201800984

(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 201800984 A

(43)公開日： 中華民國 107 (2018) 年 01 月 01 日

(21)申請案號：106117693 (22)申請日： 中華民國 106 (2017) 年 05 月 26 日

(51)Int. Cl.： *G06Q10/00 (2012.01)* *G06Q40/00 (2012.01)*

(30)優先權：2016/06/22 中國大陸 201610455469.3

(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：姚翔 (CN) ；嚴翔翔 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：8 項 圖式數：1 共 14 頁

(54)名稱

權益文件管理方法

(57)摘要

本發明提出了權益文件管理方法，所述方法包括：生成 M 組公私密金鑰對；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述 M 組公私密金鑰對中選出的 N 組公私密金鑰對，所述 N 組公私密金鑰對中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益；基於所述 N 組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述 N 組公私密金鑰對中的所有公開金鑰；所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述 N 組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益。本發明所公開的權益文件管理方法能夠對權益文件進行登記並且可由第三方進行驗證以及具有高的安全性。

指定代表圖：

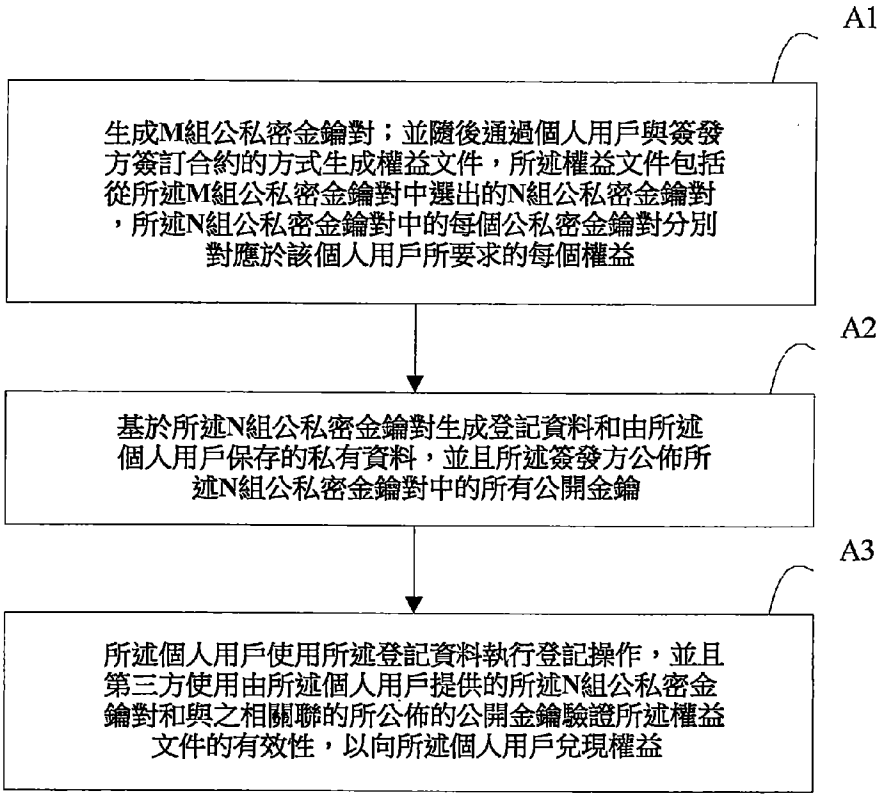
A1
生成M組公私密金鑰對；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述M組公私密金鑰對中選出的N組公私密金鑰對，所述N組公私密金鑰對中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益
A2
基於所述N組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述N組公私密金鑰對中的所有公開金鑰
A3
所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述N組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益

圖 1

201800984

發明摘要

※申請案號：106117693

※申請日：106 年 05 月 26 日　　※IPC 分類：G06Q 10/00 (2012.01)
G06Q 40/00 (2012.01)

【發明名稱】(中文/英文)

權益文件管理方法

【中文】

本發明提出了權益文件管理方法，所述方法包括：生成 M 組公私密金鑰對；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述 M 組公私密金鑰對中選出的 N 組公私密金鑰對，所述 N 組公私密金鑰對中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益；基於所述 N 組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述 N 組公私密金鑰對中的所有公開金鑰；所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述 N 組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益。本發明所公開的權益文件管理方法能夠對權益文件進行登記並且可由第三方進行驗證以及具有高的安全性。

【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

（本說明書格式、順序，請勿任意更動）

【發明名稱】(中文/英文)

