CLAIMS

1. A computer-implemented method, the method comprising:

receiving, at a second server and from a target client terminal, a request for trusted login, wherein the request for trusted login comprises a request to access a service page provided by a first server;

generating, by the second server, a trusted login token acquisition request, wherein the trusted login token acquisition request is based on the request for trusted login and a current trusted login identifier, the generating comprising:

obtaining the current trusted login identifier issued by the first server to the second server, wherein the current trusted login identifier certifies the second server to obtain a temporary trusted login token, and writing the current trusted login identifier into the request to access the service page provided by the first server to generate the trusted login token acquisition request;

sending, from the second server, the trusted login token acquisition request to the first server;

receiving, at the second server, a temporary trusted login token from the first server, wherein the temporary trusted login token includes a service authorization that identifies one or more service pages that can be accessed through temporary trusted login, the temporary trusted login token comprising a first mapping relationship between one or more service identifications corresponding to one or more allowed service pages and the temporary trusted login token, and further comprising a second mapping relationship between a current trusted login identification issued by the first server and the temporary trusted login token, wherein the first mapping relationship and the second mapping relationship are separate mapping relationships; and

sending, from the second server, the temporary trusted login token to the target client terminal, wherein the target client terminal logs in to the first server and accesses the service page using the temporary trusted login token.

2. The method of claim 1, wherein the temporary trusted login token i) is generated by the first server based on the trusted login token acquisition request and ii) sent to the second server in response to the first server determining that the current trusted login identifier is legal.

3. The computer-implemented method of claim 2, wherein the temporary trusted login token is generated according to a specific generation rule to render the temporary trusted login token valid.

4. The method of claim 2, wherein the temporary trusted login token is sent to the second server in response to the first server determining, based on the trusted login token acquisition request, that the target client terminal is a trusted client terminal.

5. The method of claim 4, wherein determining, based on the trusted login token acquisition request, that the target client terminal is a trusted client terminal comprises:

determining whether the trusted login token acquisition request comprises the current trusted login identifier issued by the first server to the second server; and

determining that the target client terminal is a trusted client terminal if the trusted login token acquisition request comprises the current trusted login identifier.

6. The method of claim 4, wherein determining, based on the trusted login token acquisition request, that the target client terminal is a trusted client terminal comprises:

determining whether a first client terminal corresponding to the target client terminal exists in the first server; and

determining that the target client terminal is a trusted client terminal if the first client terminal exists.

7. The computer-implemented method of claim 1, wherein the temporary trusted login token expires after a validity period.

8. The method of claim 1, wherein the service page is a page that can be loaded to the target client terminal in an embedded manner.

9. An apparatus for performing trusted login in a trusted login system comprising i) a first application system including a first server and a first client terminal, and ii) a second application system including a second server, and iii) a target client terminal, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 8.