

CLAIMS

1. A trusted login method, comprising:

obtaining device identifier information of a user login device after a first login state of a user in a first application is established, and associating the device identifier information with the first login state; and

sending the device identifier information and the first login state to a server of a second application prior to the user making a request to access the second application, the second application being a trusted login application associated with the first application, such that the server establishes a second login state of the user in the second application according to the first login state, and associates the device identifier information with the second login state.

2. The method of claim 1, wherein obtaining device identifier information of a user login device comprises: generating the device identifier information according to device information and login information.

3. The method of claim 1, wherein, after sending the device identifier information and the first login state to the server of the second application, the method further comprises:

receiving a validity query request for the first login state sent by the server, and feeding validity of the first login state back to the server.

4. The method of claim 1, wherein sending the first login state to the server of the second application comprises sending information indicating that the user has logged into the first application.

5. A trusted login method, comprising:

receiving a first login state and device identifier information sent by a server of a first application (105), the first application being a trusted login application associated with a second application, the first login state representing that a user logs into the first application, and the device identifier information being used for representing a login device on which the user logs into the first application;

establishing a second login state of the user in the second application according to the first login state;

associating and storing the device identifier information and the second login state; and
upon receipt of an application access request for the second application, returning an application access response if it is determined that identifier information of a device sending the application access request and a corresponding second login state have been stored.

6. The method of claim 5, wherein, after establishing a second login state of the user in the second application, the method further comprises:

establishing a corresponding relation between the first login state and the second login state;
and

after it is determined that the identifier information of the device sending the application access request and the corresponding second login state have been stored, and before returning the application access response, the method further comprises:

sending a validity query request for the first login state to the server, and
determining that the first login state and the second login state are valid.

7. A trusted login apparatus, comprising:

a login state generation module configured to obtain device identifier information of a user login device after a first login state of a user in a first application is established, and associate the device identifier information with the first login state; and

a login state synchronization module configured to send the device identifier information and the first login state to a server of a second application prior to the user making a request to access the second application, the second application being a trusted login application associated with the first application, such that the server establishes a second login state of the user in the second application according to the first login state, and associates the device identifier information with the second login state.

8. The apparatus of claim 7, wherein,

when obtaining the device identifier information of the user login device, the login state generation module is specifically configured to generate the device identifier information according to device information and login information.

9. The apparatus of claim 7, further comprising:

a login state management module configured to receive a validity query request for the first login state sent by the server, and feed validity of the first login state back to the server.

10. The apparatus of claim 7, wherein sending the first login state to the server of the second application comprises sending information indicating that the user has logged into the first application.

11. A trusted login apparatus, comprising:

a login state receiving module configured to receive a first login state and device identifier information sent by a server of a first application, the first application being a trusted login application associated with a second application, the first login state representing that a user logs into the first application, and the device identifier information being used for representing a login device on which the user logs into the first application;

a login state establishment module configured to establish a second login state of the user in the second application according to the first login state, and associate and store the device identifier information and the second login state; and

an access management module configured to, upon receipt of an application access request for the second application, return an application access response if it is determined that identifier information of a device sending the application access request and a corresponding second login state have been stored.

12. The apparatus of claim 11, wherein,

the login state establishment module is further configured to establish a corresponding relation between the first login state and the second login state after the second login state of the user in the second application is established; and

the access management module is further configured to, after it is determined that the identifier information of the device sending the application access request and the corresponding second login state have been stored, and before returning the application access response, send a validity query request for the first login state to the server, and determine that the first login state and the second login state are valid.