

AUTOMATIC LOGIN METHOD AND DEVICE BETWEEN MULTIPLE WEBSITES

TECHNICAL FIELD

[0001] The present application relates to the communications field, and in
5 particular, to an automatic login method and device between multiple websites.

BACKGROUND

[0002] In related technologies, for different websites that cooperate with each other, a user can usually use a local client of a first website to directly visit a target page on a second website. For example, the user can add a hyperlink of the target
10 page on the second website to the local client of the first website, and the user can jump to the corresponding target page by clicking the hyperlink.

[0003] When the user visits the target page on the second website by using the local client of the first website, the second website usually requests the user to use a login ID and a password of the second website to log in to the second website so as to
15 obtain visit authorization of the target page and jump to the target page, which can be quite inconvenient.

SUMMARY

[0004] The present application provides an automatic login method between multiple websites, and the method includes the following: querying a login status of a
20 user's first login account on the first website, when a visit request for a target page on a second website is received from a user-side client; generating an automatic login token based on a token generation rule agreed by the second website, if the first login account is in a logged-in state; and creating and sending a first automatic login link to the client, where the first automatic login link includes a uniform resource locator
25 (URL) address of an automatic login portal of the second website and the automatic login token, so that the client visits the first automatic login link to send the visit

request for the target page that includes the automatic login token to the automatic login portal of the second website, and after validating the automatic login token, a server of the second website authorizes the client to perform automatic login on the second website by using a second login account bound to the first login account, and
5 jump to the target page.

[0005] In this implementation, the method further includes the following: creating and sending a second automatic login link to the client when a resource visit request for the second website is received from the user-side client, where the second automatic login link includes a URL address of a local automatic login portal, and a
10 URL address of the target page on the second website on which a resource requested by the client is located, so that the client visits the second automatic login link to send the visit request for the target page to the local automatic login portal.

[0006] In this implementation, the method further includes the following: sending a URL address of a local active login portal to the client to trigger the client to jump
15 to a login page corresponding to the URL address of the local active login portal and use the first login account to complete active login, if the first login account is in a logged-off state.

[0007] In this implementation, the token generation rule agreed by the second website includes a predetermined encryption algorithm and an encryption key that are
20 stored in login domain configuration information of the second website; and the generating an automatic login token based on a token generation rule agreed by the second website includes the following: obtaining the predetermined encryption algorithm and the encryption key from the login domain configuration information of the second website; and performing calculation on a token generation parameter
25 agreed by the second website, based on the obtained predetermined encryption algorithm and the obtained encryption key, to generate a random character string that is used as the automatic login token.

[0008] The token generation parameter includes one or a combination of the following content: the first login account, a login domain name of the first website,
30 and a generation time of the automatic login token.

[0009] The present application further provides an automatic login method between multiple websites, the method is applied to a server of a second website and the method includes the following: querying a login status of a second login account bound to a user's first login account on a first website, when a visit request for a local

target page is received from a user-side client of the first website, where the visit request includes an automatic login token generated by a server of the first website based on an appointed token generation rule; validating the automatic login token based on a token validation rule agreed by the first website, if the second login
5 account is in a logged-off state; and authorizing the client to perform automatic login locally by using the second login account when the automatic login token is validated, and sending page data of the target page to the client after successful login to trigger the client to jump to the target page.

[0010] In this implementation, the method further includes the following: if the
10 second login account is in a logged-in state, sending the page data of the target page to the client to trigger the client to jump to the target page.

[0011] In this implementation, the method further includes the following: sending a URL address of a local active login portal to the client to trigger the client to jump to a login page corresponding to the URL address of the local active login portal and
15 use the second login account to complete active login, when the automatic login token fails to be validated.

[0012] In this implementation, the token generation rule agreed by the first website includes a predetermined decryption algorithm and an encryption key that are stored in local login domain configuration information; and the validating the automatic login token based on a token validation rule agreed by the first website
20 includes the following: obtaining the predetermined decryption algorithm and the encryption key from the local login domain configuration information, decrypting the automatic login token based on the obtained predetermined decryption algorithm and the obtained encryption key, and validating whether a parameter generated after the decryption is a token generation parameter agreed by the first website; and if yes,
25 determining that the automatic login token is validated.

[0013] The token generation parameter includes one or a combination of the following content: the first login account, a login domain name of the first website, and a generation time of the automatic login token.

[0014] The present application further provides an automatic login device
30 between multiple websites, the device is applied to a server of a first website and the device includes the following: a first query module, configured to query a login status of a user's first login account on the first website, when a visit request for a target page on a second website is received from a user-side client; a generation module,

configured to generate an automatic login token based on a token generation rule agreed by the second website, if the first login account is in a logged-in state; and a transmitting module, configured to create and send a first automatic login link to the client, where the first automatic login link includes a URL address of an automatic login portal of the second website and the automatic login token, so that the client visits the first automatic login link to send the visit request for the target page that includes the automatic login token to the automatic login portal of the second website, and after validating the automatic login token, a server of the second website authorizes the client to perform automatic login on the second website by using a second login account bound to the first login account, and jump to the target page.

[0015] In this implementation, the transmitting module is further configured to create and send a second automatic login link to the client when a resource visit request for the second website is received from the user-side client, where the second automatic login link includes a URL address of a local automatic login portal and a URL address of the target page on the second website on which a resource requested by the client is located, so that the client visits the second automatic login link to send the visit request for the target page to the local automatic login portal.

[0016] In this implementation, the transmitting module is further configured to send a URL address of a local active login portal to the client to trigger the client to jump to a login page corresponding to the URL address of the local active login portal and use the first login account to complete active login, if the first login account is in a logged-off state.

