授權信息的裝置，用於在第一設備的 REE 端將經加密的授權信息傳輸到第二設備的裝置，用於在第二設備的 REE 端接收經加密的授權信息的裝置，用於在第二設備的 TEE 端解密並驗證經加密的授權信息的裝置，用於在第二設備存儲該授權信息的裝置。

本發明的優勢包括：設備間的授權不限於聯網設備與伺服器端的認證；設備授權信息的傳輸、當地語系化存儲的安全通過結合 TEE 安全技術方案得到保障；支援傳統的伺服器認證方式。

當結合附圖閱讀以下描述時也將理解本發明的實施例的其它特徵和優勢，其中附圖借助於實例示出了本發明的實施例的原理。

【圖式簡單說明】

圖 1 是根據本發明實施例的在設備之間進行授權的示意圖。

圖 2 是根據本發明實施例的在設備之間進行授權的流

程圖。

圖 3 是根據本發明實施例的在設備之間進行授權的流程圖。

【實施方式】

在下文中，將結合實施例描述本發明的原理。應當理解的是，給出的實施例只是為了本領域技術人員更好地理解並且實踐本發明，而不是限制本發明的範圍。例如，本說明書中包含許多具體的實施細節不應被解釋為對發明的範圍或可能被要求保護的範圍的限制，而是應該被視為特定於實施例的描述。例如，在各實施例的上下文描述的特徵可被組合在單一實施例中來實施。在單一實施例的上下文中描述的特可在多個實施例來實施。

圖 1 是根據本發明實施例的在設備之間進行授權的示意圖。圖 1 示出了授權設備、被授權設備、伺服器。在該實施例中，伺服器是可選的。授權過程和執行授權操作可以僅通過授權設備和被授權設備之間的交互完成。授權設備和被授權設備各自能夠運行可信執行環境 TEE（Trusted Execution Environment）和多媒體執行環境 REE（Rich Execution Environment）下。TEE 技術能夠為諸如移動通信終端等智慧終端機提供受到硬體隔離保護的作業系統。TEE 獨立於 REE（例如，Android 作業系統），並執行與安全相關的應用。智慧終端機上與安全相關的敏感操作將在 TEE 中執行，而除安全應用以外的其它應用在 REE 中

執行。如圖所示，授權設備和被授權設備各自在 TEE 中設置有可信存儲單元、授權信息驗證單元、授權信息生成單元，以及在 REE 中設置有 TEE 代理單元。

在授權設備中，授權信息生成單元中可以根據使用者的指令生成授權信息。授權信息可以包括授權的操作、時間、地點或者設備 ID。在一個實例中，授權信息可以包括授權信息生成時的時間和地點。在另一個實例中，授權信息可以進一步限定授權的操作，例如授權的操作可以發送的時間和地點。授權信息驗證單元用於驗證授權信息。可信存儲單元用於在 TEE 下安全存儲授權信息。TEE 代理單元，處於 REE 下，用於輔助與被授權設備之間的信息傳輸。TEE 代理單元例如可以使用移動網路、藍牙、紅外線、近場通信與被授權設備的 REE 下的 TEE 代理單元通信。可以理解的是，被授權設備也可以包括類似的單元以便作為扮演授權設備的角色。

圖 1 中，可選的伺服器可以包括授權信息驗證單元，在被授權設備與授權設備無法完成點對點通信時用於補充驗證授權信息。

在一個實例中，授權設備通過 REE 下的 TEE 代理單元向被授權設備發送在 TEE 下加密的授權信息。被授權設備通過 REE 下的 TEE 代理單元接收該加密的授權信息，並且在 TEE 下解密並且驗證該授權信息。被解密並驗證通過的授權信息被存儲在被授權設備的可信存儲單元中。之後，被授權設備將可以根據該授權信息代理授權設

