(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 791 782 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
03.10.2018 Bulletin 2018/40

(21) Application number: **12857131.2**

(22) Date of filing: **14.12.2012**

(51) Int Cl.:
G06F 7/04 *(2006.01)* ***A61B 5/00*** *(2006.01)*
A61B 5/145 *(2006.01)* ***G06F 19/00*** *(2018.01)*
H04W 4/00 *(2018.01)* ***H04W 12/04*** *(2009.01)*
H04W 12/06 *(2009.01)*

(86) International application number:
PCT/US2012/069860

(87) International publication number:
WO 2013/090791 (20.06.2013 Gazette 2013/25)

(54) **NEAR FIELD TELEMETRY LINK FOR PASSING A SHARED SECRET TO ESTABLISH A SECURE RADIO FREQUENCY COMMUNICATION LINK IN A PHYSIOLOGICAL CONDITION MONITORING SYSTEM**

NAHFELDTELEMETRIEVERBINDUNG ZUR WEITERGABE EINES GEMEINSAMEN GEHEIMNISSES ZUM AUFBAU EINER SICHEREN FUNKFREQUENZKOMMUNIKATIONSVERBINDUNG IN EINEM ÜBERWACHUNGSSYSTEM FÜR PHYSIOLOGISCHE ZUSTÄNDE

LIAISON DE TÉLÉMÉTRIE EN CHAMP PROCHE POUR FAIRE PASSER UN SECRET PARTAGÉ POUR ÉTABLIR UNE LIAISON DE COMMUNICATION RADIOFRÉQUENCE (RF) SÛRE DANS UN SYSTÈME DE SURVEILLANCE DE CONDITION PHYSIOLOGIQUE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **15.12.2011 US 201161576309 P**

(43) Date of publication of application:
22.10.2014 Bulletin 2014/43

(73) Proprietor: **Becton, Dickinson and Company**
Franklin Lakes, NJ 07417-1880 (US)

(72) Inventors:
- **YARGER, Michael**
  Chapel Hill
  North Carolina 27516 (US)
- **PETISCE, James**
  Westford
  Massachusetts 01886 (US)
- **DIRESTA, Ellen**
  Arlington
  Massachusetts 02476 (US)
- **BURNS, Deborah**
  Westford
  Massachusetts 01866 (US)
- **MASON, David**
  Newburyport
  Massachusetts 01950 (US)

(74) Representative: **dompatent von Kreisler Selting Werner -**
Partnerschaft von Patent- und Rechtsanwälten mbB
Deichmannhaus am Dom
Bahnhofsvorplatz 1
50667 Köln (DE)

(56) References cited:
WO-A2-2009/004578
WO-A2-2009/153710
US-A- 5 991 648
US-A1- 2004 266 449
US-A1- 2007 008 140
US-A1- 2008 044 014
US-A1- 2009 054 737
US-A1- 2009 140 923
US-A1- 2010 045 425
US-A1- 2010 045 425
US-A1- 2011 145 894

EP 2 791 782 B1

Description

FIELD OF THE INVENTION

[0001] The present invention disclosed and claimed herein generally relates to a physiological condition monitor (e.g., a continuous glucose monitor) and, more particularly, to methods and apparatuses to establish a near field telemetry link for passing a shared secret to establish a secure radio frequency communication link in a physiological condition monitoring system.

BACKGROUND OF THE INVENTION

[0002] Diabetes is a disease in which a person has high blood sugar either because the body does not produce enough insulin or because the person's cells are insensitive to the produced insulin. Accordingly, it is beneficial to monitor the person's glucose levels to identify trends in glucose levels, identify factors that affect glucose levels, evaluate foods and medications on glucose levels, and identify changes in a treatment plan.

[0003] A continuous glucose monitor (CGM) is an electronic system that measures and displays glucose level in a user's body. A CGM includes a sensor that is attached to a user's skin and held securely in place by a fastener. To measure glucose levels of the user, the sensor generally includes a metal filament that penetrates and rests in the fatty layer of the user's skin. The sensor communicates with a handheld meter that displays the glucose measurements from the sensor. A CGM is helpful to avoid potentially dangerous hyperglycemia or hypoglycemia and to help the user lower their average blood sugar levels over time.