[0017] In this implementation, the token generation rule agreed by the second website includes a predetermined encryption algorithm and an encryption key that are stored in login domain configuration information of the second website.

[0018] The generation module is configured to obtain the predetermined encryption algorithm and the encryption key from the login domain configuration information of the second website; and perform calculation on a token generation parameter agreed by the second website, based on the obtained predetermined encryption algorithm and the obtained encryption key, to generate a random character string that is used as the automatic login token.

[0019] The token generation parameter includes one or a combination of the following content: the first login account, a login domain name of the first website, and a generation time of the automatic login token.

[0020] The present application further provides an automatic login device between multiple websites, the device is applied to a server of a second website and the device includes the following: a second query module, configured to query a login status of a second login account bound to a user's first login account on a first website
5 when a visit request for a local target page is received from a user-side client of the first website, where the visit request includes an automatic login token generated by a server of the first website based on an appointed token generation rule; a validation module, configured to validate the automatic login token based on a token validation rule agreed by the first website, if the second login account is in a logged-off state;
10 and an authorization module, configured to authorize the client to perform automatic login locally by using the second login account when the automatic login token is validated, and send page data of the target page to the client after successful login to trigger the client to jump to the target page.

[0021] In this implementation, the authorization module is further configured to
15 send the page data of the target page to the client to trigger the client to jump to the target page, if the second login account is in a logged-in state.

[0022] In this implementation, the validation module is further configured to send a URL address of a local active login portal to the client to trigger the client to jump to a login page corresponding to the URL address of the local active login portal and
20 use the second login account to complete active login, when the automatic login token fails to be validated.

[0023] In this implementation, the token generation rule agreed by the first website includes a predetermined decryption algorithm and an encryption key that are stored in local login domain configuration information. The validation module is
25 configured to obtain the predetermined decryption algorithm and the encryption key from the local login domain configuration information, decrypt the automatic login token based on the obtained predetermined decryption algorithm and the obtained encryption key, and validate whether a parameter generated after the decryption is a token generation parameter agreed by the first website; and if yes, determine that the
30 automatic login token is validated.

[0024] The token generation parameter includes one or a combination of the following content: the first login account, a login domain name of the first website, and a generation time of the automatic login token.

[0025] In the present application, when a server of a first website receives a visit

request for a target page on a second website from a user-side client, if a user's first login account on the first website is in a logged-in state, the server of the first website can generate an automatic login token based on a token generation rule agreed by the second website, and create and send a login link to the client, where the login link includes a URL address of an automatic login portal of the second website and the automatic login token. After receiving the login link, the client can visit the login link to send the visit request for the target URL address that includes the automatic login token to the automatic login portal of the second website. After receiving the visit request, a server of the second website validates the automatic login token in the visit request if a second login account bound to the first login account is in a logged-off state. After the validation succeeds, the server of the second website authorizes the client to perform automatic login locally by using the second login account, and send page data corresponding to the target URL address to the client after successfully logged in, to trigger the client to jump to the target page corresponding to the target URL address. In the present application, the user can directly jump to the target page on the second website when visiting the target page on the second website, by using the client of the first website without manually entering the second login account and the password on the second website to perform manual login, thereby reducing operation complexity and improving user experience.

BRIEF DESCRIPTION OF DRAWINGS

[0026] FIG. 1 is a flowchart illustrating an automatic login method between multiple websites, according to an implementation of the present application;

[0027] FIG. 2 is an architectural diagram illustrating a core component, according to an implementation of the present application;

[0028] FIG. 3 is a logical block diagram illustrating an automatic login device between multiple websites, according to an implementation of the present application;

[0029] FIG. 4 is a structural diagram illustrating hardware of a server of a first website that includes an automatic login device between multiple websites, according to an implementation of the present application;

[0030] FIG. 5 is a logical block diagram illustrating another automatic login device between multiple websites, according to an implementation of the present application; and

[0031] FIG. 6 is a structural diagram illustrating hardware of a server of a second website that includes another automatic login device between multiple websites, according to an implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

5 **[0032]** In the related technologies, when a user visits a target page on a second website by using a local client of a first website, the user usually needs to enter a login ID and a password of the second website to log in to the second website, and can obtain visit authorization of the target page only after successful login and then jump to the target page, which can be quite inconvenient.

10 **[0033]** To ease the previous problem, the present application provides an automatic login method between multiple websites. When a server of a first website receives a visit request for a target page on a second website from a user-side client, if a user's first login account on the first website is in a logged-in state, the server of the first website can generate an automatic login token based on a token generation rule
15 agreed by the second website, and create and send a login link to the client, where the login link includes a URL address of an automatic login portal of the second website and the automatic login token. After receiving the login link, the client can visit the login link to send the visit request for the target URL address that includes the automatic login token to the automatic login portal of the second website. After
20 receiving the visit request, a server of the second website validates the automatic login token in the visit request if a second login account bound to the first login account is in a logged-off state. After the validation succeeds, the server of the second website authorizes the client to perform automatic login locally by using the second login account, and send page data corresponding to the target URL address to the client
25 after successfully logged in, to trigger the client to jump to the target page corresponding to the target URL address.

[0034] In the present application, the user can directly jump to the target page on the second website when visiting the target page on the second website, by using the client of the first website without manually entering the second login account and the
30 password on the second website to perform manual login, thereby reducing operation complexity and improving user experience.

[0035] The following describes the present application by using specific

implementations and with reference to specific application scenarios.

[0036] Referring to FIG. 1, FIG. 1 illustrates an automatic login method between multiple websites, according to an implementation of the present application. The method includes the following steps.

5 **[0037]** Step 101: A server of a first website queries a login status of a user's first login account on the first website, when receiving a visit request for a target page on a second website from a user-side client.

