TRANSLATION

Japanese Patent No. 5802137
Japanese Patent Application No. 2011-549140
In the name of WWPass Corporation
Your Ref: U2003-00011

Allowed Claims

1. A token-based centralized authentication method for providing access to a service provider to user information associated with a user's relationship with the service provider, comprising the steps of:

an authentication and data storage management system (204) authenticating a user presenting a user token (224) at a user terminal (222), the user token having stored thereon a user ID;

the authentication and data storage management system or the user token deriving a resource identifier using at least two data input elements, the at least two data input elements including the user ID of the user and a service provider ID of the service provider, wherein the user information is stored in a storage network (216) and the resource identifier is associated with the user information;

the authentication and data storage management system retrieving the user information from the storage network using the resource identifier; and

the authentication and data storage management system providing the retrieved user information to the service provider,

wherein the user ID and service provider ID are separately received by the authentication and data storage management system in communication with the storage network, wherein the authentication and data storage management system performs the step of deriving the resource identifier using the user ID and service provider ID,

wherein the deriving step includes the step of deriving the resource identifier using a one way function, the method further comprising the steps of:

the authentication and data storage management system issuing a temporary transaction identifier to one of the user terminal and a service provider agent (220), the temporary transaction identifier being associated with an access or authentication request;

the authentication and data storage management system receiving the temporary transaction identifier from the other of the user terminal and the service provider agent; and

the authentication and data storage management system performing the resource identifier deriving step after receiving the temporary transaction identifier.

2. A token-based centralized authentication method for providing access to a service provider to user information associated with a user's relationship with the service provider, comprising the steps of:

an authentication and data storage management system (204) authenticating a user presenting a user token (224) at a user terminal (222), the user token having stored thereon a user ID;

the authentication and data storage management system or the user token deriving a resource identifier using at least two data input elements, the at least two data input elements including the user ID of the user and a service provider ID of the service provider, wherein the user information is stored in a storage network (216) and the resource identifier is associated with the user information;

the authentication and data storage management system retrieving the user information from the storage network (216) using the resource identifier; and

the authentication and data storage management system providing the retrieved user information to the service provider,

wherein the resource identifier deriving step is performed by the user token, the user token performing the resource identifier deriving step after receiving a temporary transaction identifier from a service provider agent, the method further comprising the steps of:

the authentication and data storage management system issuing the temporary transaction identifier to the service provider agent, the temporary transaction identifier being associated with an access or authentication request; and

thereafter, the authentication and data storage management system receiving the temporary transaction identifier from the user terminal, the authentication and data storage management system receiving the resource identifier from the user terminal; and

using the received resource identifier in performing the retrieving step.

3. The method of claim 1 or 2,

wherein the storage network is a dispersed storage network comprising a plurality of storage nodes (218), wherein the user information is stored in the storage network in accordance with an information dispersal algorithm (IDA);

wherein the user information retrieving step includes the step of reconstructing the user information from the plurality of storage nodes (218), and the providing step comprises providing the reconstructed user information to the service provider.

4. The method of any one of claims 1-3, wherein the storage network stores a plurality of separate sets of user information associated with the user, each set being associated with a respective user and service provider pair, wherein each set of user information is retrievable using a respective resource identifier derived using the user ID and a respective service provider ID.

5. The method of any one of claims 1-4, further comprising the step of, the authentication and data storage management system, after providing the retrieved user information to the service provider, receiving a set of user data for the user from the service provider for storage in the storage network in association with the resource identifier, wherein the storage network serves as the service provider's permanent storage of the received user data.

6. The method of any one of claim 1-5, wherein the step of deriving the resource identifier includes the steps of:

combining the user ID and service provider ID to provide a data element; and encrypting the data element with a public key of a public/private key encryption pair.

7. A token-based centralized authentication system for providing access to a service provider to user information associated with a user's relationship with the service provider, comprising:

an authentication and data storage management system (204) in network communication with a service provider agent (220) and a user terminal (222), including:

a user front end (208), the user front end configured to communicate with a user token (224) through the user terminal for authenticating a user, the user token having stored thereon a user ID;

a service provider front end (205), the service provider front end configured to communicate with the service provider agent for authenticating a service provider; and

a data storage management engine (210) in communication with the user front end, the service provider front end and a storage network (216) having stored therein the user information, the data storage management engine configured to receive a resource identifier and retrieve the user information from the storage network using the resource identifier and provide the retrieved user information for communication to the service provider agent,

wherein the resource identifier is derived using a function having at least two data input elements, the at least two data input elements including the user ID and a service provider ID of the service provider,

wherein the user front end is configured to issue a temporary transaction identifier to the user terminal, the temporary transaction identifier being associated with an access or authentication request, and the service provider front end is configured to receive the temporary transaction identifier from the service provide agent and authenticate the service provider after receipt of the temporary transaction identifier, or

wherein the service provider front end is configured to issue the temporary transaction identifier to the service provider agent, and the user front end is configured to receive the temporary transaction identifier from the user terminal and authenticate the user after receipt of the temporary transaction identifier.

8. The system of claim 7,

wherein the storage network is a dispersed storage network comprising a plurality of storage nodes (218), wherein the user information is stored in the storage network in accordance with an information dispersal algorithm (IDA),

wherein the data storage management engine includes a data collector (211) configured to retrieve and reconstruct the user information from the plurality of storage nodes, wherein the reconstructed user information is provided to the service provider.

9. The system of claim 7 or 8, wherein the data storage management engine is configured to derive the resource identifier using a one way function.

10. The system of claim 7 or 8, wherein the user token is configured to derive the resource identifier and the data storage management engine is configured to receive the resource identifier from the user terminal.

11. The system of claim 7 or 8, wherein the storage network stores a plurality of separate sets of user information associated with the user, each set being associated with a respective user and service provider pair, wherein each set of user information is retrievable using a respective resource identifier derived using the user ID and a respective service provider ID.

12. The system of claim 7 or 11, wherein the function combines the at least two data input elements into a data element and encrypts the data element with a public key of a public/private key encryption pair.