[0004] Because the sensor is attached to the user's skin and the meter is a handheld device, wires would make the CGM difficult to use. Accordingly, CGM systems are preferably implemented with a wireless communication link between the sensor and the monitor. Accordingly, a separate transmitter may be incorporated into the sensor to transmit data to the handheld meter. Unique information must be exchanged between the transmitter and meter to create a secure communication link. Generally, for the user's convenience, the transmitter is implemented in a small form factor and includes a fixed battery that cannot be easily replaced. As such, the transmitter must be replaced when the battery is exhausted. Current CGM systems require the user to input information into the meter that identifies the transmitter, thereby allowing the meter to receive information from the sensor. This information is typically printed on the transmitter and, therefore, available for any person to read the information.

[0005] As such, the unique information can be easily obtained by observing unique information disposed on the transmitter or intercepting the communications with the unique information. Due to the importance of wireless medical devices, regulators have become interested in the security of such wireless medical devices. Further, because the user has to manually enter the unique information, replacing the transmitter is inconvenient. Moreover, battery life is an important factor in CGM sensors, and similar devices, where the battery is not designed to be replaced. Accordingly, there is a need for a method to exchange information for encrypting data in wireless medical devices that is convenient for users, and minimize battery usage.

[0006] WO 2009/153710 A2 discloses a personal security manager for ubiquitous patient monitoring.

[0007] US 2010/0045425 A1 discloses a method for data transmission between a sensor module for measuring and storing data and a mobile device wherein the sensor module and the mobile device have identified each other.

[0008] US 2004/0266449 A1 discloses a public key infrastructure for provisioning secure wireless sensors.

[0009] WO 2009/004578 A2 discloses a multidimensional identification, authentication, authorization and key distribution system for patient monitoring.

SUMMARY OF THE INVENTION

[0010] A system and method for pairing a physiological condition meter and a physiological condition sensor in a wireless physiological condition monitoring system by exchanging a secret key is provided. The method comprises placing a physiological condition meter in proximity with a physiological condition sensor, receiving an instruction to initialize communication between the physiological condition meter and the physiological condition sensor; in response to the instruction, transmitting a secret key via a first wireless link; and transmitting measurement data to the physiological condition meter from a physiological condition sensor via a secure wireless link based on the secret key. In another illustrative method, the secret key is generated using a random process. In a further illustrative method, the data is encrypted using the secret key.

[0011] An illustrative wireless physiological condition monitoring system is disclosed. The wireless physiological condition monitoring system includes a physiological condition sensor for measuring physiological condition of a user and transmitting the measured physiological condition data using a secure link based on a secret key and a physiological condition meter for receiving the measured physiological condition data via the secure link based on the secret key and displaying the physiological condition data to the user. In the wireless physiological condition monitoring system, in response to an instruction, the secret key is generated and transmitted using a secure wireless link when the physiological condition sensor and the physiological condition meter are in proximity to each other.

[0012] Also disclosed is another illustrative method for synchronizing a wireless physiological condition monitor. The method comprises receiving an instruction to initial-

ize communication between a physiological condition sensor and a physiological condition meter; in response to the instruction, transmitting a secret key via a wireless inductive link; receiving the secret key via the wireless inductive link; encrypting data to be transmitted between the physiological condition sensor and physiological condition meter; and transmitting the encrypted data between the physiological condition sensor and the physiological condition meter via a second wireless link. In other illustrative methods, the physiological condition meter and physiological condition sensor may be placed in electrical and/or optical contact, and the secret key may be transmitted via the electrical and/or optical contact.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013]

Fig. 1 depicts a CGM system in accordance with an illustrative embodiment of the present invention;
Fig. 2 depicts a block diagram of an example glucose meter for use in the CGM system of Fig. 1;
Fig. 3 depicts a block diagram of an example glucose sensor for use in the CGM system of Fig. 1;
Fig. 4 is a flow chart of an illustrative process that the CGM system of Fig. 1 may implement to pair the glucose meter and the glucose sensor; and
Figs. 5-8 illustrate examples of communication sequences between the glucose meter and the glucose sensor according to the example process of Fig. 4.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0014] A near field telemetry link for passing a shared secret to establish a secure radio frequency communication link in a physiological condition monitoring system (e.g., continuous glucose monitoring system) is generally described herein. As will be described in detail below, an example glucose meter and an example glucose sensor of the CGM system are placed in proximity to exchange a secret key using a near field wireless link, which is used to pair the devices and encrypt data to secure a radio frequency (RF) wireless channel between the sensor and the monitor. As will be appreciated by one skilled in the art, there are numerous ways of carrying out the examples, improvements and arrangements of the methods disclosed herein. Although reference is made to the illustrative embodiments depicted in the drawings and the following descriptions, the embodiments disclosed herein are not meant to be exhaustive of the various alternative designs and embodiments that are encompassed by the disclosed invention.

