201734834

(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 201734834 A

(43)公開日： 中華民國 106 (2017) 年 10 月 01 日

(21)申請案號：106101731 (22)申請日： 中華民國 106 (2017) 年 01 月 18 日

(51)Int. Cl.： *G06F17/00 (2006.01)* *G06Q20/12 (2012.01)*
G06Q20/38 (2012.01)

(30)優先權：2016/03/15 中國大陸 201610147571.7

(71)申請人：阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)
香港

(72)發明人：范曉鋒 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：26 項 圖式數：16 共 56 頁

(54)名稱

網站登錄方法和裝置

(57)摘要

本發明提供一種網站登錄方法和裝置，其中方法包括：第一網站在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，第一許可證包括網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；第一網站根據設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，獲取該第一許可證對應的第二許可證；第一網站根據第一許可證中的網站標識，向第二網站發送無加密登錄請求，攜帶第三許可證，第三許可證中包括第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。本發明提高了由第一網站無加密登錄至第二網站的安全性。

指定代表圖：

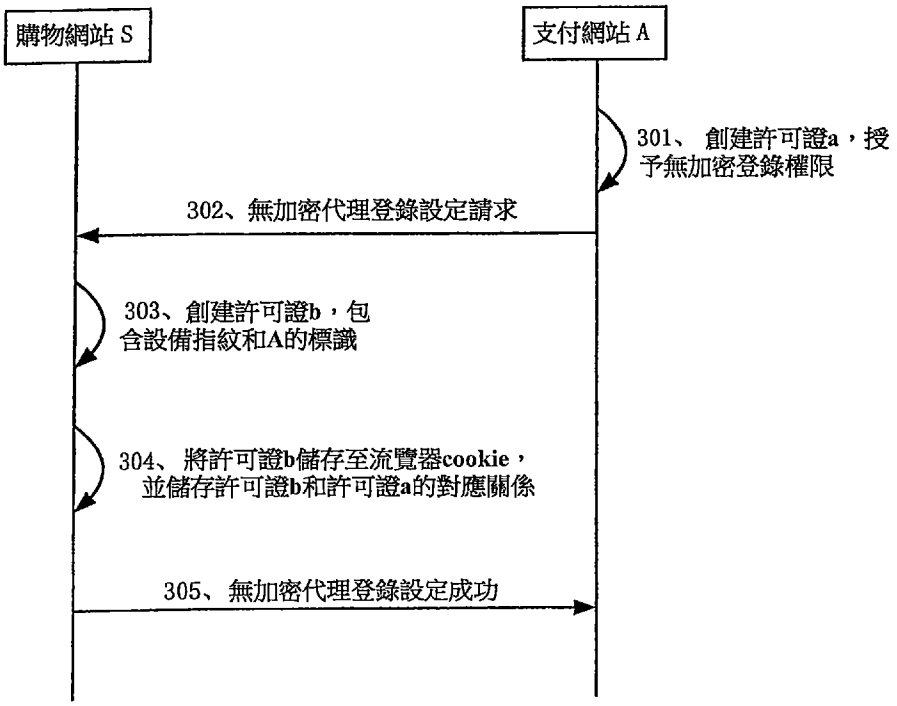
購物網站 S
支付網站 A
301、 創建許可證a，授予無加密登錄權限
302、無加密代理登錄設定請求
303、創建許可證b，包含設備指紋和A的標識
304、將許可證b儲存至流覽器cookie，並儲存許可證b和許可證a的對應關係
305、無加密代理登錄設定成功

圖 3

201734834

發明摘要

※申請案號：106101731

※申請日：106年01月18日　　※IPC分類：G06F 17/00 (2006.01)
G06Q 20/12 (2012.01)
G06Q 20/38 (2012.01)

【發明名稱】(中文/英文)

網站登錄方法和裝置

【中文】

本發明提供一種網站登錄方法和裝置，其中方法包括：第一網站在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，第一許可證包括網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；第一網站根據設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，獲取該第一許可證對應的第二許可證；第一網站根據第一許可證中的網站標識，向第二網站發送無加密登錄請求，攜帶第三許可證，第三許可證中包括第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。本發明提高了由第一網站無加密登錄至第二網站的安全性。

【英文】

【代表圖】

【本案指定代表圖】：第(3)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)

網站登錄方法和裝置

【技術領域】

本發明關於網路技術，特別關於一種網站登錄方法和裝置。

【先前技術】

使用者在上網過程中，經常遇到如下情況：用戶先通過流覽器訪問一個網站，為了完成某個操作流程，還需要從該網站再跳轉到另一個網站進行操作。比如，網上購物時，用戶通過流覽器訪問購物網站，該購物網站上展示待選擇購買的商品列表，當用戶選定商品要結算時，需要跳轉到支付網站進行付款。現有技術中，對於這種多網站間配合實現的操作流程，在進行網站跳轉時需要進行登錄，比如上述的例子中，由購物網站到支付網站時，還需要輸入支付網站的用戶名和密碼等登錄資訊，流程較為繁瑣。即使支付網站可以實現無加密登錄，不輸入登錄資訊即可直接跳轉到支付網站，但是這種無加密登錄方式的安全性就完全依賴支付網站，由於並不是所有支付網站都具有較高的自防護能力，部分網站無法保證無加密登錄的安全性，存在安全隱患。

【發明內容】

有鑑於此，本發明提供一種網站登錄方法和裝置，以使得在多網站間配合的場景下提高無加密登錄的安全性。

具體地，本發明是通過如下技術方案實現的：

第一方面，提供一種網站登錄方法，該方法用於由第一網站無加密代理登錄至第二網站；該方法包括：

該第一網站在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，該第一許可證包括該網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；

該第一網站根據該設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，則獲取該第一許可證對應的第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

該第一網站根據第一許可證中的網站標識，向該網站標識對應的第二網站發送無加密登錄請求，攜帶第三許可證，該第三許可證中包括該第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。

第二方面，提供一種網站登錄方法，該方法用於由第一網站無加密登錄至第二網站；該方法包括：

該第一網站在頁面顯示網站跳轉觸發標識，該網站跳轉觸發標識用於在選擇時觸發第一網站跳轉到包括供選擇

的多個第二網站的網站清單頁面；

回應於使用者對網站跳轉觸發標識的選擇，該第一網站跳轉至顯示該網站清單頁面中多個第二網站的其中一個第二網站的已登錄頁面。

第三方面，提供一種網站登錄方法，該方法用於由第一網站無加密登錄至第二網站；該方法包括：

該第二網站接收第一網站發送的無加密登錄請求，該無加密登錄請求攜帶第三許可證，該第三許可證中包括第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

該第二網站驗證該第二許可證成功時，執行無加密登錄。

第四方面，提供一種網站登錄裝置，該裝置應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置包括：

許可證獲取模組，用於在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，該第一許可證包括該網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；

許可證校驗模組，用於根據該設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，則獲取該第一許可證對應的第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪

問許可證；

無加密登錄模組，用於根據第一許可證中的網站標識，向該網站標識對應的第二網站發送無加密登錄請求，攜帶第三許可證，該第三許可證中包括該第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。

第五方面，提供一種網站登錄裝置，該裝置應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置包括：

標識顯示模組，用於在頁面顯示網站跳轉觸發標識，該標識用於在選擇時觸發第一網站跳轉到包括供選擇的多個第二網站的網站清單頁面；

頁面跳轉模組，用於回應於使用者對網站跳轉觸發標識的選擇，跳轉至顯示該網站清單頁面中多個第二網站的其中一個第二網站的已登錄頁面。

第六方面，提供一種網站登錄裝置，該裝置應用於第二網站，使得第一網站無加密代理登錄至第二網站；該裝置包括：

請求接收模組，用於接收第一網站發送的無加密登錄請求，該無加密登錄請求攜帶第三許可證，該第三許可證中包括第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

登錄執行模組，用於驗證該第二許可證成功時，執行無加密登錄。

本發明提供的網站登錄方法和裝置，通過在無加密代理登錄時，使得第一網站和第二網站均參與安全校驗，提高了由第一網站無加密登錄至第二網站的安全性。

【圖式簡單說明】

圖 1 是本發明一示例性實施例示出的一種支付網站登錄頁面示意圖；

圖 2 是本發明一示例性實施例示出的一種已登錄頁面示意圖；

圖 3 是本發明一示例性實施例示出的無加密代理登錄的設定流程；

圖 4 是本發明一示例性實施例示出的無加密代理登錄的取消流程；

圖 5 是本發明一示例性實施例示出的無加密代理登錄的應用流程；

圖 6 是本發明一示例性實施例示出的多網站顯示示意圖；

圖 7 是本發明一示例性實施例示出的中間網站顯示示意圖；

圖 8 是本發明一示例性實施例示出的中間網站的下層網站示意圖；

圖 9 是本發明一示例性實施例示出的一種登錄頁面示意圖；

圖 10 是本發明一示例性實施例示出的一種已登錄頁

面示意圖；

圖 11 是本發明一示例性實施例示出的一種網站登錄裝置的結構圖；

圖 12 是本發明一示例性實施例示出的另一種網站登錄裝置的結構圖；

圖 13 是本發明一示例性實施例示出的又一種網站登錄裝置的結構圖；

圖 14 是本發明一示例性實施例示出的又一種網站登錄裝置的結構圖；

圖 15 是本發明一示例性實施例示出的又一種網站登錄裝置的結構圖；

圖 16 是本發明一示例性實施例示出的又一種網站登錄裝置的結構圖。

【實施方式】

這裡將詳細地對示例性實施例進行說明，其示例表示在圖式中。下面的描述涉及圖式時，除非另有表示，不同圖式中的相同數字表示相同或相似的要素。以下示例性實施例中所描述的實施方式並不代表與本發明相一致的所有實施方式。相反，它們僅是與如所附權利要求書中所詳述的、本發明的一些方面相一致的裝置和方法的例子。

在很多網路應用中，都存在需要網站間配合實現的操作流程，這種網站間配合可以是，用戶先在一個網站進行操作，然後需要由該網站跳轉到另一個網站進行操作，才

能完成一次應用。常見的一種場景是網路購物，例如，使用者通過流覽器訪問購物網站，該購物網站上展示待選擇購買的商品列表，當用戶選定商品要結算時，需要跳轉到支付網站進行付款，即使用者的本次網路購物需要購物網站和支付網站的配合，進行這兩個網站間的跳轉。

有些網站為了方便用戶的應用體驗，可以提供無加密登錄，無加密登錄即允許使用者不輸入用戶名和密碼，而直接登錄自己在一個網站的帳戶。比如，在上述的網路購物的例子中，支付網站就可以設置為無加密登錄，這樣當用戶由購物網站向支付網站跳轉時，就不再需要輸入用戶名和密碼而直接登錄支付網站。但是，無加密登錄也不一定是安全的，如果只依賴支付網站保證無加密登錄的安全性，也是具有一定的安全風險。

為了提高安全性，本公開提供了一種網站登錄方法，該方法可以應用於網站間的跳轉登錄，比如，當用戶在購物網站向支付網站跳轉時，就可以使用本公開的方法登錄到支付網站。當然，本公開的方法並不限制於購物場景的例子，其他類似的網站間配合執行的流程中都可以使用該方法。

在如下對本公開的網站登錄方法的說明中，使用了一個概念詞“無加密代理登錄”，該詞語的使用是想說明，本公開的網站登錄方法也是要無加密登錄到跳轉網站，例如支付網站，但與通常的無加密登錄的區別在於，網站間跳轉所涉及到的兩個網站都參與了安全方面的校驗。比如，

在購物場景的例子中，由購物網站向支付網站跳轉，購物網站要執行安全校驗，支付網站也要進行安全校驗，才能最終無加密登錄支付網站，這是一種雙重授權的方式；並且，無加密代理登錄可以由購物網站自動跳轉到其中一個支付網站進行登錄（購物網站下可以連結多個支付網站），而不需要使用者選擇要無加密登錄哪個支付網站，相當於購物網站知道自己要選擇哪個支付網站去無加密登錄。

如下以購物網站（可以稱為第一網站）和支付網站（可以稱為第二網站）的應用例子，來說明本公開的網站登錄方法。其中，本公開的網站登錄方法的描述中，包括如何設定無加密代理登錄的過程、以及設定完成後如何執行無加密代理登錄的過程，這些過程都需要購物網站和支付網站之間的配合。

假設用戶在某購物網站進行購物，當用戶將所選定的商品放入購物車後，可以點擊“結算”按鈕，去進行結算和付款。該結算按鈕可以稱為網站跳轉觸發標識，該網站跳轉觸發標識的作用，可以是在該標識被使用者選擇時，將觸發購物網站跳轉到包括供選擇的多個支付網站的網站清單頁面，比如，該網站清單頁面可以顯示支付網站 A、支付網站 B、支付網站 C 等，用戶可以選擇使用何種支付方式。

假設使用者選擇了其中一種支付方式，本公開實施例中，購物網站接收到用戶對網站跳轉觸發的選擇後，可以

通過內嵌頁面的形式顯示使用者所選擇的支付網站的登錄頁面。需要說明的是，此時還未進行無加密代理登錄的設定，購物網站在使用者點擊結算按鈕時，仍然要顯示上面提到的網站清單頁面，並且當使用者選擇一個支付網站後，將顯示該支付網站的登錄頁面供使用者輸入用戶名和密碼，參見圖 1 所示的頁面顯示示例。