備執行被授權的操作。由此，在保證安全的前提下,可以提高設備之間的授權與代理的效率。

圖 2 是根據本發明實施例的在設備之間進行授權的流程圖。該實施例示出在設備之間進行授權的方法的授權過程。該授權過程包括：

步驟 201：在第一設備的 TEE 端生成並加密授權信息；

步驟 202：在第一設備的 REE 端將經加密的授權信息傳輸到第二設備；

步驟 203：該步驟是可選的，在該步驟中判斷是否將授權信息備份到伺服器；

當在步驟 203 中判斷不將授權信息備份到伺服器時，進入步驟 204：在該步驟中在在第二設備的 REE 端接收經加密的授權信息；

步驟 205：在第二設備的 TEE 端解密並驗證經加密的授權信息；

步驟 206：在第二設備存儲該授權信息，至此作為授權的設備的第一設備完成了對於作為被授權設備的第二設備的授權；

當在步驟 203 中判斷將授權信息備份到伺服器時，進入步驟 207：在該步驟中從第一設備將經加密的授權信息發送並存儲到伺服器；

步驟 208：在伺服器解密並且驗證經加密的授權信息；

步驟 209：在伺服器存儲經驗證的授權信息，至此完成授權信息在伺服器的備份。

在一個實例中，在第一設備的 TEE 端使用私密金鑰對授權信息進行簽名，在第二設備的 TEE 端使用公開金鑰解密並驗證經加密的授權信息。

在一個實例中，授權信息包括授權操作，並且還包括以下一個或多個：進行授權操作的時間、地點、設備 ID。

圖 3 是根據本發明實施例的在設備之間進行授權的流程圖。該實施例示出在設備之間進行授權的方法的授權操作的過程。該進行授權操作的過程包括：

步驟 301：從第一設備向第二設備發送請求，請求第二設備代理第一設備進行授權操作，

步驟 302：在第二設備的 REE 端接收該請求，

步驟 303：在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給第一設備，

步驟 304：在第一設備的 REE 端接收經加密的授權信息，

步驟 305：在第一設備的 TEE 端解密並驗證經加密的授權信息，

步驟 306：在驗證成功後，在第一設備響應來自第二設備的授權操作。例如，第一設備可以根據來自第二設備的請求進行相應的操作。

在一個實例中，該請求包括設備 ID。

在一個實例中，在第二設備的 TEE 端使用公開金鑰加密授權信息，在第一設備的 TEE 端使用私密金鑰解密並驗證經加密的授權信息。

在一個實例中，該進行授權操作的過程還包括：在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給伺服器，在第一設備的 TEE 端解密並驗證經加密的授權信息，在驗證成功後，通過伺服器通知第一設備響應來自第二設備的授權操作。

在本發明的上述實施例中，所述第一設備和所述第二設備是移動通信終端。

在本發明的上述實施例中，使用以下方式的一種在第一設備的 REE 端和第二設備的 REE 端之間通信：移動網路、藍牙、紅外線、近場通信。

圖 2 和圖 3 所示的各個框可被視為方法步驟、和/或被視為由於運行電腦程式代碼而導致的操作、和/或被視為構建為實施相關功能的多個耦合的邏輯電路元件。儘管操作按特定的順序在圖中被描繪，但這不應被理解為要求按照所示的特定順序或按依次順序來執行這些操作，或要求所有例示的操作被執行，以達到理想的結果。在某些情況下，多工並行處理可能是有利的。

以下描述在設備之間進行授權的裝置，其包括授權過程裝置，該授權裝置包括：用於在第一設備的 TEE 端生成並加密授權信息的裝置，用於在第一設備的 REE 端將經加密的授權信息傳輸到第二設備的裝置，用於在第二設

備的 REE 端接收經加密的授權信息的裝置，用於在第二設備的 TEE 端解密並驗證經加密的授權信息的裝置，用於在第二設備存儲該授權信息的裝置。

在一個實施例中，該授權裝置還包括：用於從第一設備將經加密的授權信息發送並存儲到伺服器的裝置。用於在第一設備的 TEE 端使用私密金鑰對授權信息進行簽名的裝置，用於在第二設備的 TEE 端使用公開金鑰解密並驗證經加密的授權信息的裝置。