權益文件管理方法

【技術領域】

[0001] 本發明涉及文件管理方法，更具體地，涉及權益文件管理方法。

【先前技術】

[0002] 目前，隨著電腦和網路應用的日益廣泛以及不同領域的業務種類的日益豐富，對權益文件（即用於指示所屬人的權益的文件，例如金融領域中的票據文件）進行管理（例如對權益文件進行登記和驗證）變得越來越重要。

[0003] 在現有的技術方案中，通常由權益文件的所有人（即用戶個人）負責管理物理實體形式或電子形式的權益文件，並且由權益文件的簽發方負責權益文件的真偽驗證。

[0004] 然而，上述現有的技術方案存在如下問題：由於僅通過所有人自身保管權益文件而無有效的登記方式，故存在被非法盜用的潛在隱患，安全性較低，並且由於僅權益文件的簽發方能夠驗證權益文件的有效性，故使用方式和場景受限，由此導致權益文件的使用效率較低。

[0005] 因此，存在如下需求：提供能夠對權益文件進行登記並且可由第三方進行驗證以及具有高的安全性的權益文件管理方法。

【發明內容】

[0006] 為了解決上述現有技術方案所存在的問題，本發明提出了能夠對權益文件進行登記並且可由第三方進行驗證以及具有高的安全性的權益文件管理方法。

[0007] 本發明的目的是通過以下技術方案實現的：

一種權益文件管理方法，所述權益文件管理方法包括下列步驟：

（A1）生成 M 組公私密金鑰對$(P_1, S_1)\cdots(P_M, S_M)$，M 是大於 1 的正整數；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述 M 組公私密金鑰對$(P_1, S_1)\cdots(P_M, S_M)$中選出的 N 組公私密金鑰對$(P_1, S_1)\cdots(P_N, S_N)$，其中 N 是小於 M 的正整數，所述 N 組公私密金鑰對$(P_1, S_1)\cdots(P_N, S_N)$中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益；

（A2）基於所述 N 組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述 N 組公私密金鑰對中的所有公開金鑰 $P_1\cdots P_N$；

（A3）所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述 N 組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益

文件的有效性，以向所述個人用戶兌現權益。

[0008] 在上面所公開的方案中，優選地，所述步驟（A2）進一步包括：

（1）計算所述權益文件的摘要值 H，其中，如果所生成的權益文件是物理實體形式的文件，則對其進行拍照並隨之計算照片的摘要值以及將所計算的摘要值用作所述權益文件的摘要值 H，而如果所生成的權益文件是電子文件，則直接計算該電子文件的摘要值以及將所計算的摘要值用作所述權益文件的摘要值 H；

（2）將所述權益文件的基本資訊以及可驗證的個人用戶資訊 K 加上所述 N 組公私密金鑰對中的私密金鑰 S_i（i=1…N）記錄為 T_i，並隨之計算 T_i 和 H 合併後的摘要值 H_i；

（3）所述個人用戶將 H 和（H_i，K）（i=1…N）作為登記資料來執行登記操作，並且將所述照片以及 T_i 作為私有資料進行保存。

[0009] 在上面所公開的方案中，優選地，所述步驟（A3）進一步包括：以如下方式驗證並使用所述權益文件：當需要使用所述權益文件所指示的某個權益時，所述個人用戶向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i，所述第三方隨之驗證該 S_i 是否是所述簽發方公佈的對應的公開金鑰 P_i 的私密金鑰以及基於對應的已登記資訊驗證該權益文件的當前可用性，並且如果驗證該 S_i 是所述簽發方公佈的對應的公開金鑰 P_i 的私密金

鑰並且該權益文件當前可用，則所述 S_i 所指示的權益有效，所述第三方隨之兌現該權益。

[0010] 在上面所公開的方案中，優選地，所述步驟（A3）進一步包括：以如下方式基於已登記資訊驗證權益文件的當前可用性：在公共可信網路上檢索與 S_i 相關的權益文件登記資訊，如果該權益文件存在登記資訊且未被轉讓，則該權益文件當前可用。

[0011] 在上面所公開的方案中，優選地，所述個人用戶經由公共可信網路向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i。