如圖 1 所示，用戶選擇的支付網站 A 的登錄頁面，可以是以內嵌頁面的形式顯示在購物網站的頁面中，當然也可以不以內嵌頁面的方式顯示，而是單獨顯示一個支付網站 A 的登錄頁面，在本發明的如下各個實施例中，涉及到網站跳轉的頁面顯示都以內嵌頁面的顯示形式來舉例，通過以內嵌頁面顯示可以方便使用者隨時切換至另一個支付網站。比如，當在購物網站的頁面中以內嵌頁面顯示支付網站 A 的登錄頁面時，與內嵌頁面同位於該購物網站頁面中顯示的還有支付網站 B 的選擇標識、支付網站 C 的選擇標識等。用戶不想登錄支付網站 A 時，可以方便的選擇支付網站 B 等其他網站。

接著仍以上面的支付網站 A 的登錄為例，具體實施中，可以是購物網站的頁面中包括一個內嵌 iframe，指向支付網站 A 的登錄頁面，url 中含有參數 container=S（S 表示購物網站），表示該支付網站 A 的登錄頁面是內嵌在 S 這個容器中。支付網站 A 的登錄頁面是由支付網站 A 載入，由伺服器傳輸至 S 運行所在的流覽器中的支付網站用戶端進行顯示。

需要注意的是，請繼續參見圖 1，支付網站 A 的登錄頁面中還顯示有“啟用無加密代理登錄”的選項，供使用者選擇是否啟用。如果使用者選擇了該選項，表明使用者想要實現在購物網站點擊結算按鈕後，自動跳轉至支付網站的已登錄頁面，該已登錄頁面可以參見圖 2 所示，相對於原有的使用者操作，使用者不再需要在網站清單頁面中選擇支付網站 A，也不再需要輸入圖 1 中的用戶名和密碼，而直接就進入到支付網站 A 的登錄成功之後的顯示頁面，進行付款確認。如果使用者不選擇該選項，表明使用者不希望實現上述操作流程的簡化。

假設用戶點擊選擇了圖 1 中所示的“啟用無加密代理登錄”選項，並點擊下一步，那麼支付網站 A 將接收到登錄資訊（例如，使用者在圖 1 的登錄頁面輸入的用戶名和密碼）、以及請求設定無加密登錄的指示（當使用者選擇上述選項，則表示向支付網站 A 發送了該指示）。

支付網站 A 在驗證登錄資訊成功後，獲知使用者在本次登錄之後的後續登錄過程希望啟用無加密代理登錄，那麼支付網站 A 將啟動無加密代理登錄的設定流程，該設定流程將在支付網站 A 和購物網站 S 之間交互實現，需要支付網站 A 向購物網站發送無加密代理登錄設定請求，請求購物網站側進行無加密代理登錄的相關設定，而購物網站在設定成功後，也會通知支付網站 A 無加密代理登錄設定成功。圖 3 示例了無加密代理登錄的設定流程。

在步驟 301 中，支付網站 A 創建許可證 a，該許可證

a 用於表示授予無加密登錄權限的訪問許可證。

例如，該許可證 a 可以稱為第二許可證（該第二，僅是為了與後續實施例中的第一許可證、第三許可證等進行區分），是支付網站 A 在驗證用戶在圖 1 中輸入的用戶名和密碼成功後進行創建。

許可證 a 中可以包括三方面資訊：由支付網站 A 以該網站私密金鑰簽名的網站標識（可以是網站名稱），以網站私密金鑰簽名的目前時間，以及，登錄資訊中的用戶名，該用戶名單獨以支付網站 A 的公開金鑰加密，並以網站私密金鑰簽名。

上述許可證 a 中的三種資訊的各自作用是：在後續步驟支付網站 A 向購物網站 S 發送無加密代理登錄設定請求時，將攜帶該許可證 a，其中的私密金鑰簽名的網站標識，可以用於向購物網站 S 保證該設定請求的真實性；其中的私密金鑰簽名的目前時間，可以使得不同時間創建的許可證隨時間變化，避免重複盜用；其中的加密並簽名的用戶名，主要是用於在後續實施例的觸發無加密代理登錄時由 S 將該用戶名傳遞回 A，以指定用於執行無加密登錄的用戶。

此外，本發明實施例中涉及到的許可證，除了以金鑰加密外，還另含該金鑰的指紋，這樣當對應網站更新金鑰委付的時候，新舊金鑰同時存在，可以根據許可證自帶的金鑰指紋，找到對應的金鑰，以完成解密或者簽名驗證。以下實施例中涉及到的其他許可證都包含相應的金鑰指

紋，不再重複敘述。

在步驟 302 中，支付網站 A 向購物網站 S 發送無加密代理登錄設定請求，攜帶許可證 a。

本實施例中，支付網站 A 和購物網站 S 之間的交互通信，可以是通過內嵌隱藏頁面實現，將所通信的資訊攜帶在該內嵌隱藏頁面的 url 中。例如，本步驟中的支付網站 A 向購物網站 S 發送無加密代理登錄設定請求，可以是通過一個內嵌 iframe（隱藏），指向 S 的無加密代理登錄設定頁面，url 中含參數 token=許可證 a。這樣 S 就可以接收到 A 發送的設定請求和許可證 a。

在步驟 303 中，購物網站 S 創建許可證 b，該許可證 b 中包含設備指紋和支付網站 A 的網站標識。

例如，購物網站 S 將首先驗證本次無加密代理登錄設定請求的真實性，可以是 S 利用支付網站 A 的公開金鑰，查看許可證 a 中包含的支付網站 A 的網站名稱的真實性。當確定該請求確實是支付網站 A 所發，則在本步驟創建許可證 b，該許可證 b 可以稱為第一許可證。

該許可證 b 中可以包括如下三方面資訊：一個是設備指紋，該設備指紋主要用於作為表示本次的無加密代理登錄設定的運行環境的標識，該運行環境例如可以包括目前的電腦和運行購物網站和支付網站的流覽器。具體實施中，比如，可以由流覽器中運用的用戶端代碼，例如 JavaScript 或者 Flash，主動收集流覽器平臺資訊，例如流覽器語言，以及由伺服器端代碼，例如 Java 或者

Python，主動收集 HTTP 和 TCP/IP 等各層網路通訊協定中自帶的欄位資訊，例如作業系統代號，資料合併後唯一標識客戶電腦（含流覽器），即設備指紋，該指紋也以 S 公開金鑰加密。另一方面資訊是以 S 公開金鑰加密的支付網站 A 的網站標識如網站名稱。再一方面資訊是以 S 公開金鑰加密的目前時間。

上述許可證 b 中的三種資訊的各自作用是：其中的設備指紋可以是購物網站 S 在後續的觸發無加密代理登錄時用於做安全性校驗，以據此查看使用者電腦和流覽器與設定無加密代理登錄時是否相同。而其中的 S 簽名的目前時間，可以供 S 內部策略判斷許可證是否過期，比如，如果超過預設的時間長度（例如，三個月），則無加密代理登錄失效。其中的支付網站 A 的網站名稱，可以用於使得 S 據此得知該許可證 b 是針對 A，且 A 已經啟用了無加密代理登錄。

在步驟 304 中，購物網站 S 將許可證 b 儲存至流覽器 cookie，並可以在網站的後臺資料庫中儲存許可證 b 和許可證 a 的對應關係。

在步驟 305 中，購物網站 S 通知支付網站 A，無加密代理登錄設定成功。

例如，購物網站 S 在儲存了許可證 b、以及兩個許可證的對應關係後，無加密代理登錄設定成功，此時的流覽器 cookie 中已經儲存了許可證 b，可以跳轉到無加密代理登錄設定成功頁面，通知支付網站 A 設定成功。

支付網站 A 以內層 iframe 載入無加密代理登錄設定成功頁面，並可以修改父 iframe，顯示無加密代理登錄已經啟用，參見圖 2 所示，支付網站 A 的已登錄頁面上顯示有已經啟用無加密代理登錄的字樣。當使用者在圖 2 所示的頁面點擊確認付款後，可以繼續顯示支付成功的頁面提示。

通過上述圖 3 所示的流程，描述了購物網站 S 和支付網站 A 之間在設定無加密代理登錄時的交互流程，可以看到，在該過程中，購物網站 S 創建了 S 執行安全校驗所需的包含設備指紋的許可證 b，並且支付網站 A 也創建了無加密登錄所需的許可證 a，包含指定無加密登錄的用戶名。

由圖 2 還可以看到，在支付網站 A 的已登錄頁面中，除了包含已經啟用無加密代理登錄的字樣，還可以提供有供使用者選擇退出無加密代理登錄的選項，比如頁面中在“已經啟用無加密代理登錄”旁邊示出的“退出”。

當用戶點擊了上述的“退出”時，表明該用戶不再想使用無加密代理登錄，即不希望從購物網站 S 點擊結算時直接跳轉到圖 2 所示的已登錄頁面，那麼，支付網站 A 接收到對退出無加密代理登錄的選項觸發。此時，支付網站 A 將啟動無加密代理登錄的取消流程，該取消流程也將在支付網站 A 和購物網站 S 之間交互實現，需要支付網站 A 向購物網站 S 發送無加密代理登錄取消請求，請求購物網站側進行無加密代理登錄的取消操作，而購物網站在取消

成功後，也可以選擇通知支付網站 A 無加密代理登錄取消成功。

圖 4 示例了無加密代理登錄的取消流程。需要說明的是，在取消無加密代理登錄時，可以是取消由購物網站向支付網站的自動跳轉，但是支付網站側的無加密登錄可以仍然保留。例如，一種可行的場景是，在取消無加密代理登錄後，當使用者在購物網站 S 點擊結算按鈕後，仍然顯示包含多個支付網站的網站清單頁面，比如包括支付網站 A、支付網站 B 等，用戶可以點擊選擇使用支付網站 A 進行結算；而在選擇支付網站 A 後，可以仍然無加密登錄至 A，即不用輸入用戶名和密碼，直接進入到 A 的已登錄頁面，或者，還可以是，當選擇支付網站 A 後，輸入用戶名和密碼再進入已登錄頁面。即無加密代理登錄的取消，可以是取消購物網站 S 到支付網站 A 的自動選擇和跳轉。

在步驟 401 中，支付網站 A 創建許可證 c，該許可證 c 用於指示購物網站 S 取消對支付網站 A 的無加密代理登錄。

例如，該許可證 c 可以稱為第四許可證，該許可證 c 中可以包括：支付網站 A 的網站標識、目前時間、以及 delete 這種指示刪除的操作標識，該許可證可以由支付網站 A 進行加密和簽名。

在步驟 402 中，支付網站 A 向購物網站 S 發送無加密代理登錄取消請求，攜帶許可證 c。

在步驟 403 中，購物網站 S 根據許可證 c，獲取包含

支付網站 A 的網站標識的許可證 b，刪除該許可證 b，並刪除許可證 b 對應的許可證 a。

例如，購物網站 S 可以根據許可證 c 中包括的支付網站 A 的網站標識，找到流覽器 cookie 中的包括該網站標識的許可證 b，刪除該許可證 b，並在後臺資料庫中刪除具有對應關係的許可證 b 和許可證 a。這樣後續用戶再點擊購物網站 S 中的結算按鈕，想要向支付網站跳轉時，由於已經刪除了許可證 b 和許可證 a，S 在流覽器 cookie 中將不能找到許可證 b，也無法獲知支付網站 A，不再自動向支付網站 A 請求無加密登錄，而只能顯示網站清單頁面，由使用者自己點擊選擇支付網站 A 進行請求跳轉。

上面的圖 3 和圖 4 對無加密代理登錄的設定和取消流程進行了說明，如下將結合圖 5，對設定完成無加密代理登錄後，使用者點擊結算按鈕時如何執行無加密代理登錄的流程進行描述，仍然以網上購物的例子來說。

在步驟 501 中，購物網站 S 接收到網站跳轉觸發。

本步驟中，使用者在購物網站 S 選定要購買的商品後，可以點擊 S 中的結算按鈕，此時就是 S 接收到網站跳轉觸發，即請求跳轉到支付網站去進行付款。通常的方式是，點擊結算按鈕後，將顯示一個包括供選擇的多個支付網站的網站清單頁面（如果將支付網站稱為第二網站，該網站清單頁面可以稱為第二網站清單頁面），但是，本實施例中的方法，當使用者點擊結算按鈕後，不會再顯示該網站清單頁面，而是由購物網站 S 直接跳轉至顯示網站清

單頁面中多個支付網站中的其中一個支付網站的已登錄頁面。比如，使用者點擊結算按鈕後，直接顯示其中一個支付網站 A 的已登錄頁面，類似圖 2 的頁面。具體的實現過程，參見圖 5 中的如下後續步驟。

在步驟 502 中，購物網站 S 獲取運行所在的流覽器的 cookie 中儲存的許可證 b，進行設備指紋的校驗。

例如，流覽器 cookie 中儲存的許可證 b，包含支付網站 A 的網站名稱，以及在設定 S 對 A 的無加密代理登錄時的運行環境的設備指紋。

本步驟中，購物網站 S 將根據許可證 b 中的設備指紋，判斷目前運行環境與設備指紋所表示的運行環境是否相同，比如，是否是同一台電腦且同一個流覽器。若通過設備指紋的校驗，則繼續執行步驟 503；否則，表明本次無加密代理登錄可能存在安全風險，購物網站可以停止執行後續步驟，且可以提示使用者該風險。並且，本步驟中，由於許可證 b 中還包括支付網站 A 的網站名稱，購物網站 S 可以據此獲知 A 已經啟用了無加密代理登錄。