在一個實施例中，授權信息包括授權操作，並且還包括以下一個或多個：進行授權操作的時間、地點、設備 ID。

在一個實施例中，該裝置還包括進行授權操作的裝置，該進行授權操作的裝置包括：用於從第一設備向第二設備發送請求的裝置，請求第二設備代理第一設備進行授權操作，用於在第二設備的 REE 端接收該請求的裝置，用於在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給第一設備的裝置，用於在第一設備的 REE 端接收經加密的授權信息的裝置，用於在第一設備的 TEE 端解密並驗證經加密的授權信息的裝置，用於在驗證成功後，在第一設備響應來自第二設備的授權操作的裝置。

在一個實施例中，該請求包括設備 ID。

在一個實施例中，該裝置還包括：用於在第二設備的 TEE 端使用公開金鑰加密授權信息的裝置，用於在第一設

備的 TEE 端使用私密金鑰解密並驗證經加密的授權信息的裝置。

在一個實施例中，該進行授權操作的裝置還包括：用於在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給伺服器的裝置，用於在第一設備的 TEE 端解密並驗證經加密的授權信息的裝置，用於在驗證成功後，通過伺服器通知第一設備響應來自第二設備的授權操作的裝置。

示例性實施例可在硬體、軟體或其組合中來實施。例如，本發明的某些方面可在硬體中實施，而其它方面則可在軟體中實施。儘管本發明的示例性實施例的方面可被示出和描述為框圖、流程圖，但很好理解的是，這裡描述的這些裝置、或方法可在作為非限制性實例的系統中被實現為功能模組。此外，上述裝置不應被理解為要求在所有的實施例中進行這種分離，而應該被理解為所描述的程式元件和系統通常可以被集成在單一的軟體產品中或打包成多個軟體產品。

相關領域的技術人員當結合附圖閱讀前述說明書時，對本發明的前述示例性實施例的各種修改和變形對於相關領域的技術人員會變得明顯。因此，本發明的實施例不限於所公開的特定實施例，並且變形例和其它實施例意在涵蓋在所附權利要求的範圍內。

【符號說明】

201、202、203、204、205、206、207、208、209、301、302、303、304、305、306：步驟

申請專利範圍

1. 一種在設備之間進行授權的方法，該方法包括授權過程，該授權過程包括：

在第一設備的 TEE 端生成並加密授權信息，

在第一設備的 REE 端將經加密的授權信息傳輸到第二設備，

在第二設備的 REE 端接收經加密的授權信息，

在第二設備的 TEE 端解密並驗證經加密的授權信息，

在第二設備存儲該授權信息。

2. 如申請專利範圍第 1 項所述的方法，其中，該授權過程還包括：

從第一設備將經加密的授權信息發送並存儲到伺服器。

3. 如申請專利範圍第 1 項所述的方法，其中，

在第一設備的 TEE 端使用私密金鑰對授權信息進行簽名，

在第二設備的 TEE 端使用公開金鑰解密並驗證經加密的授權信息。

4. 如申請專利範圍第 1 項所述的方法，其中，

授權信息包括授權操作，並且還包括以下一個或多個：進行授權操作的時間、地點、設備 ID。

5. 如申請專利範圍第 1 項所述的方法，其中，該方法還包括進行授權操作的過程，該進行授權操作的過程包

括：

從第一設備向第二設備發送請求，請求第二設備代理第一設備進行授權操作，

在第二設備的 REE 端接收該請求，

在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給第一設備，

在第一設備的 REE 端接收經加密的授權信息，

在第一設備的 TEE 端解密並驗證經加密的授權信息，

在驗證成功後，在第一設備響應來自第二設備的授權操作。

6. 如申請專利範圍第 5 項所述的方法，其中，

該請求包括設備 ID。

7. 如申請專利範圍第 5 項所述的方法，其中，

在第二設備的 TEE 端使用公開金鑰加密授權信息，

在第一設備的 TEE 端使用私密金鑰解密並驗證經加密的授權信息。

8. 如申請專利範圍第 5 項所述的方法，其中，該進行授權操作的過程還包括：

在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給伺服器，

在第一設備的 TEE 端解密並驗證經加密的授權信息，

在驗證成功後，通過伺服器通知第一設備響應來自第

二設備的授權操作。

9. 如申請專利範圍第 1 至 8 項中任意一項所述的方法，其中，所述第一設備和所述第二設備是移動通信終端。

10. 如申請專利範圍第 1 至 8 項中任意一項所述的方法，其中，使用以下方式的一種在第一設備的 REE 端和第二設備的 REE 端之間通信：移動網路、藍牙、紅外線、近場通信。