[0012] 在上面所公開的方案中，優選地，所述 S_i（$i=1\cdots N$）在由所述個人用戶公佈前被保密，並且所述簽發方無法將其重複發放。

[0013] 在上面所公開的方案中，優選地，所述權益文件中指示的權益能夠通過出讓方將 H_i 和 S_i 移交給受讓方的方式而被轉移，並且所述受讓方能夠重新登記所述 H_i 與受讓方的個人資訊合併後的摘要值 H_i'。

[0014] 在上面所公開的方案中，優選地，所述權益文件包含指示該權益文件所確定的權益是否能夠轉讓的專案。

[0015] 本發明所公開的權益文件管理方法具有以下優點：能夠對權益文件進行登記並且可由第三方進行驗證，由此具有高的安全性。

【圖式簡單說明】

[0016] 結合圖式，本發明的技術特徵以及優點將會被本領域技術人員更好地理解，其中：

圖 1 是根據本發明的實施例的權益文件管理方法的流程圖。

【實施方式】

[0017] 圖 1 是根據本發明的實施例的權益文件管理方法的流程圖。如圖 1 所示，本發明所公開的權益文件管理方法包括下列步驟：（A1）生成 M 組公私密金鑰對 $(P_1, S_1)\cdots(P_M, S_M)$，M 是大於 1 的正整數；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述 M 組公私密金鑰對 $(P_1, S_1)\cdots(P_M, S_M)$ 中選出的 N 組公私密金鑰對 $(P_1, S_1)\cdots(P_N, S_N)$，其中 N 是小於 M 的正整數，所述 N 組公私密金鑰對 $(P_1, S_1)\cdots(P_N, S_N)$ 中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益；（A2）基於所述 N 組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述 N 組公私密金鑰對中的所有公開金鑰 $P_1\cdots P_N$（即簽發方公佈的公開金鑰相當於一個挑戰，每一個公開金鑰對應一個附屬權益，而對應的私密金鑰則是擁有此權益的權利證明）；（A3）所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述 N 組公私密金鑰對和與之相關聯的所公佈的公開

金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益（例如所有權、保修權等等）。

[0018] 優選地，在本發明所公開的權益文件管理方法中，所述步驟（A2）進一步包括：（1）計算所述權益文件的摘要值 H，其中，如果所生成的權益文件是物理實體形式的文件（例如，紙質文件），則對其進行拍照並隨之計算照片的摘要值以及將所計算的摘要值用作所述權益文件的摘要值 H，而如果所生成的權益文件是電子文件，則直接計算該電子文件的摘要值以及將所計算的摘要值用作所述權益文件的摘要值 H；（2）將所述權益文件的基本資訊（例如標題、日期等等）以及可驗證的個人用戶資訊 K（例如身份證號碼、手機號碼、郵寄地址等等）加上所述 N 組公私密金鑰對中的私密金鑰 S_i（i=1…N）記錄為 T_i，並隨之計算 T_i 和 H 合併後的摘要值 H_i；（3）所述個人用戶將 H 和（H_i，K）（i=1…N）作為登記資料來執行登記操作，並且將所述照片以及 T_i 作為私有資料進行保存。

[0019] 優選地，在本發明所公開的權益文件管理方法中，所述步驟（A3）進一步包括：以如下方式驗證並使用所述權益文件：當需要使用所述權益文件所指示的某個權益時，所述個人用戶向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i，所述第三方隨之驗證該 S_i 是否是所述簽發方公佈的對應的公開金鑰 P_i 的私密金鑰以及基於對應的已登記資訊驗證該權益文件的當前可用

性，並且如果驗證該 S_i 是所述簽發方公佈的對應的公開金鑰 P_i 的私密金鑰並且該權益文件當前可用，則所述 S_i 所指示的權益有效，所述第三方隨之兌現該權益。

[0020] 優選地，在本發明所公開的權益文件管理方法中，所述步驟（A3）進一步包括：以如下方式基於已登記資訊驗證權益文件的當前可用性：在公共可信網路上檢索與 S_i 相關的權益文件登記資訊，如果該權益文件存在登記資訊且未被轉讓，則該權益文件當前可用。

[0021] 優選地，在本發明所公開的權益文件管理方法中，所述個人用戶經由公共可信網路向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i。

[0022] 優選地，在本發明所公開的權益文件管理方法中，所述 S_i（$i=1\cdots N$）在由所述個人用戶公佈前被保密，並且所述簽發方無法將其重複發放（因為實際擁有者可以舉證自己曾經登記過的 H_i,證明 S_i 的所有權，當有兩個相同的登記內容發生時，以首先登記的為准，並且當難以仲裁時，可以公佈照片來確認所有權）。