在步驟 503 中，購物網站 S 獲取許可證 b 對應的許可證 a。

例如，該許可證 a 可以是支付網站 A 在用戶登錄成功後授予無加密登錄權限的訪問許可證。S 可以由後臺資料庫中獲取許可證 b 對應的許可證 a。

在步驟 504 中，購物網站 S 根據許可證 b 中的網站標識，向支付網站 A 發送無加密登錄請求，攜帶許可證 a。

例如，在具體實現中，購物網站 S 仍然可以是通過隱藏內嵌 iframe 的 url 傳遞資訊，該內嵌 iframe 指向支付網站 A 的登錄頁面，url 中包含參數 container=S&token=許可證 d，該許可證 d 可以稱為第三許可證，該第三許可證中可以至少包含第二許可證即 S 簽名的許可證 a，以供 A 驗證，並且 A 可以解密許可證 a 後獲得其中的用戶名，進行指定用戶的無加密登錄；此外，第三許可證中還可以包含 S 簽名的 S 名稱，以向支付網站 A 保證該請求的真實性，還可以包括 S 私密金鑰簽名的目前時間。

在步驟 505 中，支付網站 A 驗證許可證 a 成功。

例如，支付網站 A 驗證許可證 d，確保是由購物網站 S 發送的請求真實性，並且，還驗證許可證 a 的真實性和完整性。若均驗證通過，則執行步驟 506，無加密登錄至支付網站 A，此時就可以跳轉到圖 2 所示的已登錄頁面，並且可以在頁面上顯示已經啟用無加密代理登錄的標識。

在步驟 506 中，無加密登錄至支付網站 A。

上述的圖 3 至圖 5，分別了描述了無加密代理登錄的設定、取消以及觸發執行的流程，由這些流程可以看到，一方面，購物網站 S 可以知道支付網站 A 啟用了無加密代理登錄，並可以主動向 A 請求無加密登錄，而不需要使用者再去由多個支付網站的列表中選擇 A，直接跳轉到 A 的已登錄頁面，加快了購物的速度，提高了操作效率；另一方面，在這個過程中 S 和 A 均參與了安全校驗，S 校驗了設備指紋，A 校驗了訪問許可證，提高了無加密登錄至

A 的安全性。

此外，本發明實施例中涉及到的許可證，可以是根據 OAuth 協定設計許可證，並且通過網站的不對稱秘鑰加密或簽名，保證保密性和真實完整性。其中，S 的校驗與使用者設定的電腦（及流覽器軟體）綁定，且不可被偽造、複製、或者抵賴，因為 S 的許可證因為不對稱金鑰的保護，是不可偽造的，所有流覽器底層通訊都是通過 HTTPS 協定，HTTPS 協定保證它們在網路上，也是不可被明文監聽並被盜用的。S 與 A 已經達成無加密代理登錄的功能約定和建設，並且 S 與 A 的服務、不對稱金鑰和資料庫都是安全運行、儲存、不被盜讀或者篡改。在觸發無加密代理登錄時，因為 S 驗證許可證 b 中的設備指紋是否與目前電腦（含流覽器）相同，所以如果有人用遠端另一台電腦冒用嘗試登錄，這是不會成功的。同時，只要 A 保存許可證 d，S 也無法抵賴它創建了這個無加密登錄請求。

在上面的例子中，是以購物網站 S 與某一個支付網站 A 之間的無加密代理登錄的執行流程為例進行說明，實際實施中，購物網站 S 可以與多個支付網站設定無加密代理登錄，比如，S 既可以無加密代理登錄至 A，也可以無加密代理登錄至支付網站 B，還可以無加密代理登錄至支付網站 C。每一個支付網站與 S 的無加密代理登錄關係的設定都可以是相同的，而由購物網站 S 的角度來看，S 可以在流覽器的 cookie 中儲存多個許可證 b，每個許可證 b 對應不同的支付網站，後臺資料庫中也儲存了各個許可證 b

與對應的許可證 a，許可證 a 是對應的支付網站創建的無加密登錄訪問許可證。

這種情況下，在使用者觸發無加密代理登錄時，比如點擊了購物網站 S 中的結算按鈕，S 可以按照預設的選擇規則，選擇其中一個已經啟用無加密代理登錄的支付網站，執行無加密代理登錄。該選擇規則，例如是，選擇最近登錄的支付網站，或者選擇登錄頻率最高的網站等等。

參見圖 6 的示例，假設有三個支付網站 A、B 和 C，都與 S 之間啟用了無加密代理登錄，並且假設 S 選擇了 A 進行預設的無加密代理登錄，當使用者點擊 S 中的結算按鈕時，S 自動跳轉至 A 的已登錄頁面，圖 6 中的內嵌頁面中顯示了 A 的該已登錄頁面。同時，S 在檢查流覽器 cookie 中的多個許可證 b 時，已經根據各個許可證 b 中包含的網站標識，得知支付網站 B 和 C 也啟用了無加密代理登錄，則可以同時在與上述內嵌頁面的同一頁面中，也顯示支付網站 B 和 C，以方便用戶切換選擇，比如，S 預設無加密代理登錄了支付網站 A，可是用戶實際希望登錄至 B，則使用者可以點擊頁面中的支付網站 B，觸發 S 更改為向 B 進行無加密代理登錄。此外，如圖 6 所示，支付網站 B 和 C 上還可以顯示已經啟用無加密代理登錄的標識，比如，用“快捷”表示其已經啟用，而頁面中的支付網站 D 並沒有顯示“快捷”，表示其沒有設定無加密代理登錄。

參見圖 6，假設用戶選擇了支付網站 C，那麼 S 將創

建一個向支付網站 C 請求無加密登錄的第三許可證，該第三許可證攜帶 S 簽名的 S 名稱、網站 C 對應的許可證 a 和目前時間，並攜帶該許可證向支付網站 C 發送無加密登錄請求，並在 C 通過校驗後，在內嵌頁面的位置切換為支付網站 C 的已登錄頁面。

圖 6 所示的實現方式，可以在多個網站都啟用了無加密代理登錄的情況下，提供了一種 S 選擇登錄的方式，並且也方便了用戶進行選擇切換。

以上的例子，說明了購物網站 S 和支付網站之間的無加密代理登錄，購物網站 S 和支付網站之間是可以直接跳轉的關係，比如，購物網站 S 提供一個網站清單頁面，只要使用者選擇了支付網站 A，就可以登錄支付網站 A 進行支付。但是還有一種應用場景，購物網站 S 和支付網站的中間，還需要有一個“中間網站”，購物網站 S 和支付網站之間是不能直接跳轉的，在這種場景中，第一網站可以是上述的中間網站，也可以稱為支付網路網站，而第二網站可以是連結在支付網路網站下的支付網站。

比如，未實施本發明的方法時的通常情況下，當使用者點擊購物網站 S 中的結算按鈕時，可以顯示一個網站清單頁面，該頁面中可以包括：支付網站 A、支付網站 B、支付網站 C 和一個作為中間網站的支付網路網站 N，如果點擊該支付網路網站 N，其下還提供了多個支付網站 N1、N2 和 N3 供用戶選擇（這些支付網站與前述的支付網站 A、B 和 C 是並列對等關係），即支付網站 N1、N2

和 N3 是接入支付網路網站 N 的下一層網站。如果使用者要使用支付網站 N1，則需要在點擊 S 中的結算後，選擇支付網路網站 N，再選擇 N 下的支付網站 N1，較為繁瑣。

而如果使用本發明的方法，在支付網路網站 N 與支付網站 N1 之間進行無加密代理登錄的設置，執行圖 3 至圖 5 的流程，其中，支付網路網站 N 相當於流程中的購物網站 S，支付網站 N1 相當於流程中的支付網站 A。那麼，當使用者選擇點擊了支付網路網站 N 後，不用再選擇 N1，支付網路網站 N 就可以直接跳轉到顯示支付網站 N1 的已登錄頁面，類似於由購物網站 S 跳轉到顯示支付網站 A 的已登錄頁面。

如下對 S——N——N1 場景下，在 N 和 N1 之間設定和觸發無加密代理登錄的過程進行描述，不過由於 N 和 N1 所執行的處理與圖 3 至圖 5 中的 S 和 A 之間的處理相同，所以這裡只簡單描述，詳細的可以參見上面的例子。

當使用者在購物網站 S 中點擊了結算按鈕時，可以顯示圖 7 所示的頁面，該頁面中可以包括支付網站 A、支付網站 B、支付網站 C，以及支付網路網站 N。當使用者點擊 N 之後，則顯示圖 8，N 下還連結有支付網站 N1、N2 和 N3 供用戶選擇；具體的可以是，當點擊 N 後，以 S 的內嵌頁面的形式顯示 N 的頁面，在該 N 的頁面中顯示 N1、N2 和 N3，該內嵌顯示可以使得使用者不想使用 N 時，方便的切換選擇其他網站，比如可以選擇支付網站

A。

如果這次初次設定 N 和 N1 間的無加密代理登錄，則當使用者在 N 頁面選擇了支付網站 N1 後，可以繼續顯示 N1 的登錄頁面，如圖 9 所示，該圖 9 所顯示的 N1 登錄頁面就類似於圖 1 中顯示的頁面，該 N1 的登錄頁面也可以內嵌頁面形式顯示，同時在 N 的頁面中顯示 N2 和 N3，以方便用戶切換。若使用者選擇該頁面中的“啟用無加密代理登錄”，並點擊下一步，則 N1 網站就會接收到請求設定無加密登錄的指示，並創建第二許可證，開始與支付網路網站 N 之間執行無加密代理登錄的設定流程，具體的過程可以參考圖 3 的 S 與 A 之間的流程，不再詳述。同理，N 和 N1 之間也可以按照圖 4 的流程進行無加密代理登錄的取消操作。

設定完成無加密代理登錄後，當使用者下次點擊購物網站 S 中的結算按鈕時，可以仍然顯示圖 7 的清單頁面，但是當使用者點擊了圖 7 中的支付網路網站 N 時，此時就相當於 N 接收到了網站跳轉觸發。本來按照通常的方式，N 根據該網站跳轉觸發將圖 8 中的支付網站 N1 至 N3 的列表供用戶選擇，但是由於上面的例子中已經設定了無加密代理登錄，此時 N 根據網站跳轉觸發，將獲取運行所在的流覽器的 cookie 中儲存的許可證，校驗設備指紋，並在校驗通過時自動向支付網站 N1 發送無加密登錄請求，即執行圖 5 中所示的流程。所以，當使用者點擊了支付網路網站 N 後，就可以直接顯示圖 10，跳轉到支付網站 N1

的已登錄頁面，並顯示有已經啟用無加密代理登錄的標識。當然，N的頁面中還可以同時顯示支付網站N1和N2供用戶切換。

在上面的例子中，是以支付網路網站N是一個不用密碼登錄的網站為例，比如圖7和圖8中，當用戶點擊N之後，可以直接顯示N1至N3的列表供用戶選擇。可選的，該支付網路網站N也可以是一個需要密碼登錄的網站，比如，當用戶點擊圖7中的支付網路網站N之後，可以先以內嵌形式顯示一個N的登錄頁面，需要使用者輸入N的用戶名和密碼後才能登錄N，登錄成功後才顯示N1、N2和N3的列表。這種場景中的無加密代理登錄的設定和觸發流程與前述相同，比如，在設定時無加密代理登錄，使用者先登錄N，再選擇N1進行設定；而在設定完成後的觸發時，用戶點擊N之後，N可以先讓使用者輸入用戶名和密碼，並在校驗登錄成功後，N再執行圖5的流程，自動向N1進行無加密登錄請求，仍然會跳轉至圖10的頁面，只是前面需要使用者先登錄N。

此外，上述結合圖7至圖10，描述了S——N——N1場景下，在N和N1之間設定和觸發無加密代理登錄的過程，還可以有其他的應用例子，比如，可以只在S和N之間設定無加密代理登錄，方法相同。簡單描述如下：當使用者在購物網站S中點擊結算按鈕時，顯示類似圖7的頁面，使用者可以選擇支付網路網站N。同樣的，N既可以有密碼，也可以不需要密碼。當N需要密碼時，使用者

輸入用戶名和密碼登錄 N，類似於圖 1 中登錄支付網站 A，並選擇啟用無加密代理登錄，那麼 N 將開始與 S 之間執行圖 3 的設定無加密代理登錄的流程。設定完成後，當用戶下次點擊 S 中的結算時，S 就可以自動跳轉至 N 的已登錄頁面，不需要使用者再選擇 N。當然，此時由於 N 和 N1 之間沒有無加密代理登錄設定，跳轉的 N 的已登錄頁面中需要顯示 N1 至 N3，供用戶選擇。即使 N 不需要密碼，也可以在頁面中設置一個對應 N 的"啟用無加密代理登錄"的選項供使用者選擇，以使得用戶在點擊 N 時同時通知 N 要啟用無加密代理登錄。

