

Claims

What is claimed is:

1. A method for secure medical device interoperability comprising:

executing, with a processor in an electronic device controlled by a user, a control application configured to communicate with a medical device operated by the user;

receiving, with the electronic device, user authentication data generated in response to a user authentication process;

establishing an untrusted connection between the electronic device and the medical device;

receiving, with the electronic device, a key identifier from the medical device through the untrusted connection;

transmitting, with the electronic device, a message containing data corresponding to an identifier of the user, the user authentication data, the key identifier, an identifier of the control application, and a cryptographic signature of the message to an authorization service, the cryptographic signature being generated using a secret key stored in a memory of the electronic device;

receiving, with the electronic device, a medical device cryptographic key from the authorization service only in response to successful verification of the message that authorizes the user and the control application; and

establishing a trusted connection between the electronic device and the medical device using the medical device cryptographic key to enable at least one of control communication and data communication between the control application and the medical device.

2. The method of claim 1, the user authentication process further comprising:

receiving, with the electronic device, authentication input data from the user, the authentication input data not being provided to the control application;

transmitting, with the electronic device, an authentication request corresponding to the authentication input data to an authentication service; and

receiving, with the control application, the user authentication data as a user authentication token from the authentication service, the user authentication token

being received in response to a successful authentication of the user based on the authentication request.

3. The method of claim 2, wherein the user authentication token contains the identifier of the user and the user authentication data.

4. The method of any of claims 1 - 3, the generating of the cryptographic signature further comprising:

generating the cryptographic signature as a hashed message authentication code (HMAC) corresponding to the identifier of the user, the user authentication data, the key identifier, and the identifier of the control application, using the secret key and a cryptographically secure hash function.

5. The method of any of the claims 1 - 4, wherein the medical device cryptographic key is a public key corresponding to a private key stored in a memory of the medical device.

6. The method of claim 5, the establishing of the trusted connection between the electronic device and the medical device further comprising:

generating, with the control application, a control application public key and corresponding control application private key;

transmitting, the control application public key to the medical device; and
performing a key exchange protocol to establish the trusted connection between the control application and the medical device based on the control application public key, the control application private key, the public key and the private key of the medical device.

7. The method of any of the claims 1 - 4, wherein the medical device cryptographic key is a shared-secret cryptographic key that is identical to a shared-secret key cryptographic stored in a memory of the medical device.

8. The method of any of the claims 1 – 7, wherein the electronic device is a smartphone.

9. The method of any of the claims 1 – 7 wherein the medical device is an insulin pump.
10. The method of any of the claims 1 – 7 wherein the medical device is a continuous glucose meter.
11. The method of any of the claims 1 – 7 wherein the medical device is a spot blood glucose meter.
12. The method of any of the claims 1 – 7 wherein the medical device is an electronic medication delivery device.
13. A system for secure medical device interoperability comprising a medical device, an electronic device, an authorization service, and an authentication service configured to perform the methods of any of claims 1 – 12.
14. A method for secure medical device interoperability comprising:
- executing, with a processor in an electronic device controlled by a user, a control application configured to communicate with a medical device operated by the user;
 - establishing an untrusted connection between the electronic device and the medical device;
 - receiving, with the electronic device, a key identifier from the medical device through the untrusted connection;
 - transmitting, with the electronic device, a message containing data corresponding to the key identifier, an identifier of the control application, and a cryptographic signature of the message to an authorization service, the cryptographic signature being generated using a secret key stored in a memory of the electronic device;
 - receiving, with the electronic device, a medical device cryptographic key from the authorization service only in response to successful verification of the message that authorizes the control application; and
 - establishing a trusted connection between the electronic device and the medical device using the medical device cryptographic key to enable at least one of

control communication and data communication between the control application and the medical device.

15. A system for secure medical device interoperability comprising a medical device, an electronic device, and an authorization service, configured to perform the method of claim 14.

16. A method for secure medical device interoperability comprising:

receiving, with an authorization service, a message from an electronic device that seeks authorization to control a medical device, the message containing data corresponding to an identifier of a user, user authentication data, a key identifier corresponding to a device cryptographic key stored in a memory of a medical device, an identifier of a control application executed by the electronic device, and a cryptographic signature of the message;

verifying, with the authorization service, authorization of the control application based on the identifier of the control application and verification of the cryptographic signature for the message using a first cryptographic key stored in the memory of the authorization service, the first cryptographic key being associated with the identifier of the control application;

verifying, with the authorization service, authorization of the user based on the data corresponding to the identifier of the user and the user authentication data using a second cryptographic key stored in a memory of the authorization service, the second cryptographic key being associated with an authentication service; and

transmitting, with the authorization service, a device cryptographic key that corresponds to the key identifier to the electronic device to enable the electronic device to establish a trusted connection with the medical device only in response to a successful verification of authorization for the control application and a successful verification of authorization for the user.