[0038] In this implementation, the user-side client can include a web client (for example, a browser) of the first website. A link to an automatic login portal of the first
10 website that is used to visit a resource on the second website can be added in advance on a user interface of the client.

[0039] The link can include a URL address of the automatic login portal of the first website, and a query parameter that needs to be transmitted to the automatic login portal of the first website when the client visits the resource on the second website.

15 **[0040]** When the user needs to use the user-side client of the first website to request to visit the resource on the second website, the user can click the link to trigger the client to send a resource visit request for the second website to the server of the first website.

[0041] After the user clicks the link, the client can generate the resource visit
20 request based on the query parameter in the link and the user's first login account on the first website, then visit the URL address of the automatic login portal of the first website, and send the generated resource visit request to the automatic login portal on the server of the first website.

[0042] In the application scenario that the user queries the service resource on the
25 second website by using the user-side client of the first website, the link for visiting the resource on the second website can be a service query link. The query parameter can include information such as a service identifier corresponding to the service resource that the user needs to query, and the resource visit request generated by the client can be a service query request.

30 **[0043]** For example, the first website is ALIPAY, and the second website is TAOBAO. The user needs to use the ALIPAY client to query details of a TAOBAO transaction that is paid by using ALIPAY. In this case, the resource visit request can be a service query request for the TAOBAO transaction, and the query parameter can be a transaction number of the TAOBAO transaction.

[0044] Assume that the transaction number of the TAOBAO transaction is "20150411252031", and a URL address of an ALIPAY's automatic login portal is "http://www.alipay.com/auto_login.htm". In this case, the service query link can be http://www.alipay.com/auto_login.htm?tradeNo=20150411252031.

5 **[0045]** In the previous link, "?" is a parameter transmission identifier in the service query link, the content behind the parameter transmission identifier is a service query parameter that needs to be transmitted to ALIPAY's automatic login portal when the ALIPAY client queries the details of the TAOBAO transaction whose transaction number is 20150411252031.

10 **[0046]** The ALIPAY client can add a "View transaction details" tag in a corresponding location of the transaction on the user interface, and the tag directs towards the service query link. When the user clicks the "View transaction details" tag on the ALIPAY client, the client can obtain the transaction number (tradeNo) in the service query link, generate a service query request that includes the trade number and
15 the user's ALIPAY account, and then visit the URL address of the ALIPAY's automatic login portal, and send the service query request to the ALIPAY's automatic login portal. The following uses the application scenario that the user queries the service resource on the second website by using the user-side client of the first website as an example for description.

20 **[0047]** In this implementation, after the server of the first website uses the automatic login portal to receive the service query request sent by the user-side client, the server of the first website can obtain the service query parameter in the service query request, and perform a corresponding service resource query in a local service database.

25 **[0048]** If the server of the first website finds the corresponding service resource in the local service database, it indicates that the service resource corresponding to the service query request is a local service resource of the first website. In this case, the server of the first website can check the login status of the first login account included in the service query request. If the first login account is in a logged-in state, it
30 indicates that the user has logged in to the first website by using the first login account, and the server of the first website can directly return the corresponding service resource to the local client.

[0049] If no corresponding service resource is found in the local service database, it indicates that the service resource corresponding to the service query request is a

non-local service resource belonging to a third-party website.

[0050] For the non-local service resource belonging to the third-party website, a mapping relationship between the service resource and a target URL address of a target page of the service resource on the third-party website is usually prestored on the server of the first server. The target URL address is the URL address of the target page on the second website that needs to be visited, when the user-side client of the first website queries the non-local service resource on the second website.

[0051] If the server of the first website does not find the service resource corresponding to the service query request in the local service database, the server of the first website can determine, based on the mapping relationship, the URL address of the target page on the second website corresponding to the service resource that needs to be queried, and then create and send an automatic login link (a second login link) to the client, where the automatic login link is used to perform automatic login in a login domain of the first website.

[0052] In this implementation, the login domain is a target system that the user wants to log in to. Multiple login domains can be maintained on the server of the first website. In practice, the server of the first website can interact with a server of another website (for example, a website that cooperates with the first website), and periodically synchronize respective login domain configuration information to the server of another website.

[0053] For example, assume that the first website is ALIPAY, and ALIPAY provides a third-party payment solution for the platforms such as TAOBAO and DANGDANG. The ALIPAY server can separately interact with TAOBAO and DANGDANG, and synchronize respective login domain configuration information to each other, so that the ALIPAY server can simultaneously maintain the login domain configuration information of the platforms such as TAOBAO and DANGDANG.

[0054] In this implementation, the automatic login link that is created and sent by the server of the first website to the client to perform automatic login in the login domain of the first website can include the URL address of the automatic login portal of the first website, the URL address of the target page on the second website on which the service resource to be visited by the user is located, and the service query parameter that needs to be transmitted to the automatic login portal of the first website when the client visits the URL address of the target page on the second website.

[0055] In an implementation, when the client visits the target page on the second

website, the service query parameter that needs to be transmitted to the automatic login portal of the first website can include a login domain name of the service request source, the URL address of the target page on the second website, a login domain name of the second website, and information such as the first login account
5 used when the user logs in to the first website.

[0056] After receiving the automatic login link sent by the server of the first website, the client can generate a visit request for the URL address of the target page on the second website based on the server query parameter included in the automatic login link, then visit the URL address of the automatic login portal of the first website,
10 and send the generated visit request for the URL address of the target page on the second website to the automatic login portal of the first website. The parameter included in the generated visit request is the same as the service query parameter included in the automatic login link.