在 S——N——N1 場景下，除了上述的 N——N1 之間設定無加密代理登錄、或者，S——N 之間設定無加密代理登錄的例子，還可以是既在 S—N 之間設定，也在 N—N1 之間設定無加密代理登錄，形成一種兩層的無加密代理登錄。這樣，當用戶在購物網站 S 中點擊結算按鈕時，出現的場景將是，直接跳轉至支付網站 N1 的已登錄頁面，已經實現無加密登錄 N1，這樣就省去了使用者選擇支付網路網站 N 的操作，也省去了使用者在支付網路網站 N 中選擇支付網站 N1 的操作，操作效率進一步實現提高。

在上面的兩層無加密代理登錄場景中，如果將購物網站 S 稱為第一網站，支付網路網站 N 稱為第二網站，將支付網站 N1 稱為第三網站，那麼上面例子實現的操作是，回應於用戶對網站跳轉觸發標識的選擇，第一網站顯

示多個第二網站的其中一個第二網站（即 N）下的其中一個第三網站（即 N1）的已登錄頁面。

在這個例子中，購物網站 S 與支付網站 N1 之間，其實經過了兩次無加密代理登錄，包括：S 與支付網路網站 N 之間的無加密代理登錄，以及，支付網路網站 N 與支付網站 N1 之間的無加密代理登錄。這兩個層次各自之間的無加密代理登錄的設定和觸發流程，與上面例子相同，不再贅述。當這種兩層無加密代理登錄觸發時，由 N 的角度來看上述操作的具體實現，當 S 無加密代理登錄至 N 之後，N 可以繼續執行如下流程，以實現由 N 到 N1 的無加密代理登錄，實際上該過程與 S 無加密代理登錄至 N 相同。

支付網路網站 N 在執行無加密登錄後，獲取運行所在的流覽器的 cookie 中儲存的第五許可證，該第五許可證包括其中一個支付網站比如支付網站 N1 的網站標識以及用於表示在設定 N1 的無加密代理登錄時的運行環境的設備指紋。

支付網路網站 N 根據該設備指紋，確定目前運行環境與 N1 無加密代理登錄設定時的運行環境相同，則獲取該第五許可證對應的第六許可證，該第六許可證為支付網站 N1 在用戶登錄成功後授予無加密登錄權限的訪問許可證。

支付網路網站 N 根據第五許可證中的網站標識，向網站標識對應的支付網站 N1 發送無加密登錄請求，攜帶該

第六許可證，並在支付網站 N1 驗證第六許可證成功時，實現支付網站 N1 的無加密登錄。

在上面的場景例子中，是以三個網站之間（S-——N-——N1）的無加密代理登錄為例來說明本公開的方法，具體實施中，還可以是更多層網站進行網站間配合實施的無加密代理登錄，例如，四層（如，S-——N-——N1-——N11）、五層或更多層，方法同上述的三個網站間的實施情況，不再詳述。

本發明實施例的網站登錄方法，可以由網站執行，具體可以是該網站的服務端或者用戶端。例如，作為第二網站的支付網站在執行該方法時，可以是由支付網站的服務端創建的第二許可證；又例如，作為第一網站的支付網路網站在執行該方法時，可以是由支付網路網站的用戶端根據第一許可證校驗設備指紋。本發明的網站登錄方法，如果以軟體功能單元的形式實現並作為獨立的產品銷售或使用時，可以儲存在一個電腦可讀取儲存介質中。基於這樣的理解，本公開的技術方案本質上或者說對現有技術做出貢獻的部分或者該技術方案的部分可以以軟體產品的形式體現出來，該電腦軟體產品儲存在一個儲存介質中，包括若干指令用以使得一台計算設備（可以是個人電腦，伺服器，或者網路設備等）執行本發明各個實施例所述方法的全部或部分步驟。而前述的儲存介質包括：隨身碟、移動硬碟、唯讀記憶體（ROM，Read-Only Memory）、隨機存取記憶體（RAM，Random Access Memory）、磁碟或者

光碟等各種可以儲存程式碼的介質。

圖 11 提供了一種網站登錄裝置，該裝置可以應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置可以包括：許可證獲取模組 1101、許可證校驗模組 1102 和無加密登錄模組 1103。

許可證獲取模組 1101，用於在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，該第一許可證包括該網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；

許可證校驗模組 1102，用於根據該設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，則獲取該第一許可證對應的第二許可證，第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

無加密登錄模組 1103，用於根據第一許可證中的網站標識，向網站標識對應的第二網站發送無加密登錄請求，攜帶第三許可證，該第三許可證中包括該第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。

在一個例子中，如圖 12 所示，該裝置還可以包括：設定接收模組 1201 和設定處理模組 1202。

設定接收模組 1201，用於接收第二網站發送的無加

密代理登錄設定請求，該無加密代理登錄設定請求攜帶該第二許可證；

設定處理模組 1202，用於創建包含該設備指紋的該第一許可證，將該第一許可證儲存至運行所在的流覽器 cookie，並儲存該第一許可證和第二許可證的對應關係，通知該第二網站無加密代理登錄設定成功。

在一個例子中，該裝置還可以包括：頁面顯示模組 1203 和登錄切換模組 1204。

頁面顯示模組 1203，用於在無加密登錄至第二網站後，以內嵌頁面的形式顯示該第二網站的已登錄頁面；當該流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證時，根據第一許可證中的網站標識，在與內嵌頁面的同一頁面中，顯示已經在第一網站啟用無加密代理登錄的其他第二網站。

登錄切換模組 1204，用於在檢測到用戶選擇該其他第二網站時，則向該其他第二網站發送無加密登錄請求，並在該第三許可證中攜帶其他第二網站的第一許可證對應的第二許可證。

在一個例子中，頁面顯示模組 1203，用於在流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證，且接收到網站跳轉觸發時，按照預設的選擇規則選擇其中一個第二網站，執行無加密代理登錄。

在一個例子中，該裝置還包括：取消接收模組 1205 和取消處理模組 1206。

取消接收模組 1205，用於接收第二網站發送的無加密代理登錄取消請求，該無加密代理登錄取消請求攜帶第三許可證，該第三許可證用於第二網站創建的指示取消無加密代理登錄，且第三許可證包括第二網站的網站標識；

取消處理模組 1206，用於根據第三許可證中的網站標識，獲取包含該第二網站的第一許可證，刪除第一許可證、以及與該第一許可證對應的第二許可證。

在一個例子中，該第一網站是購物網站，該第二網站是支付網站；或者，該第一網站是支付網路網站，該第二網站是連結在該支付網站網站下的支付網站。

圖 13 提供了一種網站登錄裝置，該裝置可以應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置可以包括：標識顯示模組 1301 和頁面跳轉模組 1302。

標識顯示模組 1301，用於在頁面顯示網站跳轉觸發標識，該網站跳轉觸發標識用於在選擇時觸發第一網站跳轉到包括供選擇的多個第二網站的網站清單頁面；

頁面跳轉模組 1302，用於回應於用戶對網站跳轉觸發標識的選擇，跳轉至顯示該網站清單頁面中多個第二網站的其中一個第二網站的已登錄頁面。

在一個例子中，該第二網站以內嵌頁面的形式顯示在該第一網站，且該第二網站的已登錄頁面上顯示已經啟用無加密代理登錄的指示。如圖 14 所示，該裝置還可以包括：頁面顯示模組 1401 和頁面切換模組 1402。

頁面顯示模組 1401，用於顯示已經啟用無加密代理登錄的其他第二網站；

頁面切換模組 1402，用於回應於用戶對該其他第二網站的選擇，在該內嵌頁面的位置上切換為該其他第二網站的已登錄頁面。

在一個例子中，該第二網站還連結供選擇的多個第三網站；頁面跳轉模組 1302，還用於回應於用戶對網站跳轉觸發標識的選擇，顯示多個第二網站的其中一個第二網站下的其中一個第三網站的已登錄頁面。

圖 15 提供了一種網站登錄裝置，該裝置可以應用於第二網站，使得第一網站無加密代理登錄至第二網站；該裝置可以包括：請求接收模組 1501 和登錄執行模組 1502。

請求接收模組 1501，用於接收第一網站發送的無加密登錄請求，該無加密登錄請求攜帶第三許可證，該第三許可證中包括第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

登錄執行模組 1502，用於驗證該第二許可證成功時，執行無加密登錄。

在一個例子中，如圖 16 所示，該裝置還可以包括：設定指示模組 1601、設定發送模組 1602 和設定結果模組 1603。

設定指示模組 1601，用於接收請求登錄的登錄資訊、以及請求設定無加密登錄的指示；

設定發送模組 1602，用於根據該指示，在驗證登錄資訊成功後創建該第二許可證，並向該第一網站發送無加密代理登錄設定請求，攜帶該第二許可證，以使得第一網站根據無加密代理登錄設定請求創建包含設備指紋的第一許可證，並儲存第一許可證和第二許可證的對應關係；

設定結果模組 1603，用於接收第一網站發送的無加密代理登錄設定成功的通知，並在第二網站的已登錄頁面中顯示無加密代理登錄已經啟用。

在一個例子中，該裝置還可以包括：取消指示模組 1604 和取消處理模組 1605。

取消指示模組 1604，用於在執行無加密登錄後，在已登錄頁面上還顯示：供使用者選擇退出無加密代理登錄的選項；

取消處理模組 1605，用於在接收到對退出無加密代理登錄的選項觸發時，創建用於指示取消無加密代理登錄的第四許可證，該第四許可證中包括第二網站的網站標識；向第一網站發送無加密代理登錄取消請求，攜帶該第四許可證，以使得第一網站根據該第四許可證取消第二網站的無加密代理登錄。

在一個例子中，該第二網站還連結供選擇的多個第三網站；該裝置還可以包括：許可證取得模組 1606、指紋校驗模組 1607 和登錄請求模組 1608。

許可證取得模組 1606，用於在執行無加密登錄後，獲取第二網站運行所在的流覽器的 cookie 中儲存的第五

許可證，該第五許可證包括其中一個第三網站的網站標識、以及用於表示在設定第三網站的無加密代理登錄時的設備指紋；

指紋校驗模組 1607，用於根據該設備指紋，確定目前運行環境與第三網站無加密代理登錄設定時的運行環境相同，則獲取該第五許可證對應的第六許可證，第六許可證為第三網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

登錄請求模組 1608，用於根據第五許可證中的網站標識，向該網站標識對應的第三網站發送無加密登錄請求，攜帶該第六許可證，並在第三網站驗證該第六許可證成功時，無加密登錄至該第三網站。

以上所述僅為本發明的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

【符號說明】

1101：許可證獲取模組

1102：許可證校驗模組

1103：無加密登錄模組

1201：設定接收模組

1202：設定處理模組

1203：頁面顯示模組

1204：登錄切換模組

1205：取消接收模組

1206：取消處理模組

1301：標識顯示模組

1302：頁面跳轉模組

1401：頁面顯示模組

1402：頁面切換模組

1501：請求接收模組

1502：登錄執行模組

1601：設定指示模組

1602：設定發送模組

1603：設定結果模組

1604：取消指示模組

1605：取消處理模組

1606：許可證取得模組

1607：指紋校驗模組

1608：登錄請求模組

申請專利範圍

1. 一種網站登錄方法，其特徵在於，該方法用於由第一網站無加密代理登錄至第二網站；該方法包括：

該第一網站在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，該第一許可證包括該網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；

該第一網站根據該設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，則獲取該第一許可證對應的第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

該第一網站根據第一許可證中的網站標識，向該網站標識對應的第二網站發送無加密登錄請求，攜帶第三許可證，該第三許可證中包括該第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。

2. 根據申請專利範圍第 1 項所述的方法，其中，該方法還包括：

該第一網站接收第二網站發送的無加密代理登錄設定請求，該無加密代理登錄設定請求攜帶該第二許可證；

該第一網站創建包含該設備指紋的該第一許可證，將該第一許可證儲存至運行所在的流覽器 cookie，並儲存該第一許可證和第二許可證的對應關係，通知該第二網站無加密代理登錄設定成功。

3. 根據申請專利範圍第 1 項所述的方法，其中，該方法還包括：

該第一網站在無加密登錄至第二網站後，以內嵌頁面的形式顯示該第二網站的已登錄頁面；

當該流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證時，該第一網站根據第一許可證中的網站標識，在與該內嵌頁面的同一頁面中，顯示已經在第一網站啟用無加密代理登錄的其他第二網站；

若該第一網站檢測到用戶選擇該其他第二網站，則向該其他第二網站發送無加密登錄請求，並在該第三許可證中攜帶其他第二網站的第一許可證對應的第二許可證。

4. 根據申請專利範圍第 3 項所述的方法，其中，該方法還包括：

若流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證，該第一網站在接收到網站跳轉觸發時，按照預設的選擇規則選擇其中一個第二網站，執行無加密代理登錄。

5. 根據申請專利範圍第 1 項所述的方法，其中，該方法還包括：

該第一網站接收第二網站發送的無加密代理登錄取消請求，該無加密代理登錄取消請求攜帶第三許可證，該第三許可證用於第二網站創建的指示取消無加密代理登錄，且第三許可證包括第二網站的網站標識；