[0023] 優選地，在本發明所公開的權益文件管理方法中，所述權益文件中指示的權益能夠通過出讓方將 H_i 和 S_i 移交給受讓方的方式而被轉移，並且所述受讓方能夠重新登記所述 H_i 與受讓方的個人資訊合併後的摘要值 H_i'（當受讓方使用權益時，與出讓方使用權益的方法一致，並且由於轉讓過程已經登記在 H_i' 當中，故出讓方若想再次使用或出讓該權益，則無法實施）。

[0024] 優選地，在本發明所公開的權益文件管理方法中，所述權益文件包含指示該權益文件所確定的權益是否能夠轉讓的專案。

[0025] 由上可見，本發明所公開的權益文件管理方法具有下列優點：能夠對權益文件進行登記並且可由第三方進行驗證，由此具有高的安全性。

[0026] 儘管本發明是通過上述的優選實施方式進行描述的，但是其實現形式並不局限於上述的實施方式。應該認識到：在不脫離本發明主旨和範圍的情況下，本領域技術人員可以對本發明做出不同的變化和修改。

申請專利範圍

1. 一種權益文件管理方法，所述權益文件管理方法包括下列步驟：

（A1）生成 M 組公私密金鑰對$(P_1, S_1)\cdots(P_M, S_M)$，M 是大於 1 的正整數；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述 M 組公私密金鑰對$(P_1, S_1)\cdots(P_M, S_M)$中選出的 N 組公私密金鑰對$(P_1, S_1)\cdots(P_N, S_N)$，其中 N 是小於 M 的正整數，所述 N 組公私密金鑰對$(P_1, S_1)\cdots(P_N, S_N)$中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益；

（A2）基於所述 N 組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述 N 組公私密金鑰對中的所有公開金鑰 $P_1\cdots P_N$；

（A3）所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述 N 組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益。

2. 根據請求項 1 所述的權益文件管理方法，其中，所述步驟（A2）進一步包括：

（1）計算所述權益文件的摘要值 H，其中，如果所生成的權益文件是物理實體形式的文件，則對其進行拍照並隨之計算照片的摘要值以及將所計算的摘要值用作所述權益文件的摘要值 H，而如果所生成的權益文件是電子文件，則直接計算該電子文件的摘要值以及將所計算的摘要

值用作所述權益文件的摘要值 H；

（2）將所述權益文件的基本資訊以及可驗證的個人用戶資訊 K 加上所述 N 組公私密金鑰對中的私密金鑰 S_i（i=1…N）記錄為 T_i，並隨之計算 T_i 和 H 合併後的摘要值 H_i；

（3）所述個人用戶將 H 和（H_i，K）（i=1…N）作為登記資料來執行登記操作，並且將所述照片以及 T_i 作為私有資料進行保存。

3. 根據請求項 2 所述的權益文件管理方法，其中，所述步驟（A3）進一步包括：以如下方式驗證並使用所述權益文件：當需要使用所述權益文件所指示的某個權益時，所述個人用戶向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i，所述第三方隨之驗證該 S_i 是否是所述簽發方公佈的對應的公開金鑰 P_i 的私密金鑰以及基於對應的已登記資訊驗證該權益文件的當前可用性，並且如果驗證該 S_i 是所述簽發方公佈的對應的公開金鑰 P_i 的私密金鑰並且該權益文件當前可用，則所述 S_i 所指示的權益有效，所述第三方隨之兌現該權益。

4. 根據請求項 3 所述的權益文件管理方法，其中，所述步驟（A3）進一步包括：以如下方式基於已登記資訊驗證權益文件的當前可用性：在公共可信網路上檢索與 S_i 相關的權益文件登記資訊，如果該權益文件存在登記資訊且未被轉讓，則該權益文件當前可用。

5. 根據請求項 4 所述的權益文件管理方法，其中，

所述個人用戶經由公共可信網路向相關的第三方公佈其所保存的與該權益相關聯的私密金鑰 S_i。

6. 根據請求項 5 所述的權益文件管理方法，其中，所述 S_i（$i=1\cdots N$）在由所述個人用戶公佈前被保密，並且所述簽發方無法將其重複發放。

7. 根據請求項 6 所述的權益文件管理方法，其中，所述權益文件中指示的權益能夠通過出讓方將 H_i 和 S_i 移交給受讓方的方式而被轉移，並且所述受讓方能夠重新登記所述 H_i 與受讓方的個人資訊合併後的摘要值 H_i'。