[0057] For example, the first website is ALIPAY, the second website is TAOBAO,
15 and the user needs to use the ALIPAY client to query details of a TAOBAO transaction that is paid by using ALIPAY. Assume a URL address of an ALIPAY's automatic login portal is http://www.ALIPAY.com/auto_login.htm, a URL address of a TAOBAO's target page that the user needs to visit is www.TAOBAO.com/trade/list.htm, and an automatic login link that is created and sent by the ALIPAY server to the ALIPAY client to perform automatic login in a login
20 domain of ALIPAY can be http://www.alipay.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com.

[0058] In the automatic login link, "?" is a parameter transmission identifier in the automatic login link, the content behind the parameter transmission identifier is the service query parameter that needs to be transmitted to the ALIPAY's automatic login portal, when the ALIPAY client visits the TAOBAO's target URL address.

[0059] "loginRequestFrom=Alipay" indicates that a visit request generated by the
30 Alipay client based on the parameter is from the login domain of Alipay; "loginAccount=test_123@alipay.com" indicates that a name of an ALIPAY account used by the user to log in to the payment system is test_123@alipay.com; "target=http%3A%2F%2Fae.com%2Ftrade%2Flist.htm" is the URL address of the TAOBAO's target page visited by the ALIPAY client; and "domain=taobao" indicates

that a name of a peer login domain connected to the ALIPAY system is TAOBAO.

[0060] After receiving the automatic login link sent by the ALIPAY server, the ALIPAY client can generate a visit request for the target URL address of the second website based on the service query parameter included in the automatic login link, visit the URL address of the ALIPAY's automatic login portal, and send the visit request to the ALIPAY server.

[0061] In this implementation, when the server of the first website receives the visit request for the URL address of the target page on the second website from the local client by using the local automatic login portal, because the destination end of the visit request is the local automatic login portal, the local client needs to log in to the login domain of the first website by using the first login account to obtain visit authorization for the target URL address of the second website.

[0062] In this case, after receiving the visit request for the URL address of the target page on the second website from the client, the server of the first website can obtain the first login account from the visit request, and then locally query the login status of the first login account.

[0063] For example, during implementation, the server of the first website can use the first login account as a query index to query whether a login success validation result corresponding to the first login account is stored locally. If the login success validation result of the first login account is not stored locally, it can be determined that the first login account is in a logged-off state; if the login success validation result corresponding to the first login account is found, it can be determined that the first login account is in a logged-in state.

[0064] Step 102: If the first login account is in a logged-in state, the server of the first website generates, based on a token generation rule agreed by the second website, an automatic login token used to perform automatic login on the second website.

[0065] In this implementation, if the server of the first website finds that the first login account is in a logged-in state, it indicates that the user has logged in to the system of the first website by using the first login account. In this case, the server of the first website can generate the automatic login token (Token) based on the token generation rule agreed by the second website.

[0066] The automatic login token is used to share a login success validation result between login domains of different websites. The server of the first website can send

the generated automatic login token to a server of the second website, and share the validation result of successful login to the login domain of the first website with the second website.

5 **[0067]** In an implementation, the token generation rule agreed between the first website and the second website can be used as login domain configuration information, and is prestored in login domain configuration information of the second website that is locally maintained on the server of the first website.

10 **[0068]** The login domain configuration information usually includes an URL address of an active login portal of the login domain and an URL address of an automatic login portal, and the token generation rule can include an appointed encryption algorithm and an encryption key. Therefore, if the token generation rule agreed between the websites is also stored in the login domain configuration information, the login domain configuration information can include information such as the encryption algorithm agreed between the websites, the encryption key, and an encryption key acquisition method in addition to the URL address of the active login portal of the login domain and the URL address of the automatic login portal.

15 **[0069]** It is worthwhile to note that the encryption algorithm agreed between the first website and the second website for generating the automatic login token is not limited in this implementation. For example, the predetermined encryption algorithm can include the DSA algorithm, the RSA algorithm, the MD5 algorithm, or other symmetric encryption algorithms.

20 **[0070]** When generating the automatic login token based on the token generation rule agreed by the second website, the server of the first website can obtain the encryption algorithm and the encryption key from the login domain configuration information of the second website, perform calculation on a token generation parameter agreed by the second website, based on the obtained encryption algorithm and the obtained encryption key, to generate a random character string, and then store the generated random character string as the automatic login token.

25 **[0071]** In an implementation, the token generation parameter can include one or a combination of information such as the first login account, a login domain name of the first website, and a generation time of the automatic login token. In this implementation, when the automatic login token is generated, the token generation parameter can be information that is completely irrelevant to the user's second login account on the second website.

[0072] Certainly, in practice, the token generation parameter can include other types of information in addition to the first login account, the login domain name of the first website, and the generation time of the automatic login token, and details are omitted in this implementation.

5 **[0073]** In this implementation, if the server of the first website finds that the first login account is in a logged-off state, it indicates that the user has not logged in to the system of the first website by using the first login account. In this case, the server of the first website can send the URL address of the local active login portal to the local client.

10 **[0074]** When receiving the URL address of the active login portal, the client can visit the URL address, jump to a login page corresponding to the URL address, and then manually enter the first login account and the corresponding login password on the login page to perform active login.

[0075] Step 103: The server of the first website creates and sends a first automatic login link to the user-side client, where the first automatic login link includes an URL address of an automatic login portal of the second website and the automatic login token.

[0076] Step 104: After receiving the first login link, the user-side client of the first website visits the first login link to send the visit request for the target page to the automatic login portal of the second website, where the visit request includes the automatic login token.

20 **[0077]** In this implementation, when determining that the first login account is in a logged-in state and generates the automatic login token, the server of the first website can create and send an automatic login link (the first login link) to the user-side client to perform automatic login in the login domain of the second website, so as to redirect the visit request of the local client for the target page on the second website to the automatic login portal of the second website.