該第一網站根據第三許可證中的網站標識，獲取包含

該第二網站的第一許可證，刪除第一許可證、以及與該第一許可證對應的第二許可證。

6. 根據申請專利範圍第 1~5 項任一項所述的方法，其中，該第一網站是購物網站，該第二網站是支付網站；

或者，該第一網站是支付網路網站，該第二網站是連結在該支付網路網站下的支付網站。

7. 一種網站登錄方法，其特徵在於，該方法用於由第一網站無加密登錄至第二網站；該方法包括：

該第一網站在頁面顯示網站跳轉觸發標識，該網站跳轉觸發標識用於在選擇時觸發第一網站跳轉到包括供選擇的多個第二網站的網站清單頁面；

回應於使用者對網站跳轉觸發標識的選擇，該第一網站跳轉至顯示該網站清單頁面中多個第二網站的其中一個第二網站的已登錄頁面。

8. 根據申請專利範圍第 7 項所述的方法，其中，該第二網站以內嵌頁面的形式顯示在該第一網站，且該第二網站的已登錄頁面上顯示已經啟用無加密代理登錄的指示；該方法還包括：

該第一網站還顯示已經啟用無加密代理登錄的其他第二網站；

回應於用戶對該其他第二網站的選擇，該第一網站在該內嵌頁面的位置上切換為該其他第二網站的已登錄頁面。

9. 根據申請專利範圍第 7 項所述的方法，其中，該

第二網站還連結供選擇的多個第三網站；該方法還包括：

回應於使用者對網站跳轉觸發標識的選擇，該第一網站顯示該多個第二網站的其中一個第二網站下的其中一個第三網站的已登錄頁面。

10. 一種網站登錄方法，其特徵在於，該方法用於由第一網站無加密登錄至第二網站；該方法包括：

該第二網站接收第一網站發送的無加密登錄請求，該無加密登錄請求攜帶第三許可證，該第三許可證中包括第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

該第二網站驗證該第二許可證成功時，執行無加密登錄。

11. 根據申請專利範圍第 10 項所述的方法，其中，該方法還包括：

該第二網站接收請求登錄的登錄資訊、以及請求設定無加密登錄的指示；

該第二網站根據該指示，在驗證登錄資訊成功後創建該第二許可證，並向該第一網站發送無加密代理登錄設定請求，攜帶該第二許可證，以使得第一網站根據無加密代理登錄設定請求創建包含設備指紋的第一許可證，並儲存第一許可證和第二許可證的對應關係；

該第二網站接收第一網站發送的無加密代理登錄設定成功的通知，並在第二網站的已登錄頁面中顯示無加密代理登錄已經啟用。

12. 根據申請專利範圍第 11 項所述的方法，其中，該方法還包括：

該第二網站在執行無加密登錄後，在已登錄頁面上還顯示：供使用者選擇退出無加密代理登錄的選項；

在接收到對退出無加密代理登錄的選項觸發時，該第二網站創建用於指示取消無加密代理登錄的第四許可證，該第四許可證中包括第二網站的網站標識；

該第二網站向第一網站發送無加密代理登錄取消請求，攜帶該第四許可證，以使得第一網站根據該第四許可證取消第二網站的無加密代理登錄。

13. 根據申請專利範圍第 10 項所述的方法，其中，該第二網站還連結供選擇的多個第三網站；該方法還包括：

該第二網站在執行無加密登錄後，獲取第二網站運行所在的流覽器的 cookie 中儲存的第五許可證，該第五許可證包括其中一個第三網站的網站標識、以及用於表示在設定第三網站的無加密代理登錄時的設備指紋；

該第二網站根據該設備指紋，確定目前運行環境與第三網站無加密代理登錄設定時的運行環境相同，則獲取該第五許可證對應的第六許可證，該第六許可證為第三網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

該第二網站根據第五許可證中的網站標識，向該網站標識對應的第三網站發送無加密登錄請求，攜帶該第六許可證，並在第三網站驗證該第六許可證成功時，無加密登

錄至該第三網站。

14. 一種網站登錄裝置，其特徵在於，該裝置應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置包括：

許可證獲取模組，用於在接收到網站跳轉觸發時，獲取第一網站運行所在的流覽器的 cookie 中儲存的第一許可證，該第一許可證包括該網站跳轉觸發所指示的第二網站清單頁面的其中一個第二網站的網站標識、以及用於表示在設定第二網站的無加密代理登錄時的設備指紋；

許可證校驗模組，用於根據該設備指紋，確定目前運行環境與第二網站無加密代理登錄設定時的運行環境相同，則獲取該第一許可證對應的第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

無加密登錄模組，用於根據第一許可證中的網站標識，向該網站標識對應的第二網站發送無加密登錄請求，攜帶第三許可證，該第三許可證中包括該第二許可證，並在第二網站驗證該第二許可證成功時，無加密登錄至該第二網站。

15. 根據申請專利範圍第 14 項所述的裝置，其中，該裝置還包括：

設定接收模組，用於接收第二網站發送的無加密代理登錄設定請求，該無加密代理登錄設定請求攜帶該第二許可證；

設定處理模組，用於創建包含該設備指紋的該第一許可證，將該第一許可證儲存至運行所在的流覽器 cookie，並儲存該第一許可證和第二許可證的對應關係，通知該第二網站無加密代理登錄設定成功。

16. 根據申請專利範圍第 14 項所述的裝置，其中，該裝置還包括：

頁面顯示模組，用於在無加密登錄至第二網站後，以內嵌頁面的形式顯示該第二網站的已登錄頁面；當該流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證時，根據第一許可證中的網站標識，在與該內嵌頁面的同一頁面中，顯示已經在第一網站啟用無加密代理登錄的其他第二網站；

登錄切換模組，用於在檢測到用戶選擇該其他第二網站時，則向該其他第二網站發送無加密登錄請求，並在該第三許可證中攜帶其他第二網站的第一許可證對應的第二許可證。

17. 根據申請專利範圍第 16 項所述的裝置，其中，

該頁面顯示模組，用於在流覽器的 cookie 中儲存有分別對應不同第二網站的多個第一許可證，且接收到網站跳轉觸發時，按照預設的選擇規則選擇其中一個第二網站，執行無加密代理登錄。

18. 根據申請專利範圍第 14 項所述的裝置，其中，該裝置還包括：

取消接收模組，用於接收第二網站發送的無加密代理

登錄取消請求，該無加密代理登錄取消請求攜帶第三許可證，該第三許可證用於第二網站創建的指示取消無加密代理登錄，且第三許可證包括第二網站的網站標識；

取消處理模組，用於根據第三許可證中的網站標識，獲取包含該第二網站的第一許可證，刪除第一許可證、以及與該第一許可證對應的第二許可證。

19. 根據申請專利範圍第 14~18 項任一項所述的裝置，其中，該第一網站是購物網站，該第二網站是支付網站；

或者，該第一網站是支付網路網站，該第二網站是連結在該支付網站網站下的支付網站。

20. 一種網站登錄裝置，其特徵在於，該裝置應用於第一網站，使得該第一網站無加密代理登錄至第二網站；該裝置包括：

標識顯示模組，用於在頁面顯示網站跳轉觸發標識，該網站跳轉觸發標識用於在選擇時觸發第一網站跳轉到包括供選擇的多個第二網站的網站清單頁面；

頁面跳轉模組，用於回應於使用者對網站跳轉觸發標識的選擇，跳轉至顯示該網站清單頁面中多個第二網站的其中一個第二網站的已登錄頁面。

21. 根據申請專利範圍第 20 項所述的裝置，其中，該第二網站以內嵌頁面的形式顯示在該第一網站，且該第二網站的已登錄頁面上顯示已經啟用無加密代理登錄的指示；該裝置還包括：

頁面顯示模組，用於顯示已經啟用無加密代理登錄的其他第二網站；

頁面切換模組，用於回應於使用者對該其他第二網站的選擇，在該內嵌頁面的位置上切換為該其他第二網站的已登錄頁面。

22. 根據申請專利範圍第 20 項所述的裝置，其中，該第二網站還連結供選擇的多個第三網站；

該頁面跳轉模組，還用於回應於用戶對網站跳轉觸發標識的選擇，顯示多個第二網站的其中一個第二網站下的其中一個第三網站的已登錄頁面。

23. 一種網站登錄裝置，其特徵在於，該裝置應用於第二網站，使得第一網站無加密代理登錄至第二網站；該裝置包括：

請求接收模組，用於接收第一網站發送的無加密登錄請求，該無加密登錄請求攜帶第三許可證，該第三許可證中包括第二許可證，該第二許可證為第二網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

登錄執行模組，用於驗證該第二許可證成功時，執行無加密登錄。

24. 根據申請專利範圍第 23 項所述的裝置，其中，該裝置還包括：

設定指示模組，用於接收請求登錄的登錄資訊、以及請求設定無加密登錄的指示；

設定發送模組，用於根據該指示，在驗證登錄資訊成

功後創建該第二許可證，並向該第一網站發送無加密代理登錄設定請求，攜帶該第二許可證，以使得第一網站根據無加密代理登錄設定請求創建包含設備指紋的第一許可證，並儲存第一許可證和第二許可證的對應關係；

設定結果模組，用於接收第一網站發送的無加密代理登錄設定成功的通知，並在第二網站的已登錄頁面中顯示無加密代理登錄已經啟用。

25. 根據申請專利範圍第 24 項所述的裝置，其中，該裝置還包括：

取消指示模組，用於在執行無加密登錄後，在已登錄頁面上還顯示：供使用者選擇退出無加密代理登錄的選項；

取消處理模組，用於在接收到對退出無加密代理登錄的選項觸發時，創建用於指示取消無加密代理登錄的第四許可證，該第四許可證中包括第二網站的網站標識；向第一網站發送無加密代理登錄取消請求，攜帶該第四許可證，以使得第一網站根據該第四許可證取消第二網站的無加密代理登錄。

26. 根據申請專利範圍第 23 項所述的裝置，其中，該第二網站還連結供選擇的多個第三網站；該裝置還包括：

許可證取得模組，用於在執行無加密登錄後，獲取第二網站運行所在的流覽器的 cookie 中儲存的第五許可證，該第五許可證包括其中一個第三網站的網站標識、以

及用於表示在設定第三網站的無加密代理登錄時的設備指紋；

指紋校驗模組，用於根據該設備指紋，確定目前運行環境與第三網站無加密代理登錄設定時的運行環境相同，則獲取該第五許可證對應的第六許可證，該第六許可證為第三網站在用戶登錄成功後授予無加密登錄權限的訪問許可證；

登錄請求模組，用於根據第五許可證中的網站標識，向該網站標識對應的第三網站發送無加密登錄請求，攜帶該第六許可證，並在第三網站驗證該第六許可證成功時，無加密登錄至該第三網站。

圖　式

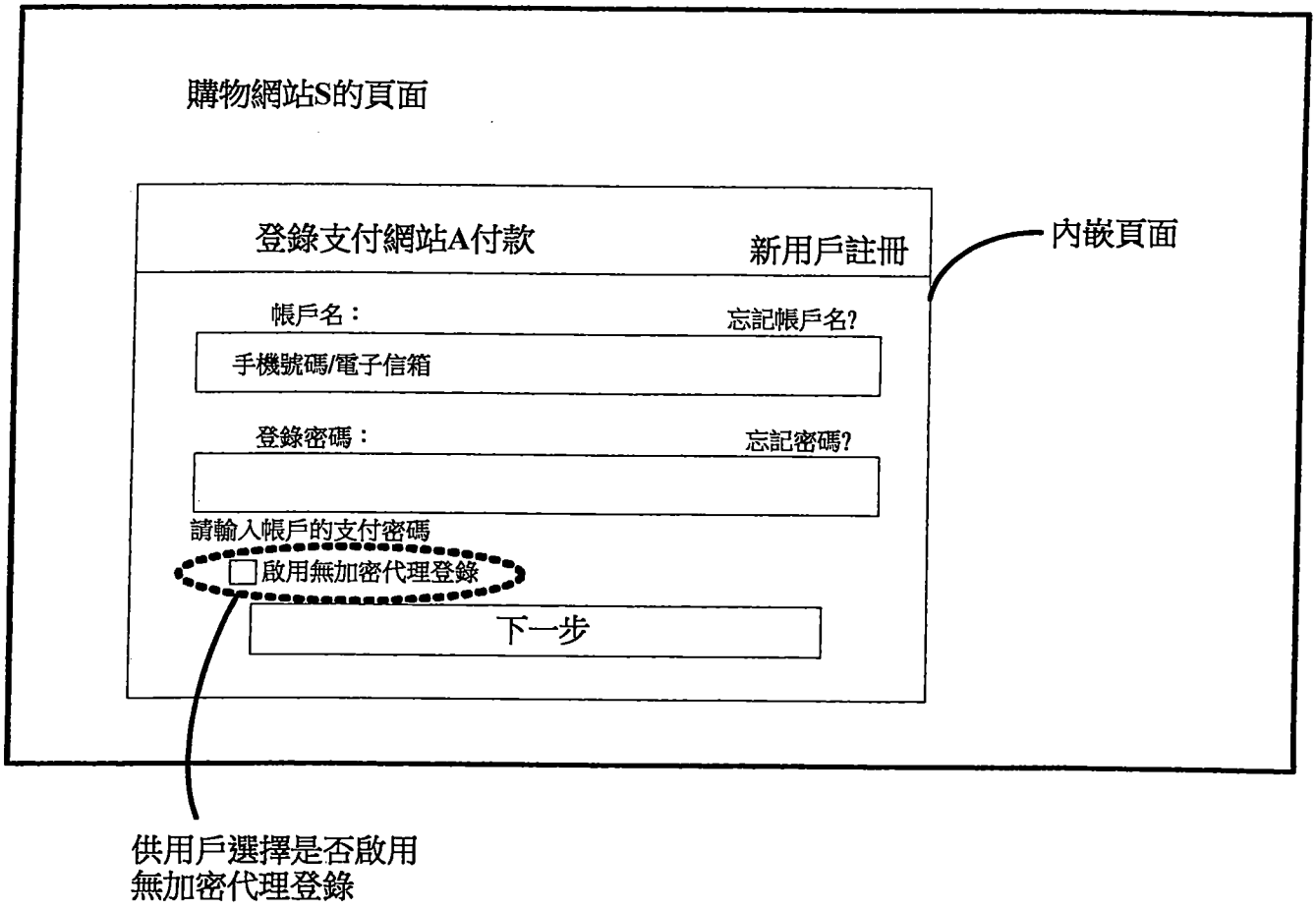
購物網站S的頁面
登錄支付網站A付款
新用戶註冊
內嵌頁面
帳戶名：
忘記帳戶名?
手機號碼/電子信箱
登錄密碼：
忘記密碼?
請輸入帳戶的支付密碼
啟用無加密代理登錄
下一步
供用戶選擇是否啟用
無加密代理登錄