[0015] Reference is now made in detail to the illustrative embodiments of the invention, which, together with the drawings and the following examples serve to explain the principles of the invention.

[0016] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. Although any methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, the example methods, devices and materials are now described.

[0017] Fig. 1 depicts an illustrative embodiment of a CGM system 100. Generally, the CGM system 100 comprises a glucose meter 105 and a glucose sensor 110. In operation, the glucose meter 105 and the glucose sensor 110 communicate by a radio frequency (RF) wireless link. To establish the RF wireless link, the glucose meter 105 and the glucose sensor 110 must be linked together (paired) so that the glucose meter 105 only receives information from the paired glucose sensor 110 and not another nearby sensor or other unauthorized device. In the example of Fig. 1, the glucose sensor 110 and the glucose meter 105 securely exchange a secret key that is used to encrypt information transmitted on a different wireless link. That is, for example, the glucose sensor 110 uses the secret key to encrypt data that is transmitted to the glucose meter 105, which uses an identical secret key to decrypt the encrypted data. The glucose meter 105 may also preferably include an error check field in the decrypted data to verify successful reception and decryption of the received data.

[0018] The glucose sensor 110 typically includes a filament 115 that is inserted into the user's skin and rests in the fatty later beneath the user's skin. Other methods of sensor deployment (e.g., subcutaneous, intravenous, and so on) can be used as described below. In other examples, the glucose sensor 110 may be implemented by an optical sensor, a chemical sensor, or any device suitable for detecting a body characteristic or analyte such as glucose. As such, the user generally does not feel the filament 115 piercing the user's skin. To secure the position of the sensor, a suitable fastener such as an adhesive patch fixes the sensor in place. In the CGM system 100, the glucose meter 105 includes any suitable display 120 to provide graphical and/or textual information to the user, such as the user's current glucose level. However, the display 120 may provide the information in any suitable form, such as a line graph illustrating the glucose level over time. In such an example, the user is able to monitor their glucose level based on food and beverage consumption or other relevant events occurring throughout the day.

[0019] In the example of Fig. 1, the glucose meter 105 and the glucose sensor 110 preferably include a low power radio link by using inductive coupling of inductors in each device, which is also known as near field communication (NFC). When such inductors are placed in close proximity (e.g., 10cm), the magnetic field generated by a current in a transmitting inductor will induce a voltage in a receiving inductor, thereby enabling a very short range wireless communication link. In the example of Fig.

1, after an instruction from a user or another indication that the glucose meter 105 and the glucose sensor 110 are close in proximity, the glucose meter 105 and/or glucose sensor 110 exchange a shared key using the NFC wireless link. As will be described below, the shared key is randomly generated data for encrypting communications between the glucose meter 105 and the glucose 110 using a different low power wireless link.

[0020] Because the glucose meter 105 and the glucose sensor 110 must be close in proximity due to the NFC wireless channel, security of the shared key is transmitted in confidence that another sensor is not nearby and can intercept the shared key. Further, the user is not required to enter information to manually pair the glucose meter 105 and the glucose sensor 110, thereby facilitating the operation of the CGM system 100 due to replacing a glucose sensor 110, for example. In another example, the glucose sensor must be placed in electrical and/or optical contact with the glucose meter and a secret key may be transmitted via the electrical and/or optical contact.

[0021] In the CGM system 100, the example glucose sensor 110 is a low power device that is typically replaced every 5-7 days. As such, the glucose sensor 110 is initially in a low power state or a powerless state to preserve its power source before being actuated to communicate with the glucose meter 105. Accordingly, to activate the CGM system 100, the glucose sensor 110 must be actuated (i.e., turned on) and the glucose meter 105 and the glucose sensor 110 must be exchange information to enable wireless communication to enable the CGM system 100.

