

WHAT IS CLAIMED IS:

1 1. A method for password management, the method comprising:
2 sending, by a user device, a request message to a password
3 management server, the request message including a public key of the user device,
4 the public key and a private key forming a public-private key pair;
5 receiving, by the user device, a response message from the password
6 management server, the response message including an encrypted password;
7 decrypting, by the user device, the encrypted password using the
8 private key to obtain a decrypted password; and
9 obtaining, by the user device, access to account information using the
10 decrypted password, and wherein the method further comprises:
11 receiving, by the user device, one or more account names associated
12 with the public key from the password management server, the one or more account
13 names including a first account name; and
14 sending, by the user device, a password retrieval request to the
15 password management server, the password retrieval request including the first
16 account name.

1 2. The method of claim 1, further comprising:
2 displaying, by the user device, the one or more account names on a
3 user interface of the user device; and
4 determining, by the user device, the first account name based on input
5 to the user interface.

1 3. A method for password management, the method comprising:
2 sending, by a user device, a request message to a password
3 management server, the request message including a public key of the user device,
4 the public key and a private key forming a public-private key pair;
5 receiving, by the user device, a response message from the password
6 management server, the response message including an encrypted password;
7 decrypting, by the user device, the encrypted password using the
8 private key to obtain a decrypted password; and

obtaining, by the user device, access to account information using the decrypted password, wherein the method further comprises:

prompting, via a user interface the user device, a user to provide authentication information;

obtaining, by the user device, the authentication information from the user;

comparing, by the user device, the authentication information to registered authentication information; and

validating, by the user device, the authentication information based on the comparing of the authentication information to the registered authentication information.

4. The method of claim 1, further comprising:

obtaining, by the user device, authentication information of a user of the user device;

generating, by the user device, the public-private key pair; and

associating, by the user device, the public-private key pair with the authentication information.

5. The method of claim 1, further comprising:

sending, by the user device, a registration request message to the password management server, the registration request message including the public key; and

receiving, by the user device, a registration response from the password management server, the registration response including an indication that the public key is registered to the user device.

6. The method of claim 5, further comprising:

determining, by the user device, a password management account name based on an input from a user interface of the user device; and

creating, by the user device, the registration request message based on the input from the user interface, wherein the registration request message further includes the password management account name.

1 7. The method of claim 1, further comprising:
2 obtaining, by the user device, a first password associated with a first
3 account name;
4 sending, by the user device, a password storage request to the
5 password management server, the password storage request including the public
6 key, the first password, and the first account name; and
7 receiving, by the user device, a password storage response message
8 from the password management server, the password storage response message
9 including an indication that the first password is stored in association with the first
10 account name and the public key.

1 8. The method of claim 7, further comprising:
2 obtaining, by the user device, a second password associated with a
3 second account name;
4 sending, by the user device, a second password storage request to the
5 password management server, the second password storage request including the
6 public key, the second password, and the second account name; and
7 receiving, by the user device, two or more account names associated
8 with the public key from the password management server, the two or more account
9 names including the first account name and the second account name.

1 9. The method of claim 7, further comprising:
2 establishing, by the user device, a secure communication channel with
3 the password management server, wherein the sending of the password storage
4 request to the password management server uses the secure communication
5 channel.

1 10. The method of claim 1, further comprising:
2 sending, by the user device, an account information request message
3 to an authentication server, the account information request message including the
4 decrypted password and an account name, wherein the obtaining of the access to
5 the account information using the decrypted password includes receiving the
6 account information from the authentication server.

1 11. A method for password management, the method comprising:

receiving, by a password management server, a request message from a user device, the request message including a public key;
determining, by the password management server, a stored password associated with the public key;
encrypting, by the password management server, the stored password using the public key to obtain an encrypted password; and
sending, by the password management server, a response message to the user device, the response message including the encrypted password, and wherein the method further comprises:
determining, by the password management server, one or more account names associated with the public key, the one or more account names including a first account name;
sending, by the password management server, the one or more account names to the user device;
receiving, by the password management server, a password retrieval request from the user device, the password retrieval request including the first account name;
determining, by the password management server, that the first account name is associated with the public key; and
determining, by the password management server, the stored password using the first account name.

12. The method of claim 11, further comprising:
receiving, by the password management server, a registration request message from the user device, the registration request message including the public key;
determining, by the password management server, whether the public key included in the registration request message does or does not match at least one of a plurality of registered public keys;
determining, by the password management server, whether to register the public key based on the determining of whether the public key included in the registration request message does or does not match the at least one of the plurality of registered public keys; and

12 sending, by the password management server, a registration response
13 message to the user device, the registration response message including an
14 indication of whether or not the public key is registered.

1 13. The method of claim 12, wherein the registration request
2 message further includes a password management account name, the method
3 further comprising:

4 storing, by the password management server, the public key; and
5 associating, by the password management server, the password
6 management account name with the public key.

1 14. The method of claim 11, wherein the stored password is a first
2 password, the method further comprising:

3 receiving, by the password management server, a password storage
4 request from the user device, the password storage request including the public key,
5 the first password, and a first account name;

6 storing, by the password management server, the first password in
7 association with the first account name and the public key; and

8 sending, by the password management server, a password storage
9 response message to the user device, the password storage response message
10 including an indication that the first password is stored in association with the first
11 account name and the public key.