圖 1

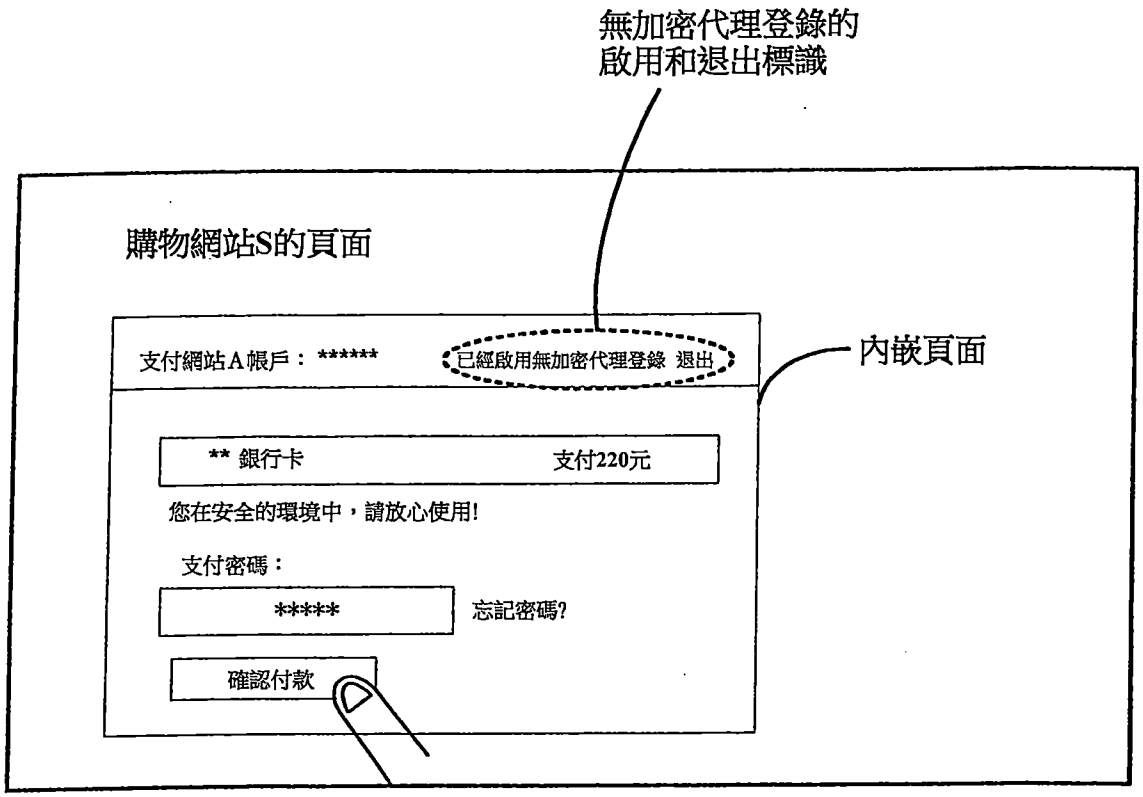
無加密代理登錄的
啟用和退出標識
購物網站S的頁面
支付網站A帳戶：******
已經啟用無加密代理登錄 退出
內嵌頁面
** 銀行卡
支付220元
您在安全的環境中，請放心使用!
支付密碼：
*****
忘記密碼?
確認付款

圖 2

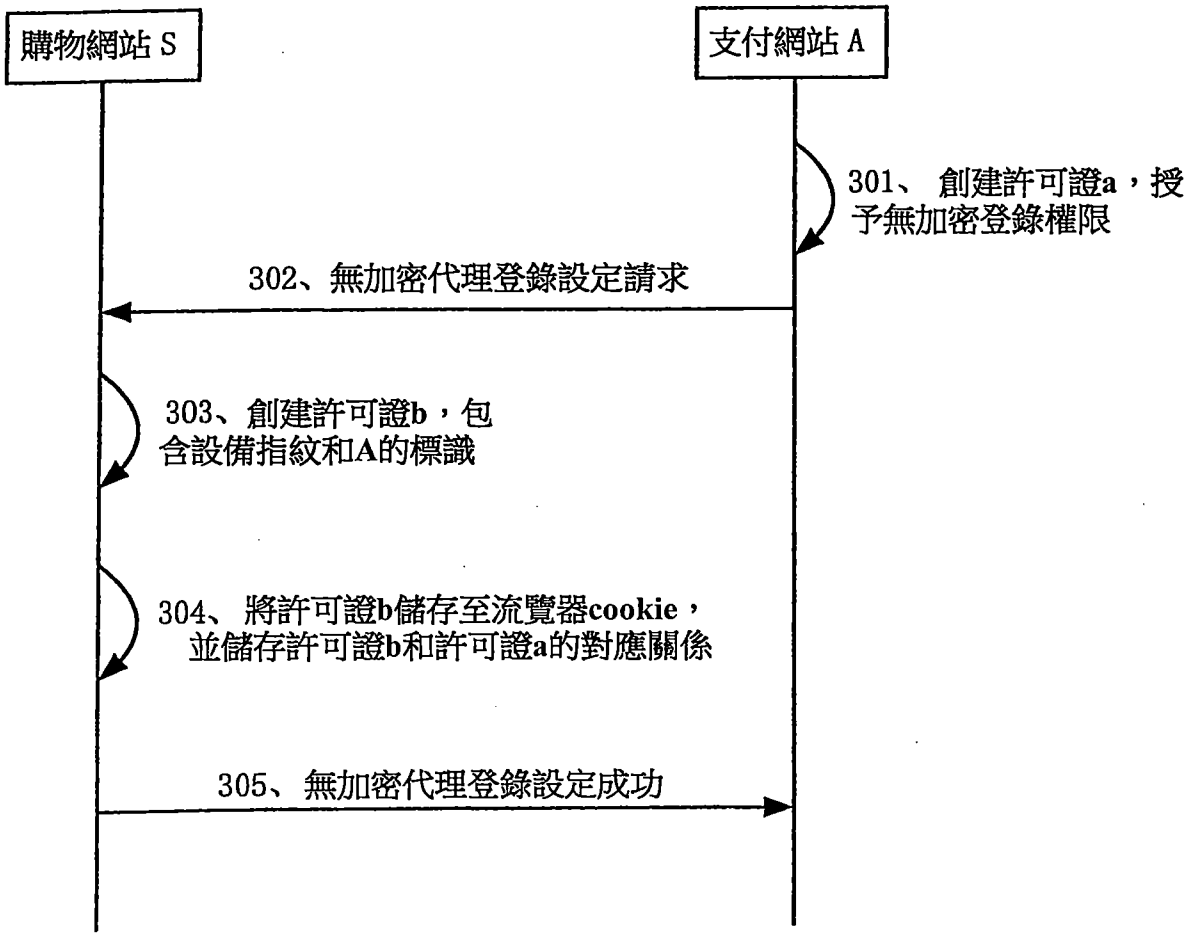
購物網站 S
支付網站 A
301、 創建許可證a，授予無加密登錄權限
302、無加密代理登錄設定請求
303、創建許可證b，包含設備指紋和A的標識
304、 將許可證b儲存至流覽器cookie，並儲存許可證b和許可證a的對應關係
305、無加密代理登錄設定成功

圖 3

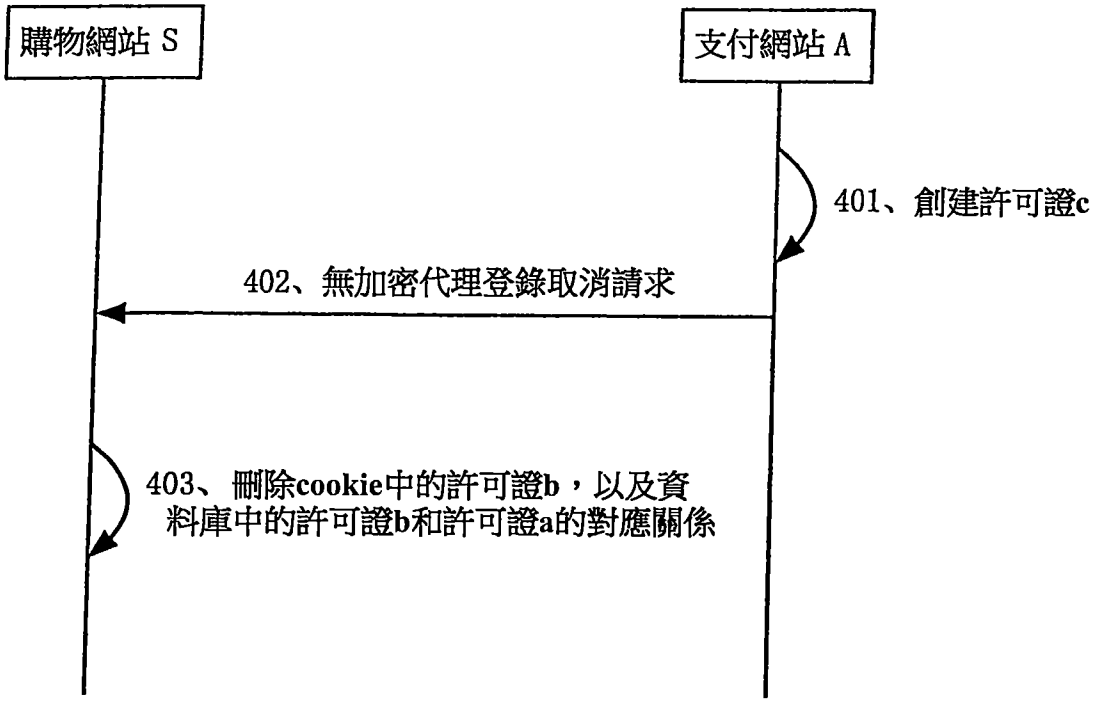
購物網站 S
支付網站 A
401、創建許可證c
402、無加密代理登錄取消請求
403、刪除cookie中的許可證b，以及資料庫中的許可證b和許可證a的對應關係

圖 4

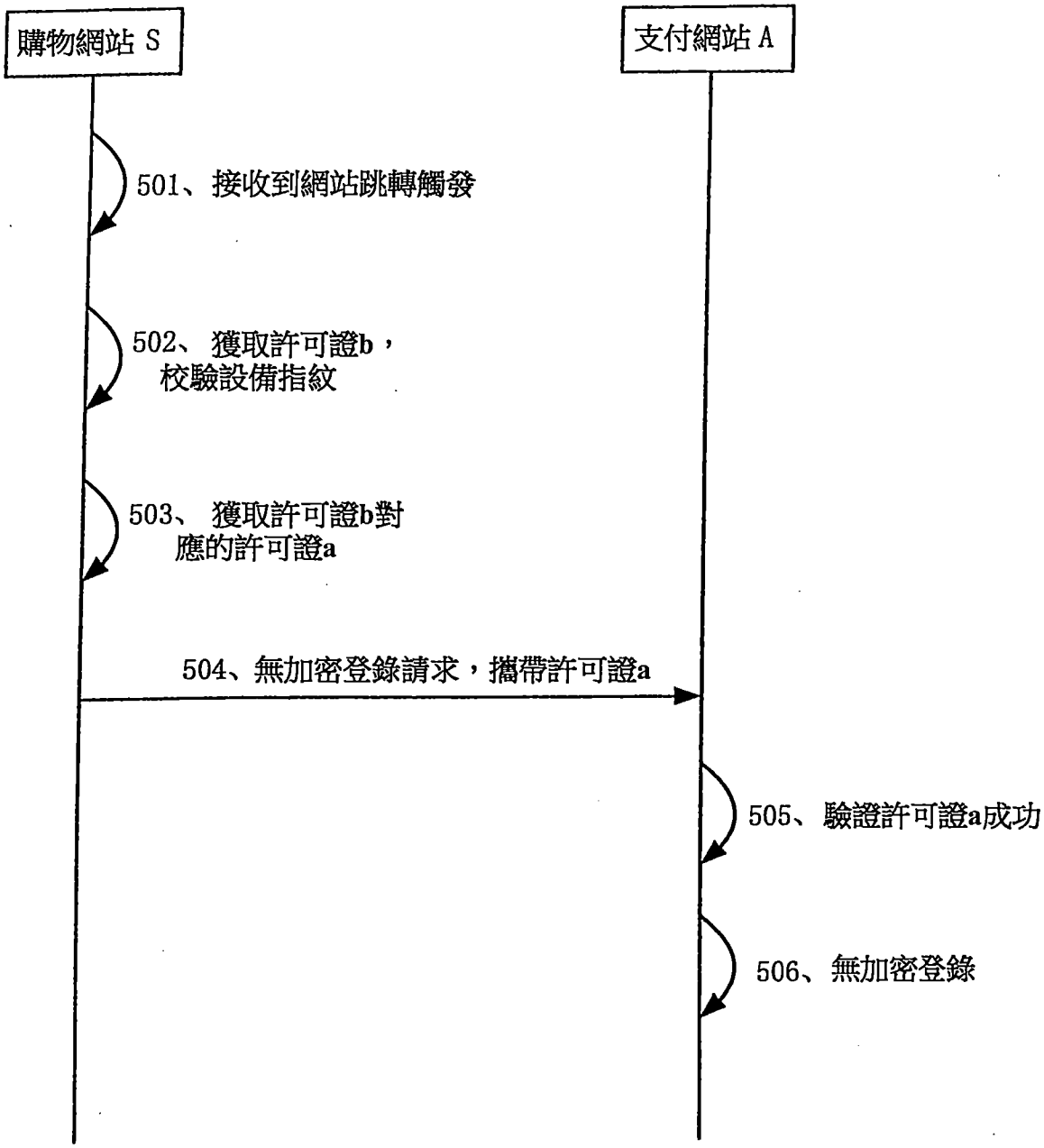
購物網站 S
支付網站 A
501、接收到網站跳轉觸發
502、 獲取許可證b，
校驗設備指紋
503、 獲取許可證b對
應的許可證a
504、無加密登錄請求，攜帶許可證a
505、驗證許可證a成功
506、無加密登錄