[0022] To preserve power, the power source of the glucose sensor 110 may not be electrically coupled to the other electric devices in the glucose sensor 110 using, for example, any suitable latch or a switch. An operation by a user may cause the latch to close, thereby electrically coupling the power source to the electrical devices in the glucose sensor 110 to turn it on. For example, the glucose meter 105 in Fig. 1 includes a receptacle 125 configured to receive the glucose sensor 110. The receptacle 125 may also include a mechanical contact that biases a latch in the glucose sensor 110 to couple the power source to the electrical devices therein, thereby actuating the glucose sensor 110. The receptacle 125 may also include a switch (e.g., optical, mechanical, electrical, etc.) that detects the presence of the glucose sensor 110 when disposed therein.

[0023] In this example, when the glucose sensor 110 is disposed in the receptacle 125, the glucose sensor 110 is actuated and the glucose meter 105 is informed that the glucose sensor 110 is disposed in the receptacle 125 in a single step. In other examples, the user may initiate that the glucose sensor is proximate to the glucose meter by depressing a button disposed on the glucose meter 105 and/or the glucose sensor 110, for example. To enable communication, unique information must be exchanged to indicate that the transmitted data is provided from the glucose meter 105 and/or glucose sensor 110. As noted above, prior devices used a number unique on the device itself that identified it. However, the example glucose meter and/or the example sensor generate a secret key using a random process and exchange the secret key using the NFC wireless link. Using the secret key, the glucose meter 105 and glucose sensor 110 encrypt and decrypt data based on the secret key.

[0024] In a preferred embodiment, the glucose sensor 110 remains idle in a low or zero power state until the glucose meter 105 is brought into close proximity to the sensor. In this example, it will be understood that the roles of the sensor and meter may be exchanged, and only the example of the sensor remaining in a low power state until activated is provided herein. Both the sensor 110 and the meter 105 include an inductive element 208/308 for NFC communication. Preferably, the meter 105 is brought into close proximity to the sensor 110, and then the meter's inductive element 208 is energized. The energized inductive element 208 produces a magnetic field that induces a current in the sensor 105 inductive element 308 due to their close proximity. The sensor is preferably programmed to begin the pairing process when the appropriate current is induced in the inductive element 308 by the energized meter inductive element 208. Advantageously, this method avoids unnecessary battery drain that results from conventional methods of pairing including periodic polling. Moreover, the inductive nature of the pairing permits energy to be delivered to the sensor from the energized meter inductive element 308 due to the inductive link, further reducing battery drain, and even charging the battery of the sensor.

[0025] Further, the glucose meter 105 and the glucose sensor 110 may also exchange information relating to the health of the glucose sensor 110 (e.g., spoilage information, battery status, expiration date, etc.) to determine if the glucose sensor 110 is suitable for use. For instance, the glucose sensor 110 may transmit a preprogrammed expiration date to the glucose meter 105, which determines if the glucose sensor 110 is safe to use. In another example, the glucose sensor 110 may determine that it has spoiled by being exposed to a predetermined temperature for a particular period of time. As such, the glucose sensor 110 may transmit an indication of the duration it was exposed to the predetermined temperature to the glucose meter 105, which determines if the glucose sensor 110 is safe to use. In the event that the glucose meter 105 determines the glucose sensor 110 is not safe to use, the shared key is not exchanged to prevent use of the glucose sensor 110 with the glucose meter 105.

[0026] Fig. 2 illustrates a block diagram of an example glucose meter 105. Generally, the glucose meter 105 includes a controller 200 that is implemented by any suitable device to control the operation of the glucose meter 105 (e.g., a microcontroller, a microprocessor, an application specific integrated circuit, a functional programmable gate array, etc.). The controller 200 in the example

of Fig. 2 includes an antenna 202 configured for receiving wireless communication signals and transmitting the received signals to an RF receiver 204, which converts (e.g., amplifies, demodulates, decodes, etc.) the received signal into data for the controller 200. In some examples, the controller 200 may need to process (e.g., decode, error check, etc.) the received data before use.