25 **[0078]** The automatic login link that is created and sent by the server of the first website to the user-side client to perform automatic login in the login domain of the second website can include the URL address of the automatic login portal of the second website, the generated automatic login token, and the service query parameter that needs to be transmitted to the automatic login portal of the second website when the client visits the URL address of the target page on the second website.

[0079] In an implementation, when the client visits the target page on the second

website, the service query parameter that needs to be transmitted to the automatic login portal of the second website can include the login domain name of the service request source, the URL address of the target page on the second website, the user's first login account used for logging in to the first website, the automatic login token generated by the server of the first website, and the generation time of the automatic login token (used by the server of the second website to validate the automatic login token).

[0080] After receiving the automatic login link sent by the server of the first website, the client can generate the visit request for the target URL address of the second website based on the service query parameter included in the automatic login link, then visit the URL address of the automatic login portal of the second website, and redirect the generated visit request for the URL address of the target page on the second website to the automatic login portal of the second website. The parameter included in the generated visit request is the same as the service query parameter included in the automatic login link.

[0081] For example, the first website is ALIPAY, the second website is TAOBAO, and the user needs to use the ALIPAY client to query details of a TAOBAO transaction that is paid by using ALIPAY. Assume a URL address of a TAOBAO's automatic login portal is http://www.taobao.com/auto_login.htm, a URL address of a TAOBAO's target page that the user needs to visit is www.taobao.com/trade/list.htm, and an automatic login link that is created and sent by the ALIPAY server to the ALIPAY client and that is used to perform automatic login in a login domain of TAOBAO can be http://www.taobao.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com&token=432085320498320841fjkdsjljfdsj&tokentime=201504111104.

[0082] "loginRequestFrom=Alipay" indicates that a visit request generated by the ALIPAY client based on the parameter is from a login domain of ALIPAY; "loginAccount=test_123@alipay.com" indicates that a name of an ALIPAY account used by the user to log in to the payment system is test_123@alipay.com; "target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm" is the encoded URL address of the TAOBAO's target page visited by the ALIPAY client; "domain=alipay" indicates that a name of a peer login domain connected to the TAOBAO system is ALIPAY; "token=432085320498320841fjkdsjljfdsj" indicates an automatic login token

generated on the ALIPAY server; and "tokentime=201504111104" indicates a generation time of the automatic login token.

[0083] After receiving the automatic login link sent by the ALIPAY server, the ALIPAY client can generate a visit request for the URL address of the TAOBAO's target page based on the service query parameter included in the automatic login link. Then the ALIPAY client can visit the URL address of the TAOBAO's automatic login portal, and send the visit request to the TAOBAO server.

[0084] Step 105: A server of the second website queries a login status of a second login account bound to the user's first login account on the first website, when receiving the visit request for the local target page from the user-side client of the first website.

[0085] In this implementation, the user logs in to the first login account of the first website, and the first login account can be bound in advance to the second login account for the user to log in to the second website. The binding relationship can be separately prestored on the server of the first website and the server of the second website.

[0086] For example, the first website is ALIPAY, and the second website is TAOBAO. Assume that the first login account is a user's ALIPAY account test_123@alipay.com for logging in to the ALIPAY system, and the second login account is a user's TAOBAO account test_123@taobao.com for logging in to the TAOBAO system. In this case, the ALIPAY server and the TAOBAO server can separately store a binding relationship between test_123@alipay.com and test_123@taobao.com.

[0087] When receiving the visit request for the URL address of the local target page from the local client of the first website, the server of the second website can obtain the first login account from the visit request, and query the second login account bound to the first login account based on the established binding relationship. When finding the second login account bound to the first login account, the server of the second website can locally query the login status of the second login account.

[0088] Step 106: The server of the second website validates the automatic login token based on a token validation rule agreed by the first website if the second login account is in a logged-off state.

[0089] In this implementation, if the server of the second website finds that the second login account is in a logged-off state, the server can obtain the automatic login

token included in the visit request, and validate the automatic login token based on the token validation rule agreed by the first website.

[0090] The token validation rule agreed between the second website and the first website corresponds to the token generation rule used when the first website generates the automatic login token.

[0091] In this implementation, the token validation rule can still be used as the login domain configuration information, and is prestored in the login domain configuration information of the second website. The token validation rule can include an appointed encryption algorithm and an encryption key, where the encryption algorithm and the encryption key that are used as the token validation rule need to be the same as the encryption algorithm and the encryption key that are used when the server of the first website generates the automatic login token.

[0092] When validating the automatic login token, the server of the second website can obtain the encryption algorithm and the encryption key from the local login domain configuration information, and perform reverse decryption calculation on the automatic login token based on the obtained encryption algorithm and the obtained encryption key to obtain several parameters. Then the server of the second website can validate the parameters obtained through validation decryption, and determine whether the parameters are the same as the token generation parameters that are agreed by the first website and that are used to generate the automatic login token.

[0093] For example, when the server of the first website generates the automatic login token, the token generation parameter includes information such as the first login account, the login domain name of the first website, and the generation time of the automatic login token (the token generation parameter can be included in the visit request sent by the client). When validating the automatic login token, the server of the second website can perform reverse decryption on the automatic login token based on the same algorithm and the same encryption key to obtain several parameters. Then the server of the second website can compare the parameters obtained through reverse decryption with the token generation parameters used by the server of the first website for generating the automatic login token. When all the information such as the first login account, the login domain name of the first website, and the generation time of the automatic login token are matched, the server of the second website determines that the automatic login token is validated. Otherwise, if any parameter in the

previous parameters does not match, the server of the second website can determine that the automatic login token fails to be validated.