11. 一種在設備之間進行授權的裝置，授權過程裝置，該授權裝置包括：

用於在第一設備的 TEE 端生成並加密授權信息的裝置，

用於在第一設備的 REE 端將經加密的授權信息傳輸到第二設備的裝置，

用於在第二設備的 REE 端接收經加密的授權信息的裝置，

用於在第二設備的 TEE 端解密並驗證經加密的授權信息的裝置，

用於在第二設備存儲該授權信息的裝置。

12. 如申請專利範圍第 11 項所述的裝置，其中，該授權裝置還包括：

用於從第一設備將經加密的授權信息發送並存儲到伺服器的裝置。

13. 如申請專利範圍第 11 項所述的裝置，其中，

用於在第一設備的 TEE 端使用私密金鑰對授權信息進行簽名的裝置，

用於在第二設備的 TEE 端使用公開金鑰解密並驗證經加密的授權信息的裝置。

14. 如申請專利範圍第 11 項所述的裝置，其中，

授權信息包括授權操作，並且還包括以下一個或多個：進行授權操作的時間、地點、設備 ID。

15. 如申請專利範圍第 11 項所述的裝置，其中，該裝置還包括進行授權操作的裝置，該進行授權操作的裝置包括：

用於從第一設備向第二設備發送請求的裝置，請求第二設備代理第一設備進行授權操作，

用於在第二設備的 REE 端接收該請求的裝置，