[0027] As described above, the glucose meter 105 also includes an NFC transceiver 206 for sending and receiving data over the NFC wireless link. In such an example, the NFC transceiver 206 receives data from the controller 200 to transmit the data via an inductor 208. As described above, a current flowing through the inductor 208 creates an electric field that induces a voltage in a corresponding inductor. Similarly, a voltage can be induced on the inductor 208 that is received by the NFC transceiver 206, thereby receiving a signal from a transmitting device. The NFC transceiver 206 receives the transmitted signal, converts it into the transmitted signal into data, which is then provided to the controller 200.

[0028] The controller 200 is coupled to receive data from an interface unit 210. The interface unit 210 is any suitable interface to operate the glucose meter. For example, the interface unit 210 may include a one or more buttons that allow the user to control the glucose meter 105. The controller 200 is further coupled to the display driver 212 to provide instructions thereto to control a display 214. That is, the controller 200 provides instructions to the display driver 212 to display information for the user's consumption. In some examples, the display driver 212 may be integral with the controller 200.

[0029] Fig. 3 illustrates a block diagram of an example glucose sensor 110. Although the glucose sensor 110 is illustrated as a single device, it can be implemented by detachable modules that are fastened together. Generally, the glucose sensor 110 includes a controller 300 that is implemented by any suitable device to control the operation of the glucose sensor 110 (e.g., a microcontroller, a microprocessor, an application specific integrated circuit, a functional programmable gate array, etc.). The controller 300 is the example of Fig. 3 includes an antenna 302 configured for transmitting wireless communication signals and received signals from an RF transmitter 304, which converts (e.g., amplifies, demodulates, decodes, interleaves, etc.) data received from the controller 300 for transmission to a receiving device such as the glucose meter 105, for example. In some examples, the controller 300 may need to process (e.g., encode, generate error check data, etc.) the data before transmission.

[0030] As described above, the glucose sensor 110 also includes an NFC transceiver 306 for sending and receiving data over the NFC wireless link. In such an example, the NFC transceiver 306 receives data from the controller 300 to transmit the data via an inductor 308. In the event a current flows through the inductor 308, the inductor 308 creates an electric field that induces a voltage in a corresponding inductor. Similarly, a voltage can be induced on the inductor 308 that is received by the NFC transceiver 306, thereby receiving a signal from a transmitting device. The NFC transceiver 306 receives the transmitted signal, converts it into the transmitted signal into data, which is then provided to the controller 300. In other examples, the NFC transceiver 306 may be configured for simplex transmission as well.

[0031] The glucose sensor 110 also includes a sensor 310 that is configured to interface with the filament 115 and receive data therefrom. The sensor 310 converts the data into digital form and transmits the information to controller 300. Accordingly, the controller 300 receives the data and generates a glucose measurement of the user, and then transmits the measurement via the RF transmitter 304 to the glucose meter 105. Using the received data, the glucose meter 105 displays the current glucose measurement on its display 214. In another example, the sensor 310 may be integral with the controller 300. As noted above, the glucose sensor 110 may be modular such that different modules can be replaced at different time intervals. For example, the sensor 310 may be implemented in a separate module for replacement every week.

[0032] In the examples of Figs. 2 and 3, the RF receiver 204 and the RF transmitter 304 are generally described using a simplex transmission scheme. However, in other examples, duplex communication may be required. As such, the glucose meter 105 and glucose sensor 110 would include an RF transceiver for duplex communication. Further, any suitable wireless link that allows encryption of traffic and an error check to determine that the data was properly decrypted may be implemented between the glucose meter 105 and glucose sensor 110. For example, a suitable communication link may be provided by standardized communication protocols such as ZigBee®, Bluetooth®, 802.11 related standards, radio frequency identification (RFID), and so forth. Generally, low power modes such as Bluetooth® low energy (BLE) are preferable due to the glucose sensor 110 being disposable.

[0033] Fig. 4 illustrates an example process 400 of synchronizing the glucose meter and glucose sensor. The particular sequence of communications is described with reference to the data that is transmitted and received, but without reference to the transmitting or receiving device because the glucose meter and glucose sensor may perform either function. That is, the glucose meter could be the transmitter, receiver, or both. Similarly, the glucose sensor could be the transmitter, the receiver, or both.