17. The method of claim 16, the verifying of the cryptographic signature further comprising:

generating, with the authorization service, a hashed message authentication code (HMAC) corresponding to the identifier of the user, the user authentication

data, the key identifier, and the identifier of the control application using the first cryptographic key and a cryptographically secure hash function; and

verifying, with the authorization service, that the HMAC matches the cryptographic signature in the message.

18. The method of any of claims 16 – 17, the verifying authorization of the user further comprising:

receiving, with the authorization service, an authentication token generated by an authentication service in the message as the user authentication data; and

verifying, with the second cryptographic key, the authentication token to verify that the control application executed by the electronic device is operated by an authorized user corresponding to the identifier of the user.

19. The method of any of claims 16 – 18 wherein the user authentication token contains the identifier of the user and the user authentication data.

20. The method of any of claims 16 – 19 wherein the medical device is an insulin pump.

21. The method of any of claims 16 – 19 wherein the medical device is a continuous glucose meter.

22. The method any of claims 16 – 19 wherein the medical device is a blood glucose meter.

23. The method any of claims 16 – 19 wherein the medical device is an electronic medication delivery device.

24. The method of any of claims 16 – 22 wherein the device cryptographic key is a public key corresponding to a private key stored in a memory of the medical device.

25. An authorization service configured to perform the methods of any of claims 16 – 24.

26. A method for secure medical device interoperability comprising:

receiving, with an authorization service, a message from an electronic device that seeks authorization to control a medical device, the message containing data corresponding to a key identifier corresponding to a device cryptographic key stored in a memory of a medical device, an identifier of a control application executed by the electronic device, and a cryptographic signature of the message;

verifying, with the authorization service, authorization of the control application based on the identifier of the control application and verification of the cryptographic signature for the message using a first cryptographic key stored in the memory of the authorization service, the first cryptographic key being associated with the identifier of the control application; and

transmitting, with the authorization service, a device cryptographic key that corresponds to the key identifier to the electronic device to enable the electronic device to establish a trusted connection with the medical device only in response to a successful verification of authorization for the control application.

27. An authorization service configured to perform the method claim 26.

28. A method for secure medical device interoperability comprising:

establishing, with a medical device, an untrusted connection with an electronic device;

transmitting, with the medical device, a key identifier corresponding to a public key and private key associated with the medical device to the electronic device, the key identifier and the private key being stored in a memory of the medical device;

establishing, with the medical device, a trusted connection with the electronic device using the private key held in a memory of the medical device only in response to a control application that is executed by the electronic device receiving the public key based on the key identifier; and

performing an operation based on a command received from the control application in the electronic device only in response to the command being received via the trusted connection.

29. The method of claim 28, wherein the medical device establishes the trusted connection using an elliptic curve Diffie-Hellman key exchange protocol.

30. The method of any of claims 28 - 29, wherein the medical device receives a public key corresponding to the control application during the establishing of the trusted connection.
31. The method of any of claims 28 – 30 wherein the medical device performs the operation to deliver a dose of a medication to a user in response to the command.
32. The method of any of claims 28 - 30 wherein the medical device performs the operation to transmit a measurement of a blood glucose level in a user to the electronic device in response to the command.
33. A medical device configured to perform any of the methods of claims 28 –32.
34. A method for secure medical device interoperability comprising:
- establishing, with a medical device, an untrusted connection with an electronic device;
 - transmitting, with the medical device, a key identifier corresponding to a shared-secret cryptographic key associated with the medical device to the electronic device, the key identifier and the shared-secret cryptographic key being stored in a memory of the medical device;
 - establishing, with the medical device, a trusted connection with the electronic device using the shared-secret cryptographic key held in a memory of the medical device only in response to a control application that is executed by the electronic device receiving the shared-secret cryptographic key from an authorization service based on the key identifier; and
 - performing an operation based on a command received from the control application in the electronic device only in response to the command being received via the trusted connection.
35. A medical device configured to perform the method of claim 34.