[0094] Step 107: The server of the second website authorizes the client to perform automatic login locally by using the second login account when the automatic login token is validated, and sends page data of the target page to the client after successful login to trigger the client to jump to the target page.

[0095] In this implementation, if the server of the second website validates the automatic login token, the server of the second website can directly confirm, in the local login domain, that the first login account successfully logs in to the login domain of the first website. That is, the server of the second website can determine, by validating the automatic login token, whether the login result of the user on the first website can be directly shared in the login domain of the second website.

[0096] In this case, the server of the second website can perform login authorization on the second login account in the login domain of the second website, and authorize the client to perform automatic login in the login domain of the second website by using the second login account bound to the first login account. In the entire process, the server of the second website does not need to perform any form of login validation on the second login account.

[0097] After the automatic login succeeds, the client has obtained the visit authorization for the target URL address on the second website, and the server of the second website can send the page data corresponding to the target URL address to the client to trigger the client to jump to the corresponding target page.

[0098] Certainly, if the automatic login token fails to be validated, the server of the second website can send the URL address of the local active login portal to the local client. When receiving the URL address of the active login portal, the client can visit the URL address, jump to the login page corresponding to the URL address, and then manually enter the second login account and the corresponding login password on the login page to perform active login.

[0099] Step 108: The user-side client of the first website jumps to the target page after receiving the page data of the target page.

[0100] In this implementation, after receiving the page data that is sent by the server of the second website and that is corresponding to the target URL address, the user-side client of the first website can load the received page data in the browser, and then jump to the target page corresponding to the target URL address.

[0101] In this case, the user completes visit to the target page on the second website by using the user-side client of the first website. In the entire process, when visiting the target page on the second website, the user-side client of the first website needs to validate whether the user successfully logs in to the first website by using the first login account. If the user has logged in to the first website by using the first login account, the automatic login token can be generated to share the validation result of user's successful login to the first website with the second website. After the second website validates the automatic login token, automatic login is performed by using the second login account bound to the first login account. Any form of authentication does not need to be performed on the second login account in the entire login process.

[0102] In the previously described implementation, when the user visits the target page on the second website by using the user-side client of the first website, if the user's first login account on the first website has logged in to the login domain of the first website, the server of the first website can generate the automatic login token based on the token generation rule agreed by the server of the second website, send the automatic login token to the server of the second website, and share the validation result that the first login account successfully logs in to the login domain of the first website with the second website.

[0103] The server of the second website can validate the automatic login token. The server can directly authorize the client to log in to the login domain of the second website by using the second login account bound to the first login account if the validation succeeds, so that the user can directly jump to the target page by using the client without repeatedly entering the second login account and the login password on the login page to log in to the second website. Because any form of validation does not need to be performed on the second login account in the entire login process, operation complexity can be reduced and user experience can be improved.

[0104] It is worthwhile to note that the previously described implementation describes a detailed process of visiting the target page on the second website by the user by using the user-side client of the first website. In practice, the user can visit a target page on the first website by using a user-side client of the second website, and details are omitted in the present application. For implementation, a person skilled in the art can refer to the descriptions of the previously described implementation.

[0105] The following described the technical solution in the previously described implementation by using an example in which the first website is ALIPAY and the

second website is TAOBAO and with reference to an application scenario that the user views TAOBAO transaction details by using the ALIPAY client.

[0106] In this example, the scenario includes a browser of the ALIPAY client, an ALIPAY server, and a TAOBAO server.

5 **[0107]** In this example, ALIPAY can be used as a third-party payment company to provide online payment for TAOBAO. In the ALIPAY's transaction history, the user can usually view transaction information of all third parties that are related to payment, and the transaction information in ALIPAY usually includes only digest information of the transaction. For example, the transaction information can include
10 only a transaction name. Therefore, if the user needs to view the transaction details, the user needs to jump to the TAOBAO website for query.

[0108] In the related technologies, when the user jumps to the TAOBAO website by using the browser to query the transaction details, the TAOBAO system usually requires the user to enter a login account registered in TAOBAO and a login password.
15 After successful login, the user has authorization to view the transaction details, which can be quite inconvenient.

[0109] In this example, to enable the browser to automatically jump to the target page of the transaction details when the user views the TAOBAO transaction details in the ALIPAY's transaction history, a same core component can be integrated in an
20 ALIPAY website architecture and a TAOBAO website architecture.

[0110] Referring to FIG. 2, FIG. 2 is an architectural diagram illustrating a core component, according to an implementation of the present application.

[0111] The core component architecture shown in FIG. 2 includes an auto login service (ALS) controller, a token (automatic login token) generate service (TGS)
25 component, a token validate service (TVS) component, a login service (LS) component, and login domain configuration information.

[0112] The auto login service controller is a main automatic login portal and is responsible for controlling all processes of automatic login. The user can visit the URL address of the automatic login portal by using the browser, access the auto
30 service controller, and transmit a parameter to the auto login service controller to implement automatic login.

[0113] The token generate service component is running in a logged-in system, and is configured to generate a token based on a token generation rule agreed by a peer login system. Main parameters for generating the token can include a logged-in

account, a peer login domain name, and a token generation time. The token generation rule is agreed between websites, and can include symmetric encryption algorithms such as DSA, RSA, or MD5 and an encryption key.

[0114] The token validate service component is running in a system to be logged in, and is configured to validate, based on an appointed token validation rule, the token that is sent by the logged-in system. A validation method corresponds to the generation rule when the token generate service component generates the token.

[0115] The login service component is configured to check whether a login pending account currently logs in to the system, and performs automatic login for the login pending account.

[0116] The login domain configuration information is responsible for managing configuration information of each login domain, including information such as a URL address of an active login portal of each login domain, a URL address of an automatic login portal, an encryption algorithm, an encryption key, or an encryption key acquisition method.