用於在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給第一設備的裝置，

用於在第一設備的 REE 端接收經加密的授權信息的裝置，

用於在第一設備的 TEE 端解密並驗證經加密的授權信息的裝置，

用於在驗證成功後，在第一設備響應來自第二設備的授權操作的裝置。

16. 如申請專利範圍第 15 項所述的裝置，其中，

該請求包括設備 ID。

17. 如申請專利範圍第 15 項所述的裝置，其中，還

包括：

用於在第二設備的 TEE 端使用公開金鑰加密授權信息的裝置，

用於在第一設備的 TEE 端使用私密金鑰解密並驗證經加密的授權信息的裝置。

18. 如申請專利範圍第 15 項所述的方法，其中，該進行授權操作的裝置還包括：

用於在第二設備的 TEE 端加密授權信息，並通過 REE 端將經加密的授權信息發送給伺服器的裝置，

用於在第一設備的 TEE 端解密並驗證經加密的授權信息的裝置，

用於在驗證成功後，通過伺服器通知第一設備響應來自第二設備的授權操作的裝置。

圖式

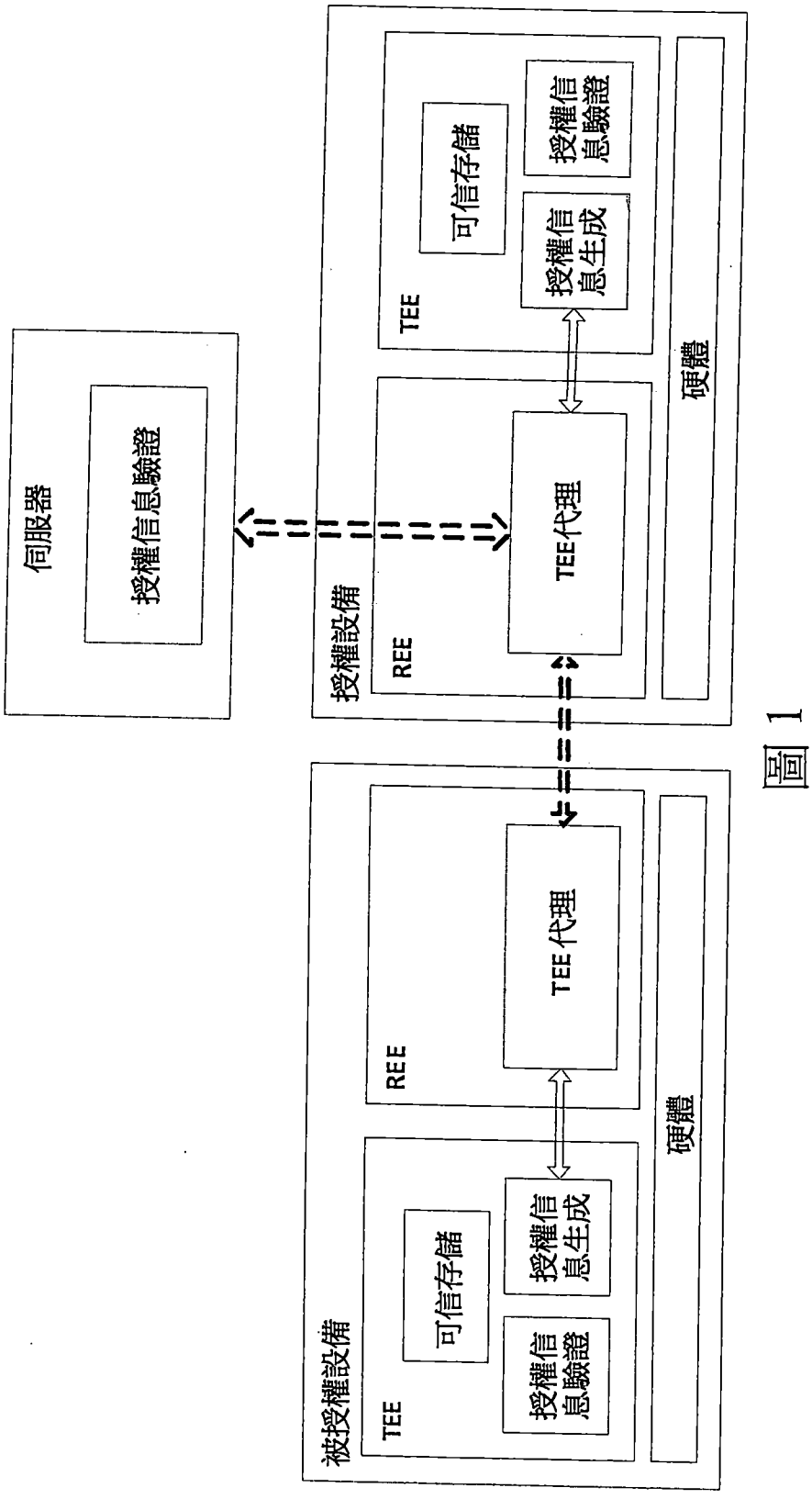
伺服器
授權信息驗證
授權設備
TEE
可信存儲
授權信息驗證
授權信息生成
REE
TEE代理
硬體
被授權設備
TEE
可信存儲
授權信息驗證
授權信息生成
REE
TEE代理
硬體