8. 根據請求項 7 所述的權益文件管理方法，其中，所述權益文件包含指示該權益文件所確定的權益是否能夠轉讓的專案。

圖 式

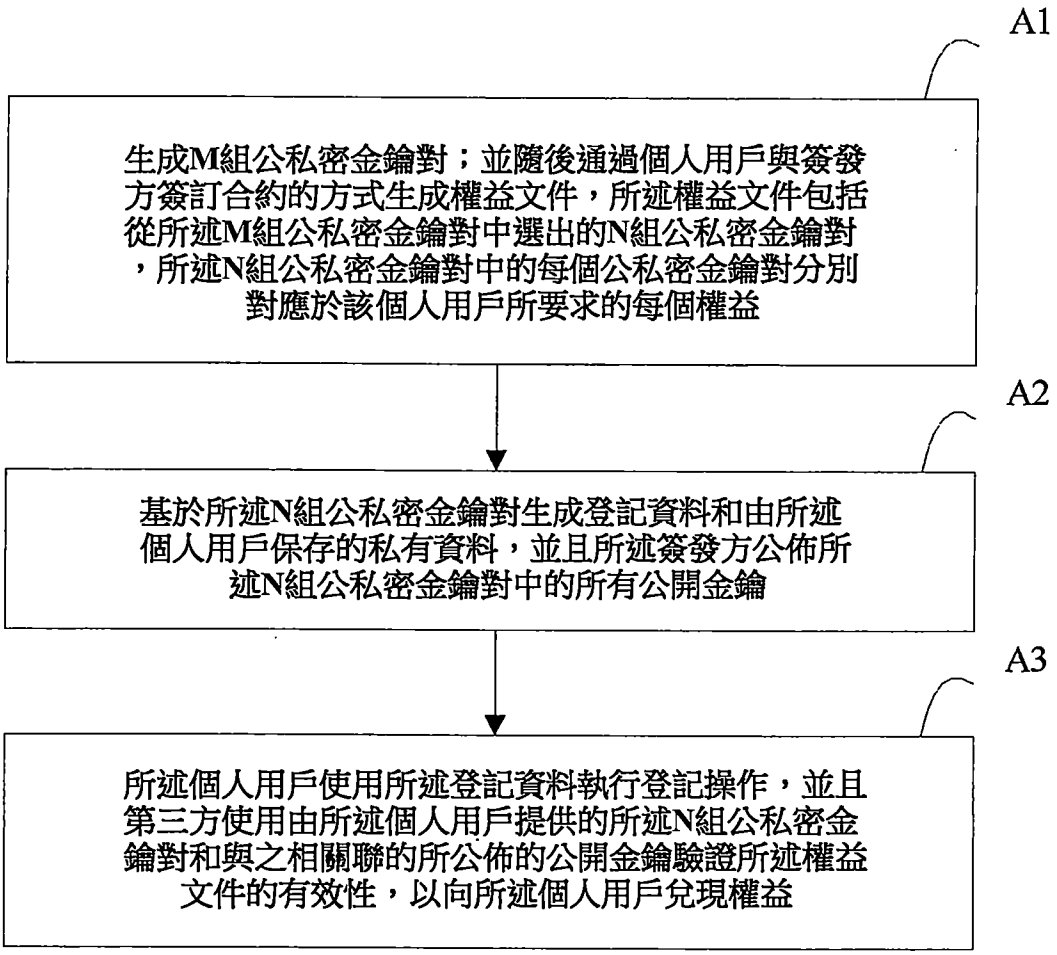
A1
生成M組公私密金鑰對；並隨後通過個人用戶與簽發方簽訂合約的方式生成權益文件，所述權益文件包括從所述M組公私密金鑰對中選出的N組公私密金鑰對，所述N組公私密金鑰對中的每個公私密金鑰對分別對應於該個人用戶所要求的每個權益
A2
基於所述N組公私密金鑰對生成登記資料和由所述個人用戶保存的私有資料，並且所述簽發方公佈所述N組公私密金鑰對中的所有公開金鑰
A3
所述個人用戶使用所述登記資料執行登記操作，並且第三方使用由所述個人用戶提供的所述N組公私密金鑰對和與之相關聯的所公佈的公開金鑰驗證所述權益文件的有效性，以向所述個人用戶兌現權益

圖 1