

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a directory server computer, an indication that a resource
3 provider is trusted by a user;
4 providing, by the directory server computer, a first level of authentication
5 to the user;
6 storing, by the directory server computer in a database, data representing
7 the indication that the resource provider is trusted, the data comprising a trusted
8 marker, wherein the first level of authentication is provided prior to the storing of the
9 data;
10 receiving, by the directory server computer, an authentication request
11 message from the user conducting an interaction at a resource provider computer
12 operated by the resource provider;
13 determining, by the directory server computer, that the data comprising
14 the trusted marker is present in the database;
15 in response to the determining that the data comprising the trusted marker
16 is present, providing, by the directory server computer, a second level of authentication
17 to the user before the user is allowed to complete the interaction, wherein the second
18 level of authentication is lower than the first level of authentication;
19 sending, by the directory server computer to the resource provider,
20 information indicating that the user has been authenticated at the second level of
21 authentication and the trusted marker;
22 receiving, by a processing computer, an authorization request message
23 for the interaction from the resource provider, the authorization request message
24 comprising the trusted marker having been received by the resource provider from the
25 directory server computer;
26 validating, by the processing computer, the trusted marker; and
27 sending, by the processing computer, the authorization request message
28 comprising information related to the interaction and the validated trusted marker to an
29 authorizing entity computer.

- 1 2. The method of claim 1, wherein the resource provider stores an
2 account identifier for an account of the user.
- 1 3. The method of claim 2, wherein the interaction is a stored
2 credential transaction.
- 1 4. The method of claim 1, wherein the second level of authentication
2 is no authentication.
- 1 5. The method of claim 1, wherein the providing the first level of
2 authentication includes initiating an authentication process, during which the user is
3 requested to input a password.
- 1 6. The method of claim 1, wherein the authentication request
2 message includes a resource provider identifier of the resource provider and a
3 verification value of the user.
- 1 7. The method of claim 1, wherein the indication that the resource
2 provider is trusted is received from the resource provider computer.
- 1 8. The method of claim 1, wherein the indication that the resource
2 provider is trusted is received from the authorizing entity computer.
- 1 9. A directory server computer comprising:
2 a processor; and
3 a computer-readable medium, coupled to the processor, the computer-
4 readable medium comprising code which, when executed by the processor, causes the
5 processor to perform a method including:
6 receiving an indication that a resource provider is trusted by a user;
7 providing a first level of authentication to the user;
8 storing, in a database, data representing the indication that the
9 resource provider is trusted, the data comprising a trusted marker, wherein the
10 first level of authentication is provided prior to the storing of the data;

11 receiving an authentication request message from the user
12 conducting an interaction at a resource provider computer operated by the
13 resource provider;
14 determining that the data comprising the trusted marker is present
15 in the database;
16 in response to the determining that the data comprising the trusted
17 marker is present, providing a second level of authentication to the user before
18 the user is allowed to complete the interaction, wherein the second level of
19 authentication is lower than the first level of authentication; and
20 sending, to the resource provider, information indicating that the
21 user has been authenticated at the second level of authentication and the trusted
22 marker,
23 wherein the resource provider sends, to a processing computer, an authorization
24 request message for the interaction, the authorization request message comprising the
25 trusted marker having been received by the resource provider from the directory server
26 computer, and
27 wherein the processing computer validates the trusted marker, and sends the
28 authorization request message comprising information related to the interaction and the
29 validated trusted marker to an authorizing entity computer.

1 10. The directory server computer of claim 9, wherein the resource
2 provider stores an account identifier for an account of the user.

1 11. The directory server computer of claim 10, wherein the interaction
2 is a stored credential transaction.

1 12. The directory server computer of claim 9, wherein the second level
2 of authentication is no authentication.

1 13. The directory server computer of claim 9, wherein the providing the
2 first level of authentication includes initiating an authentication process during which the
3 user is requested to input a password.

1 14. The directory server computer of claim 9, wherein the
2 authentication request message includes a resource provider identifier of the resource
3 provider and a verification value of the user.

1 15. The directory server computer of claim 9, wherein the indication
2 that the resource provider is trusted is received from the resource provider computer.

1 16. The directory server computer of claim 9, wherein the indication
2 that the resource provider is trusted is received from the authorizing entity computer.

1 17. A system comprising:
2 a directory server computer comprising a first processor and a first
3 computer-readable medium comprising code which, when executed by the first
4 processor, causes the first processor to perform operations including:
5 receiving an indication that a resource provider is trusted by a user;
6 providing a first level of authentication to the user;
7 storing data representing the indication that the resource provider is
8 trusted in a database, the data comprising a trusted marker, wherein the first
9 level of authentication is provided prior to the storing of the data;
10 receiving an authentication request message from the user
11 conducting an interaction at a resource provider computer operated by the
12 resource provider;
13 determining that the data comprising the trusted marker is present
14 in the database;
15 in response to the determining that the data comprising the trusted
16 marker is present, providing a second level of authentication to the user before
17 the user is allowed to complete the interaction, wherein the second level of
18 authentication is lower than the first level of authentication; and
19 sending, to the resource provider computer, information indicating
20 that the user has been authenticated at the second level of authentication and
21 the trusted marker; and

22 a processing computer comprising a second processor and a second
23 computer-readable medium comprising code which, when executed by the second
24 processor, causes the second processor to perform operations including:
25 receiving an authorization request message for the interaction from
26 the resource provider, the authorization request message comprising the trusted
27 marker having been received by the resource provider from the directory server
28 computer;
29 validating the trusted marker; and
30 sending the authorization request message comprising information
31 related to the interaction and the trusted marker to an authorizing entity
32 computer.