圖 1

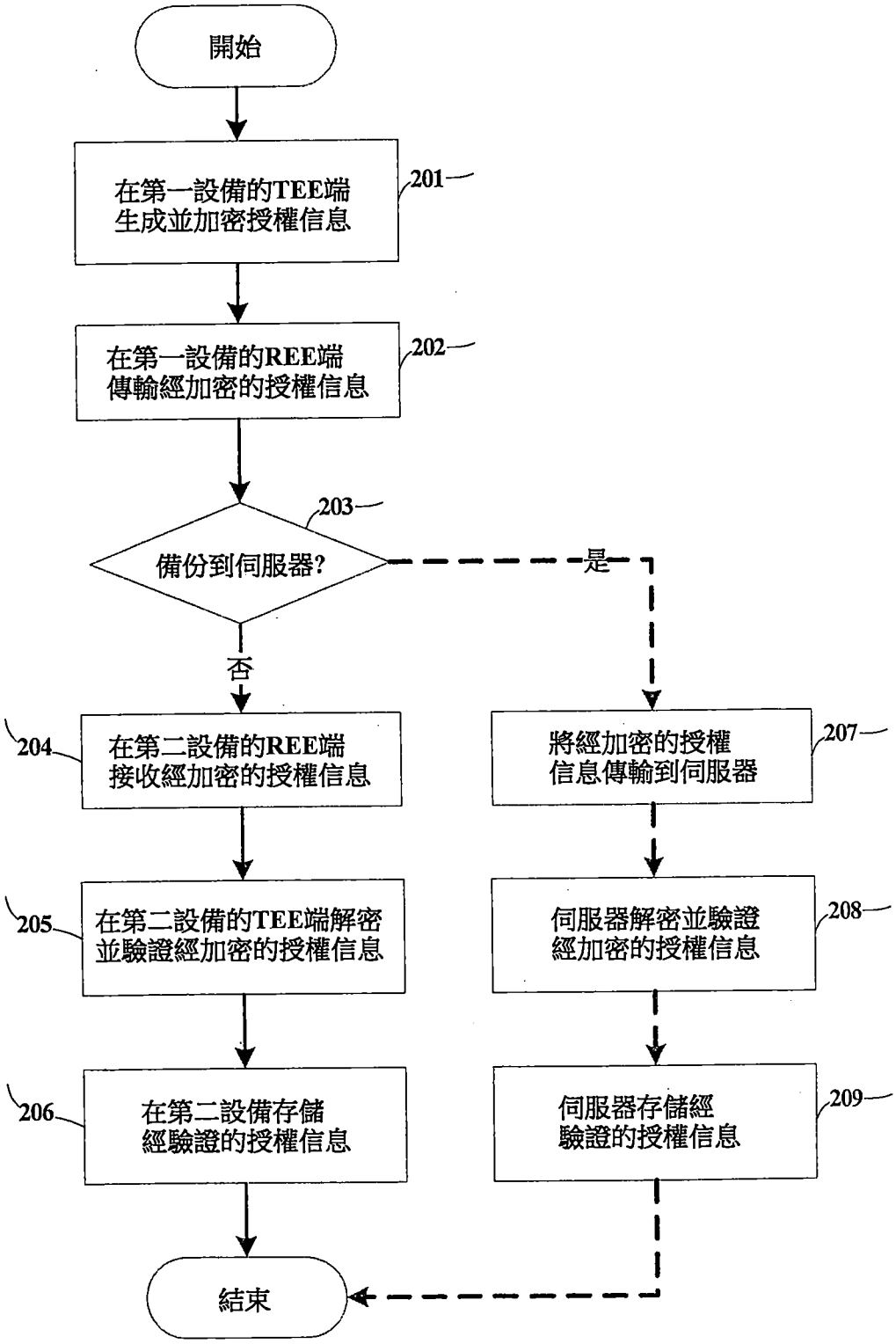
開始
在第一設備的TEE端
生成並加密授權信息
201
在第一設備的REE端
傳輸經加密的授權信息
202
203
備份到伺服器?
是
否
204
在第二設備的REE端
接收經加密的授權信息
207
將經加密的授權
信息傳輸到伺服器
205
在第二設備的TEE端解密
並驗證經加密的授權信息
208
伺服器解密並驗證
經加密的授權信息
206
在第二設備存儲
經驗證的授權信息
209
伺服器存儲經
驗證的授權信息
結束

