SUMMARY

[007] According to an aspect of the present disclosure, there is provided a method for secure medical device interoperability includes 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, the untrusted connection enables communication between the control application of the electronic device and the medical device, the medical device does not accept operational command messages from the control application and only provides access to publicly available data to the electronic device, 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.

[007a] According to a second aspect of the present disclosure, there is provided 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 defined in the first aspect.

[007b] According to a third aspect of the present disclosure, there is provided 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.

[007c] According to a fourth aspect of the present disclosure, there is provided a system for secure medical device interoperability comprising a medical device, an electronic device, and an authorization service, configured to perform the method defined in the third aspect.

[008] According to a fifth aspect of the present disclosure, there is provided a method for secure medical device interoperability includes 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 medical 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.

[008a] According to a sixth aspect of the present disclosure, there is provided an authorization service configured to perform the methods defined in the fifth aspect.

[008b] According to a seventh aspect of the present disclosure, there is provided 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.

[008c] According to an eighth aspect of the present disclosure, there is provided an authorization service configured to perform the method defined in the seventh aspect.

[009] According to a ninth aspect of the present disclosure, there is provided a method for secure medical device interoperability includes 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.

[009a] According to a tenth aspect of the present disclosure, there is provided a medical device configured to perform any of the methods defined in the ninth aspect.

[009b] According to an eleventh aspect of the present disclosure, there is provided 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.

[009c] According to a twelfth aspect of the present disclosure, there is provided a medical device configured to perform the method defined in the eleventh aspect.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The advantages, effects, features and objects other than those set forth above will become more readily apparent when consideration is given to the detailed description below. Such detailed description makes reference to the following drawings, wherein:

[0011] FIG. 1 is a schematic diagram of a system that enables secure interoperability between an electronic device controlled by a user and a medical device.

[0012] FIG. 2 is a schematic diagram depicting stored program instructions and other data used and generated by a control application in the electronic device of FIG. 1.

[0013] FIG. 3 is a diagram that depicts an illustrative embodiment of a message that the electronic device transmits to an authorization service in the system of FIG. 1.

[0014] FIG. 4 is a block diagram of a process for user and control application authentication and authorization to establish a trusted connection between the electronic device and the medical device in the system of FIG. 1.

[0015] FIG. 5 is a block diagram depicting a process for operation of an authorization service during the process depicted in FIG. 4.

DETAILED DESCRIPTION

[0016] These and other advantages, effects, features and objects are better understood from the following description. In the description, reference is made to the accompanying drawings, which form a part hereof and in which there is shown by way of illustration, not

Claims

What is claimed is:

1. A method for secure medical device interoperability comprising:

executing, with a processor (106) in an electronic device (104) controlled by a user (102), a control application (114) configured to communicate with a medical device (124) operated by the user (102);

receiving, with the electronic device (104), user authentication data generated in response to a user authentication process;

establishing an untrusted connection between the electronic device (104) and the medical device (124);

receiving, with the electronic device (104), a key identifier (138) from the medical device (124) through the untrusted connection, wherein the untrusted connection enables communication between the control application of the electronic device (104) and the medical device (124), wherein the medical device (124) does not accept operational command messages from the control application (114) and only provides access to publicly available data to the electronic device (104);

transmitting, with the electronic device (104), a message containing data corresponding to an identifier of the user (102), the user authentication data, the key identifier (138), an identifier of the control application (114), and a cryptographic signature of the message to an authorization service (154), the cryptographic signature being generated using a secret key stored in a memory (112) of the electronic device (104);

receiving, with the electronic device (104), a medical device cryptographic key from the authorization service (154) only in response to successful verification of the message that authorizes the user (102) and the control application (114); and

establishing a trusted connection between the electronic device (104) and the medical device (124) using the medical device cryptographic key to enable at least one of control communication and data communication between the control application (114) and the medical device (124).

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

receiving, with the electronic device (104), authentication input data from the user (102), the authentication input data not being provided to the control application (114);

transmitting, with the electronic device (104), an authentication request corresponding to the authentication input data to an authentication service (174); and

receiving, with the control application (114), the user authentication data as a user authentication token from the authentication service (174), the user authentication token being received in response to a successful authentication of the user (102) based on the authentication request.

3. The method of claim 2, wherein the user authentication token contains the identifier of the user (102) 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 (102), the user authentication data, the key identifier (138), and the identifier of the control application (114), 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 (124).

6. The method of claim 5, the establishing of the trusted connection between the electronic device (104) and the medical device (124) further comprising:

generating, with the control application (114), a control application public key and corresponding control application private key;

transmitting, the control application public key to the medical device (124); and

performing a key exchange protocol to establish the trusted connection between the control application (114) and the medical device (124) based on the control application public key, the control application private key, the public key and the private key of the medical device (124).

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 (124).
8. The method of any of the claims 1 – 7, wherein the electronic device (104) is a smartphone.

9. The method of any of the claims 1 – 7 wherein the medical device (124) is an insulin pump.

10. The method of any of the claims 1 – 7 wherein the medical device (124) is a continuous glucose meter.

11. The method of any of the claims 1 – 7 wherein the medical device (124) is a spot blood glucose meter.

12. The method of any of the claims 1 – 7 wherein the medical device (124) is an electronic medication delivery device.

13. A system for secure medical device interoperability comprising a medical device(124), an electronic device (104), an authorization service (154), and an authentication service (174) configured to perform the methods of any of claims 1 – 12.