[0034] Initially, the glucose sensor is placed in proximity with the glucose meter at block 405. Generally, the glucose sensor must be placed within range to initiate an NFC link, as described above. In some examples, the glucose sensor may be placed in a receptacle of the glucose meter. Preferably, the glucose meter inductor 208 is energized in close proximity to the glucose sensor inductor 308, such that a current is induced in the glucose

sensor inductor 308. The induced current in the glucose sensor inductor 308 preferably triggers the pairing process to begin. At block 410, the example process 400 receives an instruction to setup a secure channel between the glucose sensor and the glucose meter. For example, in the event the glucose meter includes a receptacle having a detector to detect when the sensor is disposed therein, the glucose meter generates a signal to indicate to setup a secure channel with the glucose sensor. In other examples, the glucose meter and/or glucose sensor may include a switch that a user depresses to pair the glucose sensor with the glucose meter.

[0035] In response to the instruction provided at block 410, a determination is made if the glucose sensor is suitable for operation at block 415 using the NFC wireless link. For example, a determination is made that the glucose sensor has suitable battery power to operate for a required period (e.g., at least one day, etc.). In another example, a determination is made that the glucose sensor has not spoiled due to an expiration date or due to exposure to unsuitable environmental conditions (e.g., temperature, humidity, etc.). If the sensor fails the determination at block 415, the glucose meter cannot pair the glucose sensor and the example process 400 ends.

[0036] In the event that the sensor succeeds in the determination at block 415, the example process 400 generates a secret key and transmits the secret key over the NFC link so that both the glucose sensor and the glucose meter share the same secret key at step 420. In one example, the secret key is generated by any suitable random process for securing a wireless link. For example, the example process 400 may implement a cryptographically secure pseudorandom number generator to generate a 128-bit secret key. Because the glucose meter and the glucose sensor must be close in proximity, it is unlikely any other device will be nearby to receive or intercept the secret key. Further, once transmitted, there generally is no need to exchange the secret key again.

[0037] After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter setup a secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc). In particular, the glucose meter and glucose sensor transmit data over the wireless channel that is encrypted using any suitable encryption algorithm (e.g., advanced encryption standard, data encryption standard, etc.) using the secret key, thereby forming a secure wireless link. In one example, using the data for transmission, the transmitting device generates an error check information such as a cyclic redundancy check (CRC) or a hash such as MD5, which is encrypted and transmitted with the data. The receiving device will decrypt the received information using the secret key and verify that the decryption is successful using the error check information. In another example, the CGM system 100 may verify that the secret key was successfully received before transmission of glucose measurement data over the secure wireless link.

[0038] After the glucose meter and the glucose sensor are transmitting the data via the secure wireless link at step 430, the example process 400 ends. Generally, the glucose meter or the glucose sensor will provide a perceptible indication to the user that communication has initiated and the user may fasten the glucose sensor to their skin.

[0039] Although example process 400 describes a particular sequence of events, the example process 400 and not limited and could be modified to perform all or some of the described functionality. For instance, determining that the sensor is suitable for operation at block 415 may be omitted.

[0040] Figs. 5-8 illustrate examples of different sequences of communication between the glucose meter 105 and the glucose sensor 110 to implement the example process 400. In the described examples, the glucose meter 105 and glucose sensor 110 are close in proximity such that they communicate via the NFC wireless link. Unless otherwise indicated, the described communications are generally performed over the NFC wireless link until the secure wireless link is fully setup.

[0041] Fig. 5 illustrates an example of a CGM system 100 that determines the health of the glucose sensor 110 before data transmission can begin. At step 502, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 transmits a request to the glucose sensor 110 for health information at step 504. In some examples, an initial message would indicate that the glucose meter 105 is requesting the information without explicit instructions. The glucose sensor 110 generates its health information (e.g., battery voltage, spoilage information, temperature information, expiration date, etc.) and transmits the health information to the glucose meter 105 at step 506. Using the received health information of the glucose sensor 110, the glucose meter 105 determines if the glucose sensor 110 is suitable for use in the CGM system at step 508. If the glucose sensor 110 is not suitable, the communications ends and the glucose sensor 110 is not paired with the glucose meter 105, as described above. For example, the glucose meter 105 could transmit a kill signal to the glucose sensor 110, which fully disables the glucose sensor 110.