[0117] In this implementation, assume that a user's first login account for ALIPAY is test_123@alipay.com, and a user's second login account for TAOBAO is test_123@taobao.com. A binding relationship between test_123@alipay.com and @taobao.com can be prestored on a TAOBAO server.

[0118] An ALIPAY's transaction history includes digest information of a TAOBAO transaction. In a predetermined location of the digest information, a "View transaction details" tag is added in advance, and the tag corresponds to a URL address http://www.alipay.com/auto_login.htm of an ALIPAY's automatic login portal.

[0119] When the user clicks the "View transaction details" tag to jump to a TAOBAO's transaction page and query details of the TAOBAO transaction, the browser sends a query request for the transaction details to the ALIPAY server. After receiving the query request, and finding a URL address www.taobao.com/trade/list.htm of the TAOBAO's transaction page based on a mapping relationship, the ALIPAY server can send a first automatic login link http://www.alipay.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com to the browser.

[0120] After receiving the first automatic login link, the browser generates a visit request for the URL address of the TAOBAO's transaction page, visits the URL

address of the ALIPAY's automatic login portal, and sends the visit request to the automatic login portal of the ALIPAY server.

[0121] In this case, information included in the visit request includes the visit request source ALIPAY, the URL address of the TAOBAO's transaction page, a login domain name of TAOBAO, and the ALIPAY account test_123@alipay.com that the user needs to log in to.

[0122] The ALS component on the ALIPAY server processes the visit request, and finds that the visit request is from the local login domain. In this case, the ALS component triggers generation of the token, and invokes the LS component to query a login status of the login account test_123@alipay.com. If the login account test_123@alipay.com is in a logged-in state, the ALS component continues to invoke the TGS component to generate the token.

[0123] After the token is generated, the ALS component obtains configuration information of a login domain of TAOBAO, and creates and sends a second automatic login link to the ALIPAY client to redirect the visit request from the ALIPAY client for the URL address of the TAOBAO's transaction page to a TAOBAO's automatic login portal.

[0124] In this case, the second automatic login link is http://www.taobao.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com&token=432085320498320841fjkdsjljfdsj&tokentime=201504111104.

[0125] After receiving the second automatic login link, the browser generates a visit request for the URL address of the TAOBAO's transaction page again, visits the URL address of the TAOBAO's automatic login portal, and redirects the newly-generated visit request to the TAOBAO's automatic login portal.

[0126] In this case, information included in the visit request includes the visit request source ALIPAY, the URL address of the TAOBAO's transaction page, a login domain name of ALIPAY (the peer login domain changes after the redirection), the ALIPAY account test_123@alipay.com that the user needs to log in to, the generated token, and a generation time of the token.

[0127] The ALS component on the TAOBAO server processes the visit request, and finds that the visit request is from the login domain of ALIPAY. In this case, the ALS component triggers validation of the token, and invokes the LS component to query a login status of the login account test_123@taobao.com that is bound to

test_123@alipay.com. If the login account test_123@taobao.com is in a logged-in state, the ALS component continues to invoke the TVS component to validate the token.

[0128] When the token is validated, the TAOBAO system confirms that the user successfully logs in to the login domain of ALIPAY by using test_123@alipay.com. In this case, the ALS component can invoke the LS component to authorize the login account test_123@taobao.com to perform automatic login.

[0129] When the login account test_123@taobao.com automatically logs in to the login domain of TAOBAO, the TAOBAO server can send page data of the transaction page corresponding to www.TAOBAO.com/trade/list.htm to the browser of the ALIPAY client. After receiving the page data from the TAOBAO server, the browser can load the page data, and then automatically jump to the TAOBAO's transaction page to display the details of the TAOBAO transaction to the user.

[0130] In this case, the user has completed the operation of viewing the details of the TAOBAO transaction in the ALIPAY's transaction history. In the entire process, the user does not need to enter the TAOBAO login account test_123@taobao.com and the login password on the login page to log in to the login domain of TAOBAO, and the browser can automatically jump to the TAOBAO's transaction page to display the transaction details to the user.

[0131] Corresponding to the previously described method implementation, the present application further provides an apparatus implementation.

[0132] Referring to FIG. 3, the present application provides an automatic login device 30 between multiple websites, and the device is applied to a server of a first website. Referring to FIG. 4, a hardware architecture of a server that includes the automatic login device 30 between multiple websites generally includes a CPU, a memory, a nonvolatile memory, a network interface, an internal bus, etc. In an example in which the automatic login device 30 between multiple websites is implemented by software, the automatic login device 30 between multiple websites can be usually understood as a computer program loaded in the memory, and forms a logical software and hardware combined device after running by using the CPU. The device 30 includes the following: a first query module 301, configured to query a login status of a user's first login account on the first website, when a visit request for a target page on a second website is received from a user-side client; a generation module 302, configured to generate an automatic login token based on a token

generation rule agreed by the second website, if the first login account is in a logged-in state; and a transmitting module 303, configured to create and send a first automatic login link to the client, where the first automatic login link includes a URL address of an automatic login portal of the second website and the automatic login token, so that the client visits the first automatic login link to send the visit request for the target page that includes the automatic login token to the automatic login portal of the second website, and after validating the automatic login token, a server of the second website authorizes the client to perform automatic login on the second website by using a second login account bound to the first login account, and jump to the target page.

[0133] In this implementation, the transmitting module 303 is further configured to create and send a second automatic login link to the client when a resource visit request for the second website is received from the user-side client, where the second automatic login link includes a URL address of a local automatic login portal and a URL address of the target page on the second website on which a resource requested by the client is located, so that the client visits the second automatic login link to send the visit request for the target page to the local automatic login portal.