1 15. The method of claim 11, wherein the user device is a first user
2 device, wherein the public key is a first public key, the method further comprising:

3 associating, by the password management server, a password
4 management account name with the first public key;

5 receiving, by the password management server, a second registration
6 request message from a second user device, the second registration request
7 message including the password management account name and a second public
8 key;

9 determining, by the password management server, that the password
10 management account name included in the second registration request message is
11 associated with the first public key of the first user device;

12 sending, by the password management server, a verification request
13 message to the first user device in response to the determination that the password
14 management account name included in the second registration request message is
15 associated with the first public key of the first user device, the verification request
16 message including an identifier or indicator of the second user device;
17 receiving, by the password management server, a verification response
18 message from the first user device, the verification response message including an
19 indication that the second user device is authorized to access passwords associated
20 with the password management account name;
21 associating, by the password management server, the second public
22 key with the password management account name and each stored password
23 associated with the first public key; and
24 sending, by the password management server, a second registration
25 response message to the second user device, the second registration response
26 message including a second indication that the second public key is registered.

1 16. A user device, comprising:
2 one or more processor circuits;
3 a communication interface; and
4 a computer readable storage medium storing a plurality of instructions
5 that, when executed by the one or more processor circuits, cause the one or more
6 processor circuits to:
7 send, using the communication interface, a request message to
8 a password management server, the request message including a public key
9 of the user device, the public key and a private key forming a public-private
10 key pair;
11 receive, using the communication interface, a response
12 message from the password management server, the response message
13 including an encrypted password;
14 decrypt the encrypted password using the private key to obtain a
15 decrypted password; and
16 obtain access to account information using the decrypted
17 password, and

18 further comprising a user interface, wherein the plurality of instructions
19 further cause the one or more processor circuits to:
20 receive, using the communication interface, one or more account
21 names associated with the public key from the password management server, the
22 one or more account names including a first account name;
23 send, using the communication interface, a password retrieval request
24 to the password management server, the password retrieval request including the
25 first account name;
26 display, using the user interface, the one or more account names on
27 the user interface; and
28 determine the first account name based on input to the user interface.

1 17. The user device of claim 16, wherein the plurality of instructions
2 further cause the one or more processor circuits to:
3 obtain authentication information of a user of the user device;
4 generate the public-private key pair;
5 associate the public-private key pair with the authentication
6 information;
7 determine a password management account name based on input
8 from the user interface;
9 send, using the communication interface, a registration request
10 message to the password management server, the registration request message
11 including the public key and the password management account name; and
12 receive, using the communication interface, a registration response
13 from the password management server, the registration response including an
14 indication that the public key is registered.

1 18. A password management server comprising:
2 one or more processor circuits;
3 a communication interface; and
4 a computer readable storage medium storing a plurality of instructions
5 that, when executed by the one or more processor circuits, cause the one or more
6 processor circuits to:

7 receive a request message from a user device, the request
8 message including a public key;
9 determine a stored password associated with the public key;
10 encrypt the stored password using the public key to obtain an
11 encrypted password; and
12 send a response message to the user device, the response
13 message including the encrypted password,
14 wherein the plurality of instructions further cause the one or more
15 processor circuits to:
16 determine one or more account names associated with the public key,
17 the one or more account names including a first account name;
18 send the one or more account names to the user device;
19 receive a password retrieval request from the user device, the
20 password retrieval request including the first account name;
21 determine that the first account name is associated with the public key;
22 and
23 determine the stored password using the first account name.

1 19. The password management server of claim 18, wherein the
2 stored password is a first password, and wherein the plurality of instructions further
3 cause the one or more processor circuits to:
4 receive a registration request message from the user device, the
5 registration request message including the public key and a password management
6 account name;
7 determine whether the public key included in the registration request
8 message does or does not match at least one of a plurality of registered public keys;
9 determine whether to register the public key based on the determining
10 of whether the public key included in the registration request message does or does
11 not match the at least one of the plurality of registered public keys;
12 store the public key;
13 associate the password management account name with the public
14 key; and

15 send a registration response message to the user device, the
16 registration response message including an indication of whether or not the public
17 key is registered.

1 20. The password management server of claim 18, wherein the user
2 device is a first user device, wherein the public key is a first public key, and wherein
3 the plurality of instructions further cause the one or more processor circuits to:
4 receive a password storage request from the user device, the
5 password storage request including the public key, a first password, and a first
6 account name;
7 store the first password in association with the first account name and
8 the public key; and
9 send a password storage response message to the user device, the
10 password storage response message including an indication that the first password
11 is stored in association with the first account name and the public key.

1 21. The password management server of claim 18, wherein the
2 public key is a first public key, wherein the user device is a first user device, and
3 wherein the plurality of instructions further cause the one or more processor circuits
4 to:
5 associate a password management account name with the first public
6 key;
7 receive a second registration request message from a second user
8 device, the second registration request message including the password
9 management account name and a second public key;
10 determine that the password management account name included in
11 the second registration request message is associated with the first public key of the
12 first user device;
13 send a verification request message to the first user device in response
14 to the determination that the password management account name included in the
15 second registration request message is associated with the first public key of the first
16 user device, the verification request message including an identifier or indicator of
17 the second user device;

18 receive a verification response message from the first user device, the
19 verification response message including an indication that the second user device is
20 authorized to access passwords associated with the password management account
21 name;
22 associate the second public key with the password management
23 account name and each stored password associated with the first public key; and
24 send a second registration response message to the second user
25 device, the second registration response message including a second indication that
26 the second public key is registered.

1