[0042] If the glucose sensor 110 is determined to be suitable for use at step 508, the glucose meter 105 generates a secret key that is transmitted to the glucose sensor at step 510. As noted above, the secret key may be generated by any suitable random process for securing the wireless link. At step 512, the glucose sensor 110 stores the secret key and sets up the channel with the glucose meter 105. The glucose sensor 110 then begins transmitting data associated with a measurement of the user (e.g., glucose information, etc.) to the glucose meter at step 514 over the secure channel.

[0043] Fig. 6 illustrates another example of a CGM system that implements a passive glucose sensor that having a one-time programmable (OTP) radio frequency

identification (RFID) tag. In such an example, at step 602, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 generates a secret key and transmits the secret key to the glucose sensor 110 at step 604. Using the received secret key, the glucose sensor 110 programs the secret key into its memory at step 606. For example, the glucose sensor 110 could include a Class 1 RFID tag that is programmable a single time with the secret key. In this example, the glucose meter 105 initiates reception of data using the secret key in response to transmitting the secret key. After the glucose sensor 110 has programmed the secret key, it begins transmitting data over the secure channel at step 608. In other examples, the glucose sensor 110 can be disabled by providing a kill instruction from the glucose meter 105.

[0044] In the example of Fig. 6, the OTP glucose sensor 110 implements a simple, low cost passive NFC link that provides limited functionality and is disposable. In this example, the glucose sensor 110 cannot be programmed with another secret key, thereby preventing it from being used again for safety purposes.

[0045] In other examples, the glucose sensor 110 may provide more functionality and thereby require a longer operational period. As such, it may be beneficial to enable the glucose sensor 110 to be reconfigured with the glucose meter 105. In the example of Fig. 7, at step 702, the glucose sensor 110 receives instruction to setup a secure wireless link with the glucose meter 105. In response, at step 704, the glucose sensor 110 generates a secret key and transmits it to the glucose meter 105. In response to receiving the secret key, the glucose meter 706 initiates reception of the wireless channel using the secret key at step 706. The glucose sensor 110 may wait a predetermined period of time (e.g., 1 second) for the glucose meter 105 to initiate data reception. After this period of time expires, the glucose sensor 110 transmits data over the secure channel at step 708.

[0046] In the example of Fig. 7, the glucose sensor 110 is reprogrammable and therefore can be reused. For instance, the glucose meter 105 may also include an insulin pump that is replaced monthly by the user. In such an example, the glucose meter 105 may need its power source (e.g. a battery, etc.) to be replaced, thereby requiring the secure wireless channel to be temporarily disabled. As such, after actuating the glucose meter 105 with a new power source, the glucose meter 105 and the glucose sensor 110 would exchange another secret key to initiate communication again. In another example, the battery in the glucose sensor 110 may be fastened such that it is not replaceable, and a new glucose sensor would be needed.

[0047] Fig. 8 illustrates another CGM system 100 that verifies successful reception of the secret key. At step 802, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 generates and transmits a secret key to the glucose sensor 110 at step 804. The glucose sensor 110 stores the secret key at step 806 to initiate setup the secure wireless link. Initially, the glucose sensor 110 transmits test data to the glucose meter 105 at step 808. The test data could be a random data or predetermined data that the glucose meter 105 also possesses. In the event the data is random, the transmitted data would include error check information to determine successful reception and decryption of the random data.

[0048] In response to receiving the test data, the glucose meter 105 decrypts the test data and determines if the test data was successfully received at step 810. If the test data is successfully received, the glucose meter 105 then determines that the secret key was successfully received by the glucose sensor 110. The glucose meter 105 then transmits an acknowledge message to the glucose sensor 110 via either the NFC link of the secure wireless channel at step 812. Upon reception of the acknowledge message, the glucose sensor 110 has fully setup the secure wireless channel and begins transmission of data using the secure wireless channel at step 814. In the event that the glucose meter 105 does not verify the secret key at 810, the sequence of communication would return to step 804 until the secret key is successfully determined to be received by the glucose sensor 110.