圖 5

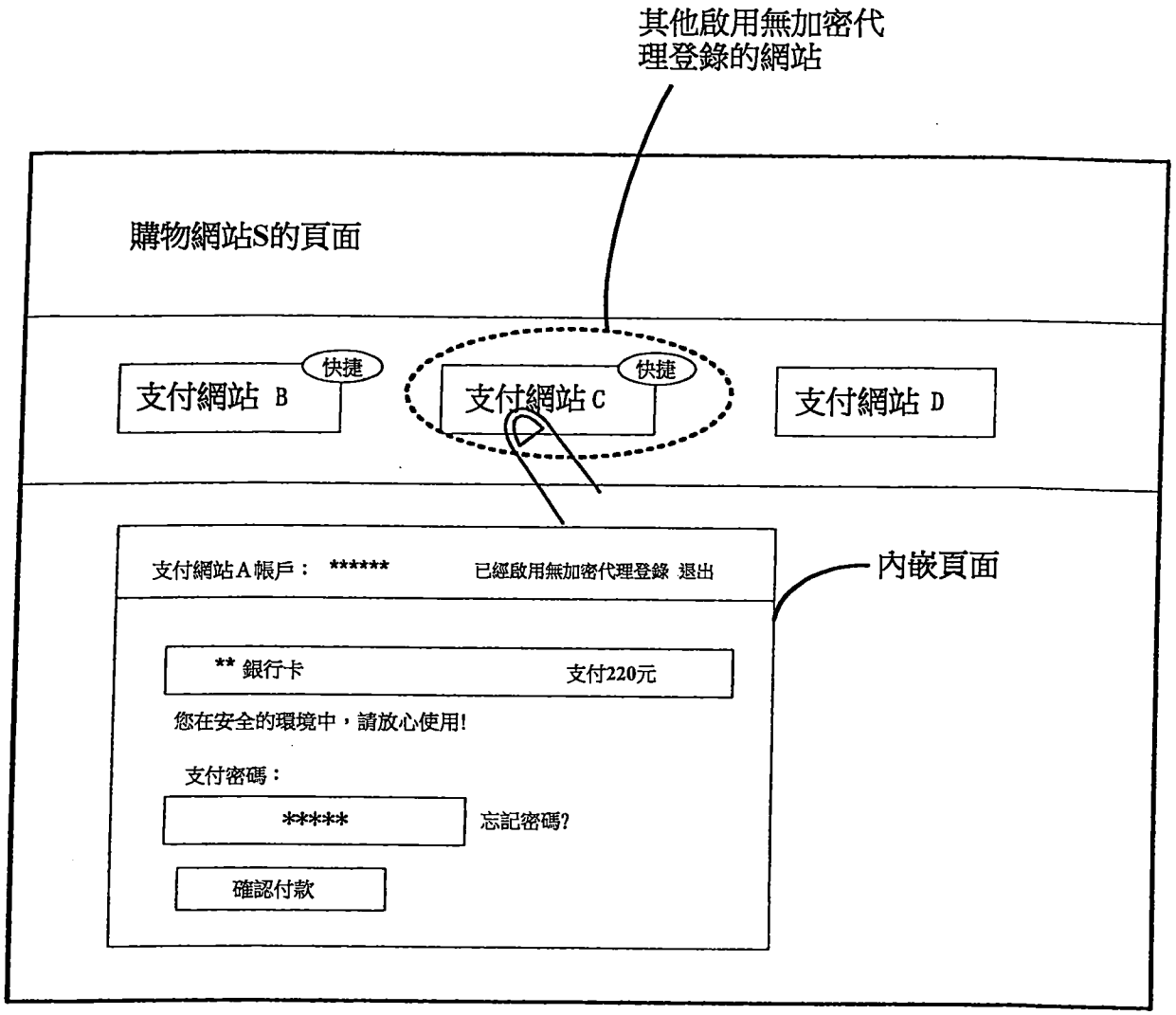
其他啟用無加密代理登錄的網站
購物網站S的頁面
快捷
支付網站 B
快捷
支付網站 C
支付網站 D
支付網站A帳戶： ******
已經啟用無加密代理登錄 退出
內嵌頁面
** 銀行卡
支付220元
您在安全的環境中，請放心使用!
支付密碼：
*****
忘記密碼?
確認付款

圖 6

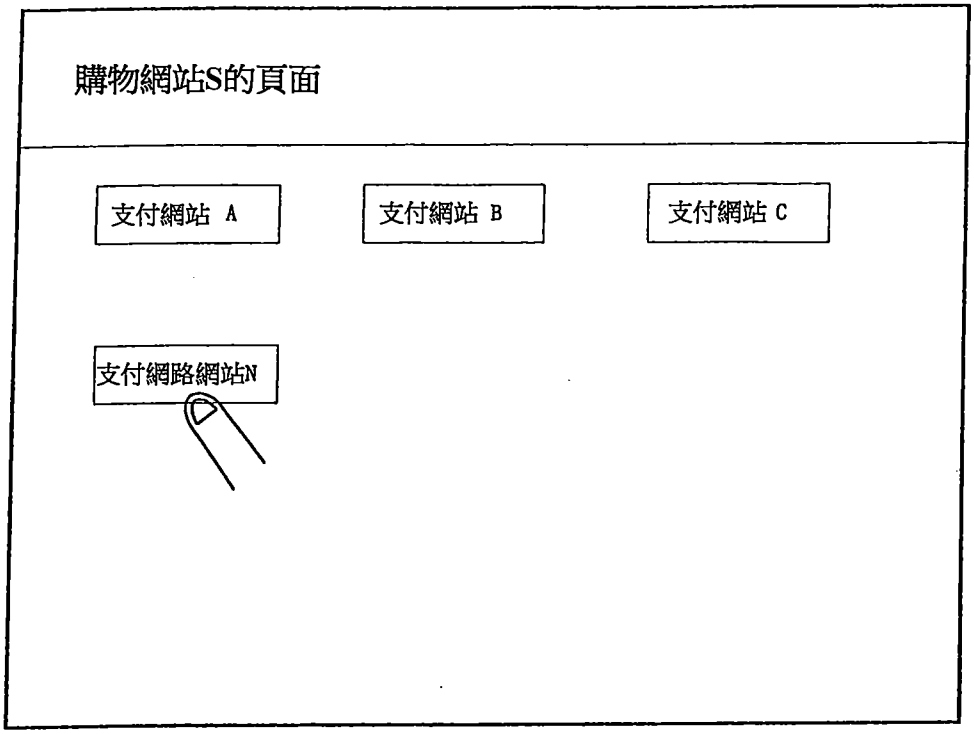
購物網站S的頁面
支付網站 A
支付網站 B
支付網站 C
支付網路網站N

圖 7

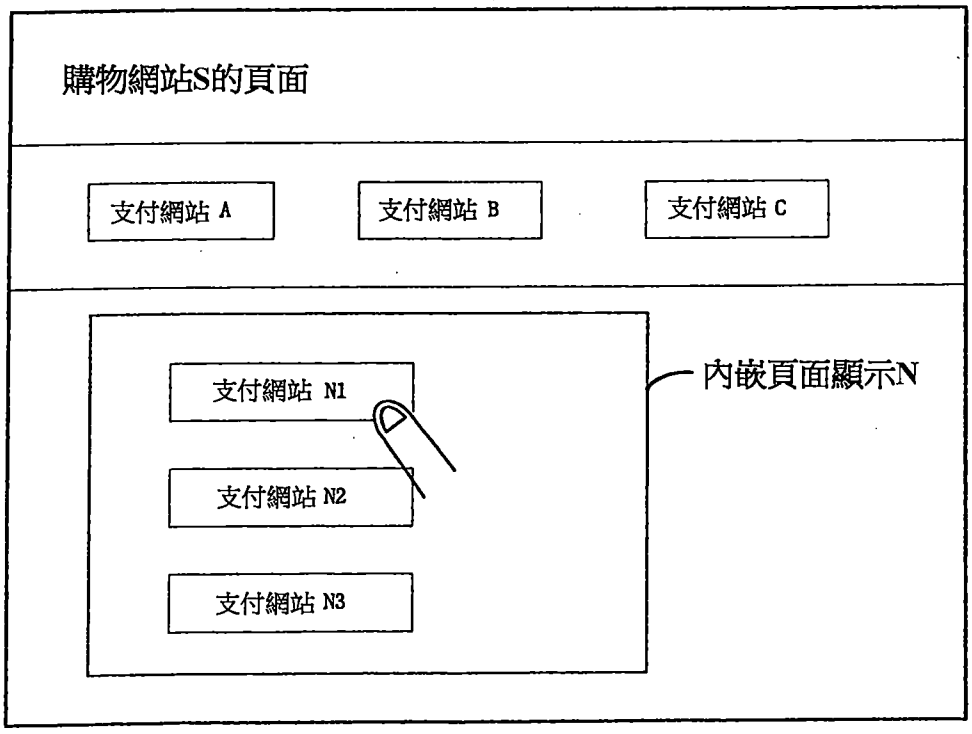
購物網站S的頁面
支付網站 A
支付網站 B
支付網站 C
支付網站 N1
支付網站 N2
支付網站 N3
內嵌頁面顯示N

圖 8

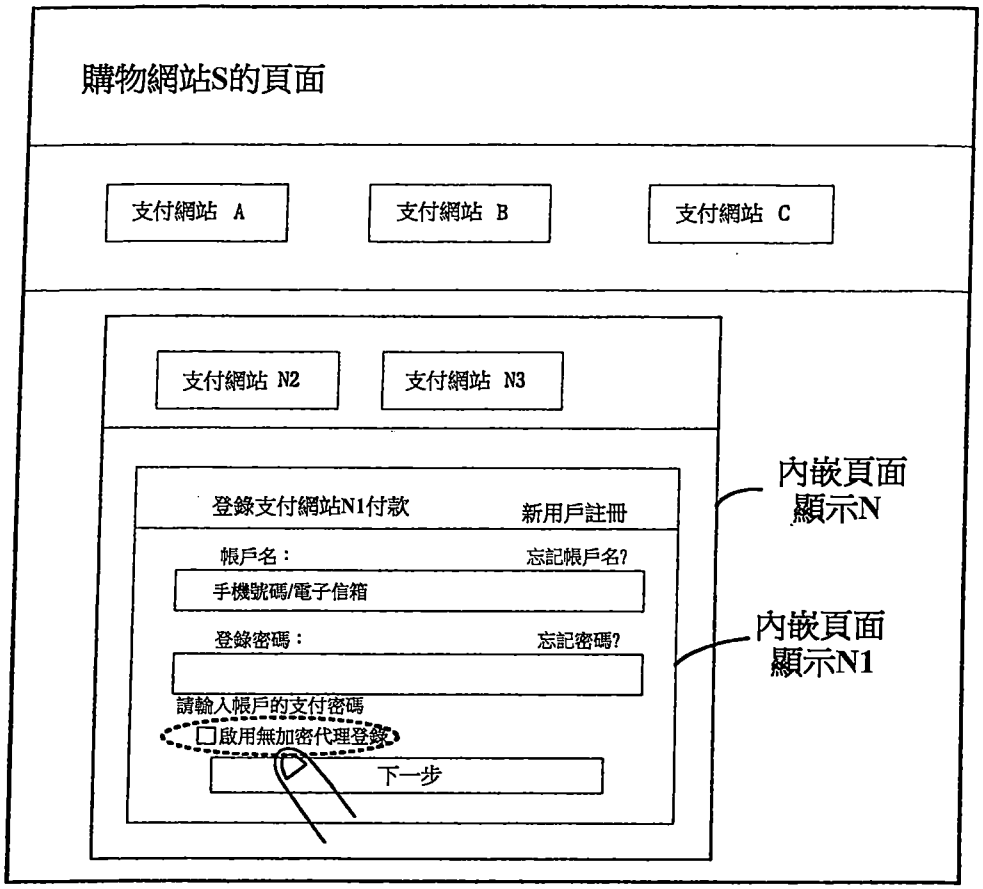
購物網站S的頁面
支付網站 A
支付網站 B
支付網站 C
支付網站 N2
支付網站 N3
登錄支付網站N1付款
新用戶註冊
帳戶名：
忘記帳戶名?
手機號碼/電子信箱
登錄密碼：
忘記密碼?
請輸入帳戶的支付密碼
啟用無加密代理登錄
下一步
內嵌頁面顯示N
內嵌頁面顯示N1