圖 2

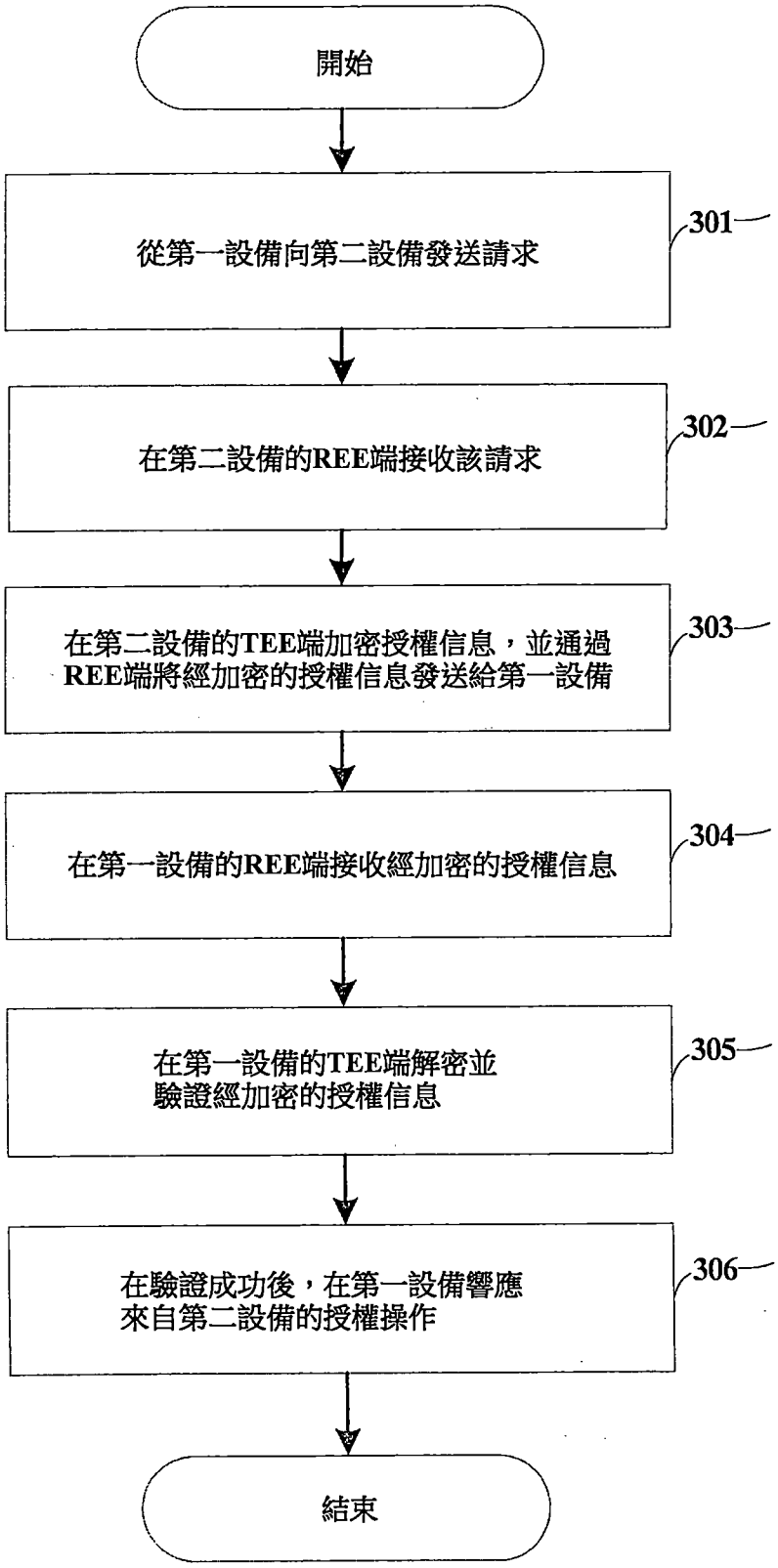
開始
從第一設備向第二設備發送請求
301
在第二設備的REE端接收該請求
302
在第二設備的TEE端加密授權信息，並通過REE端將經加密的授權信息發送給第一設備
303
在第一設備的REE端接收經加密的授權信息
304
在第一設備的TEE端解密並驗證經加密的授權信息
305
在驗證成功後，在第一設備響應來自第二設備的授權操作
306
結束

圖 3