[0134] In this implementation, the transmitting module 303 is further configured to send a URL address of a local active login portal to the client to trigger the client to jump to a login page corresponding to the URL address of the local active login portal, and use the first login account to complete active login, if the first login account is in a logged-off state.

[0135] In this implementation, the token generation rule agreed by the second website includes a predetermined encryption algorithm and an encryption key that are stored in login domain configuration information of the second website.

[0136] The generation module 302 is configured to obtain the predetermined encryption algorithm and the encryption key from the login domain configuration information of the second website; and perform calculation on a token generation parameter agreed by the second website, based on the obtained predetermined encryption algorithm and the obtained encryption key, to generate a random character string that is used as the automatic login token.

[0137] The token generation parameter includes one or a combination of the following content: the first login account, a login domain name of the second website, and a generation time of the automatic login token.

[0138] Referring to FIG. 5, the present application provides another automatic login device 50 between multiple websites, and the device is applied to a server of a second website. Referring to FIG. 6, a hardware architecture of a server that includes the automatic login device 50 between multiple websites generally includes a CPU, a memory, a nonvolatile memory, a network interface, an internal bus, etc. In an example in which the automatic login device 50 between multiple websites is implemented by software, the automatic login device 50 between multiple websites can be usually understood as a computer program loaded in the memory, and forms a logical software and hardware combined device after being processed by the CPU.

10 The device 50 includes the following: a second query module 501, configured to query a login status of a second login account bound to a user's first login account on a first website when a visit request for a local target page is received from a user-side client of the first website, where the visit request includes an automatic login token generated by a server of the first website based on an appointed token generation rule;

15 a validation module 502, configured to validate the automatic login token based on a token validation rule agreed by the first website if the second login account is in a logged-off state; and an authorization module 503, configured to authorize the client to perform automatic login locally by using the second login account when the automatic login token is validated, and send page data of the target page to the client

20 after successful login to trigger the client to jump to the target page.

[0139] In this implementation, the authorization module 503 is further configured to send the page data of the target page to the client to trigger the client to jump to the target page, if the second login account is in a logged-in state.

[0140] In this implementation, the validation module 502 is further configured to

25 send a URL address of a local active login portal to the client to trigger the client to jump to a login page corresponding to the URL address of the local active login portal and use the second login account to complete active login, when the automatic login token fails to be validated.

[0141] In this implementation, the token generation rule agreed by the first

30 website includes a predetermined decryption algorithm and an encryption key that are stored in local login domain configuration information.

[0142] The validation module 502 is configured to obtain the predetermined decryption algorithm and the encryption key from the local login domain configuration information, decrypt the automatic login token based on the obtained

predetermined decryption algorithm and the obtained encryption key, and validate whether a parameter generated after the decryption is a token generation parameter agreed by the first website; and if yes, determine that the automatic login token is validated.

5 **[0143]** The token generation parameter includes one or a combination of the following content: the first login account, a local login domain name, and a generation time of the automatic login token.

10 **[0144]** A person skilled in the art can easily figure out another implementation solution of the present application after considering the specification and practicing the present application. The present application is intended to cover any variations, functions, or adaptive changes of the present application. These variations, functions, or adaptive changes comply with general principles of the present application, and include common knowledge or a commonly used technical means in the technical field that is not disclosed in the present application. The specification and the
15 implementations are merely considered as examples, and the actual scope and the spirit of the present application are described by the following claims.

20 **[0145]** It should be understood that the present application is not limited to the accurate structures that are described above and that are shown in the accompanying drawings, and modifications and changes can be made without departing from the scope of the present application. The scope of the present application is limited only by the appended claims.

25 **[0146]** The previous descriptions are merely preferred implementations of the present application, but are not intended to limit the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.

CLAIMS

1. A computer-implemented method, comprising:

receiving, by a server of a first website, a request from a user for logging in to an account of a second website associated with an account of the first website;

determining, by the server of the first website, that the account of the first website is logged in to by the user;

generating, by the server of the first website, an automatic login token based on one or more token generation rules agreed to by the second website for performing an automatic login on the second website, wherein the one or more token generation rules include a predetermined encryption algorithm and an encryption key that are stored in configuration information of a login domain of the second website, wherein generating the automatic login token comprises:

obtaining the predetermined encryption algorithm and the encryption key from the configuration information of the login domain of the second website; and

generating the automatic login token based on one or more token generation parameters encrypted by the encryption key using the predetermined encryption algorithm; and

generating and sending, by the server of the first website, an automatic login link to the user; wherein the automatic login link includes the automatic login token, the automatic login link allowing the user to send an automatic login request that includes the automatic login token, and wherein the automatic login token is verified based on one or more token verification rules to allow the user to automatically log in to the account of the second website.

2. The computer-implemented method of claim 1, wherein the automatic login link includes a uniform resource locator (URL) address that includes an URL field of a target page, the URL address directing the user to the target page after the user automatically logs in to the second website with the account of the second website.

3. The computer-implemented method of claim 1, wherein the predetermined encryption algorithm is agreed to by the first website and the second website.

4. The computer-implemented method of claim 1, wherein the one or more token generation parameters include at least one of the account of the first website, a login domain name of the first website, and a time the automatic login token is generated.

5. The computer-implemented method of claim 1, wherein the automatic login token is a random character string.

6. The computer-implemented method of claim 1, wherein the account of the second website is not logged in to the second website by the user before the automatic login token is verified.

7. A non-transitory, computer-readable medium storing one or more instructions when executed by a computer system to perform the method of any one of claims 1 to 6.

8. A computer-implemented system, comprising:
one or more computers; and
one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform the method of any one of claims 1 to 6.