圖 9

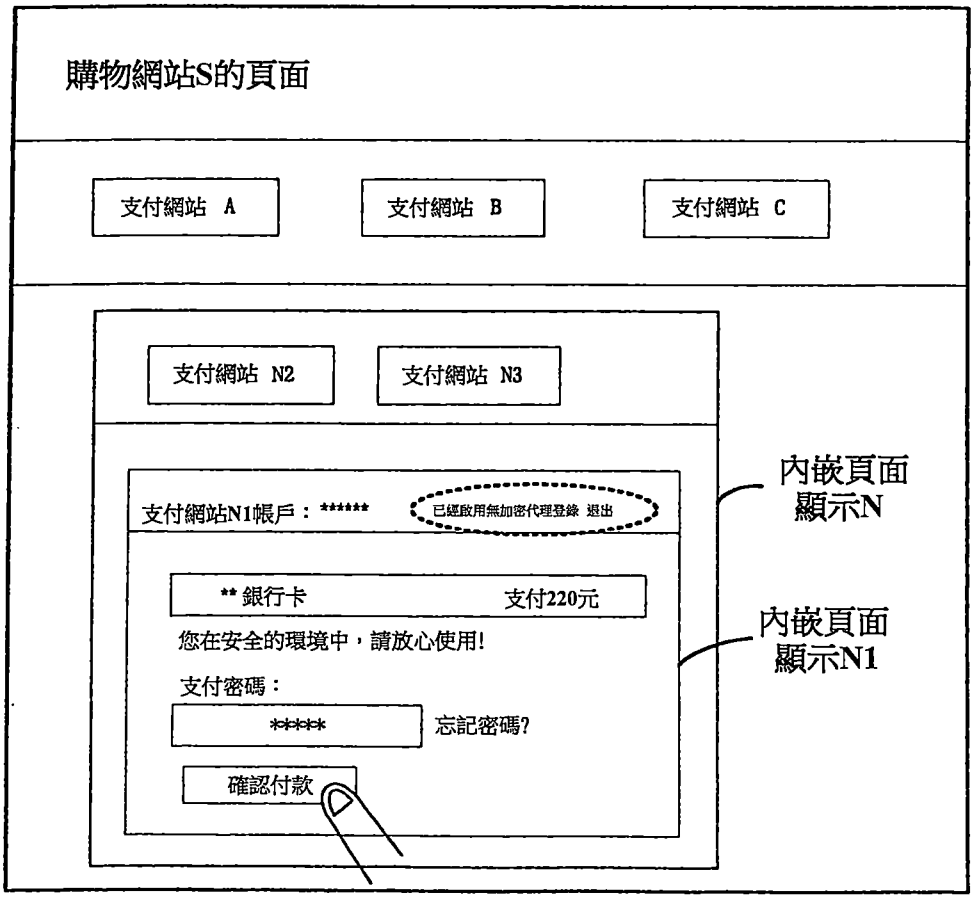
購物網站S的頁面
支付網站 A
支付網站 B
支付網站 C
支付網站 N2
支付網站 N3
支付網站N1帳戶：******
已經啟用無加密代理登錄 退出
** 銀行卡
支付220元
您在安全的環境中，請放心使用!
支付密碼：
*****
忘記密碼?
確認付款
內嵌頁面顯示N
內嵌頁面顯示N1

圖 10

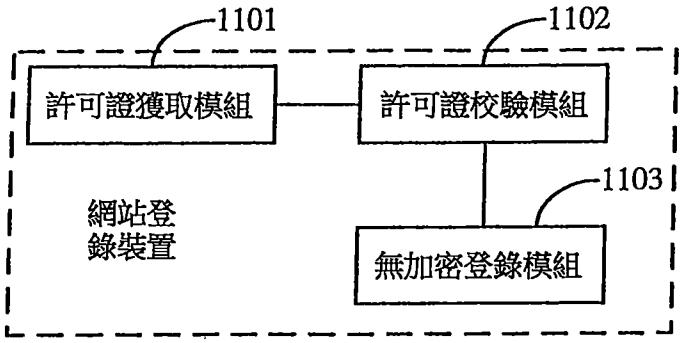
1101
1102
許可證獲取模組
許可證校驗模組
1103
網站登
錄裝置
無加密登錄模組

圖 11

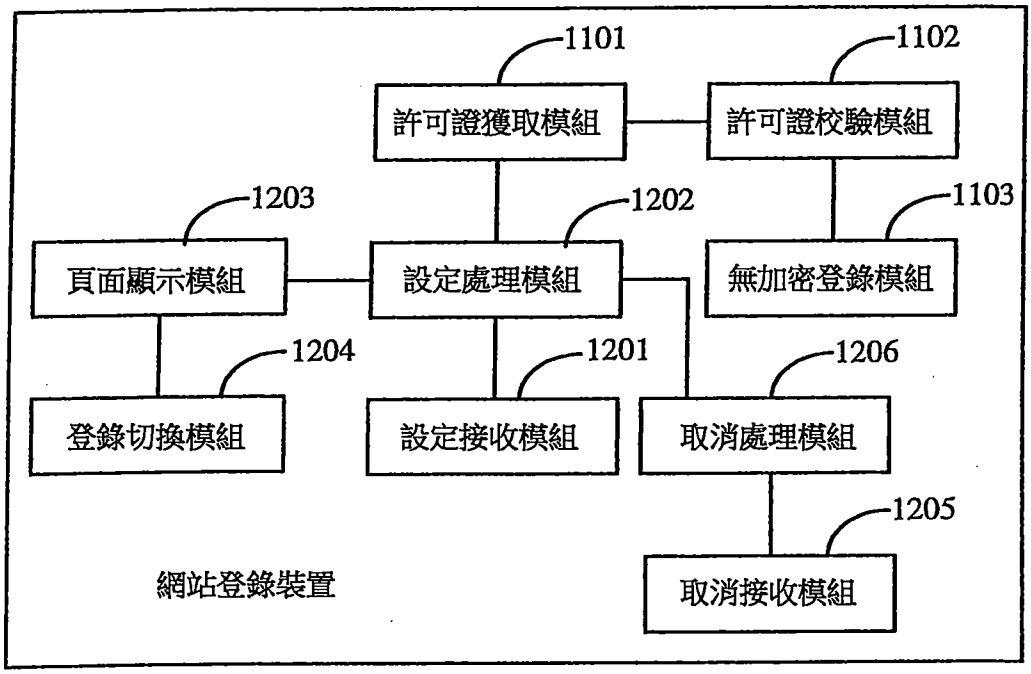
1101
1102
許可證獲取模組
許可證校驗模組
1203
1202
1103
頁面顯示模組
設定處理模組
無加密登錄模組
1204
1201
1206
登錄切換模組
設定接收模組
取消處理模組
1205
網站登錄裝置
取消接收模組

圖 12

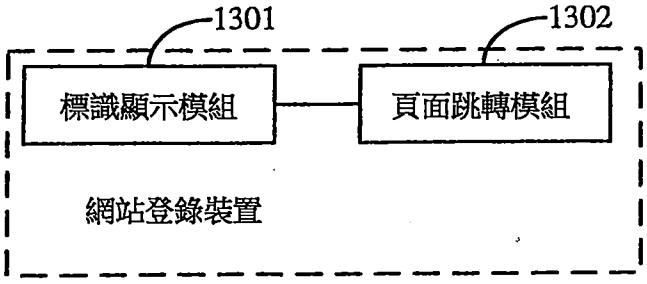
1301
1302
標識顯示模組
頁面跳轉模組
網站登錄裝置

圖 13

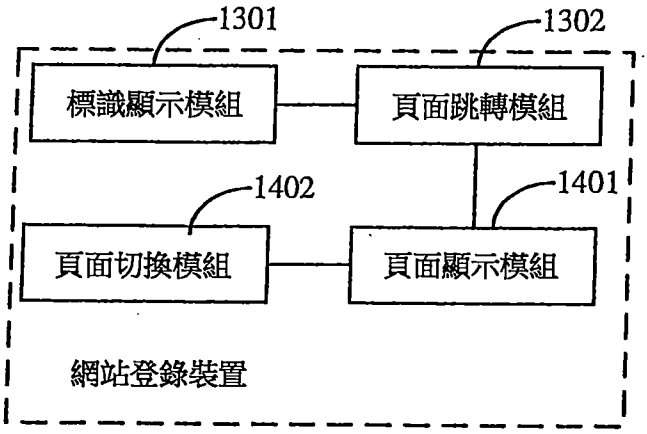
1301
1302
標識顯示模組
頁面跳轉模組
1402
1401
頁面切換模組
頁面顯示模組
網站登錄裝置

圖 14

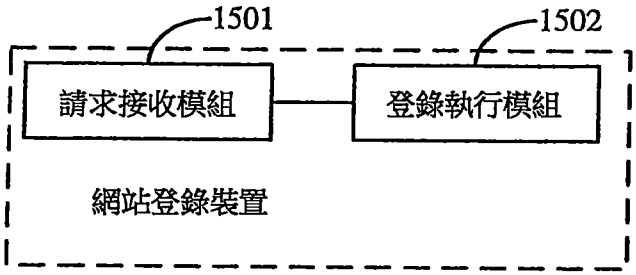
1501
1502
請求接收模組
登錄執行模組
網站登錄裝置

圖 15

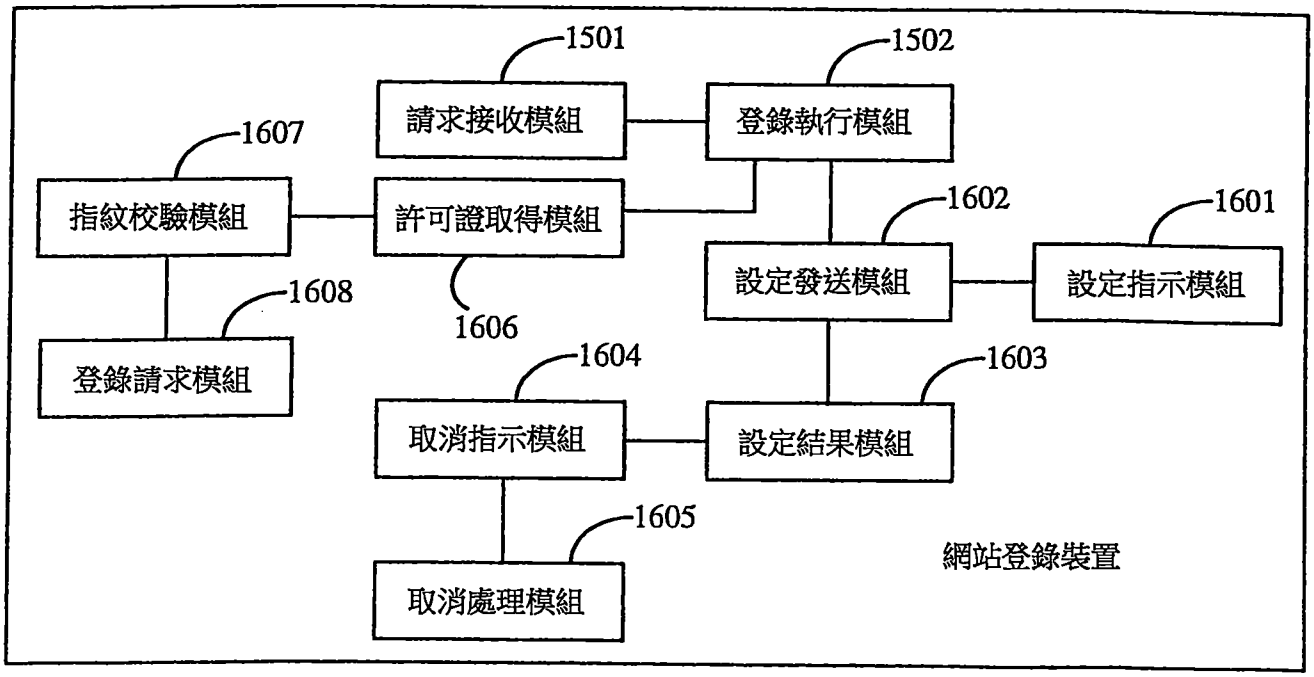
1501
1502
請求接收模組
登錄執行模組
1607
指紋校驗模組
許可證取得模組
1602
1601
設定發送模組
設定指示模組
1608
1606
登錄請求模組
1604
1603
取消指示模組
設定結果模組
1605
網站登錄裝置
取消處理模組

圖 16