[0049] In accordance with an illustrative embodiment of the present invention, an inductive coupling link is provided to extend product shelf-life and improve patient data security of RF-controlled devices having factory-installed, non-accessible primary-cell batteries such as an internal sensor (such as an internal patch, subcutaneous sensor, or internal electrode, among other sensing devices). RF receiver circuitry for the heavily used bands available to such devices demodulates and examines received signals in order to determine whether the signal is of interest to the device. This can require too much power to be performed continuously. Therefore, low-power RF devices generally synchronize with their counterparts, and thereafter operate intermittently (e.g., on a predetermined schedule).

[0050] In the case of a sealed consumable product (such as an implanted consumable sensor 110), linked via RF communication to a reusable/durable user interface and control device (such as a durable handheld meter 105), deployment of a new device involves, in part, the synchronization and "pairing" of the consumable device and the durable device(s). In order for this initial, unscheduled exchange to take place, the consumable device must be listening for a message from an as-yet unknown instance of a durable device. Because the initial communication may occur days or months after manufacture, the consumable device's pre-synchronization listening would occur only at fairly infrequent intervals. The length of the interval would directly affect the user, as synchronization at time of deployment would require maintaining the new consumable device 30 within com-

munication range of the durable device(s) for at least the length of this interval prior to use.

[0051] In accordance with an aspect of an illustrative embodiment of the present invention, the inductive coupling link augments the consumable device 110 by including a second means of communication between the durable device(s) 105 and the consumable device 110. This second communication mechanism is used, for example, in lieu of the normal RF link (that is, the RF link used during regular operation of the sensor 30 following initialization) for the purpose of initial synchronization and pairing. By employing inductive (quasi-static H-field) coupling with relatively simple modulation, for example, a passive detector on the consumable product 110 can draw its operating power from the signal itself, and remain ready-to-detect at all times without consuming battery power. This improves responsiveness of the sensor 110, while extending its shelf life.

[0052] The pairing operation mentioned above allows the durable device(s) 105 and consumable devices 110 to exchange cryptographic keys and identifying information that ensures that subsequent communication between the devices 110 and 105 is secure. The pairing operation itself, however, is vulnerable to attack. If the pairing is compromised, the security of subsequent operations may also be compromised. By using an inductive coupling link to perform certain steps of the pairing operation, however, the security of the transaction is greatly increased because of the unlikelihood of the short-range, relatively nonstandard inductive coupling transmission being correctly received and decoded.

[0053] It should further be appreciated that the nature of the inductive coupling described above is capable of delivering energy to the consumable device 110 from the durable device 105 via the inductive link, further lengthening the battery and shelf life of the consumable device 110.

[0054] A diabetes management system (e.g., a continuous glucose monitoring system) is described for illustrative purposes, but it is to be understood that the improved methods, devices and systems can be used for monitors or other devices for management of other physiological conditions such as, but not limited to, arrhythmia, heart failure, coronary heart disease, diabetes, sleep apnea, seizures, asthma, chronic obstructive pulmonary disease (COPD), pregnancy complications, tissue or wound state, state of wellness and fitness of a person (e.g., weight loss, obesity, heart rate, cardiac performance, dehydration rate, blood glucose, physical activity or caloric intake), or combinations thereof.

[0055] Some examples of a meter 105 can be, but is not limited to, a personal computer, a portable computer such as a laptop or a handheld device (e.g., personal digital assistant (PDA), iPod), mobile telephone such as a cellular telephone, Blackberry device, Palm device, or Apple iPhone device, a watch, a portable exercise device or other physiological data monitor (e.g., a meter connectable to a patient via a strap or incorporated into an article of clothing), among other user devices, each of which may be configured for data communication with the sensor or consumable device 110.

[0056] Some examples of measured or monitored physiological data include, but are not limited to ECG, EEG, EMG, SpO2, tissue impedance, heart rate, accelerometer, blood glucose, coagulation (e.g., PT-INR or prothrombin time (PT) and its derived measures of prothrombin ratio (PR) and international normalized ratio), respiration rate and airflow volume, body tissue state, bone state, pressure, physical movement, body fluid density, skin or body impedance, body temperature, patient physical location, or audible body sounds, among others, or a combination thereof.

[0057] The measured data can also be related to analytes such as, but not limited to, a substance or chemical constituent in a biological fluid (for example, blood, interstitial fluid, cerebral spinal fluid, lymph fluid or urine) that can be analyzed. Analytes can include naturally occurring substances, artificial substances, medicaments, metabolites, and/or reaction products. By way of examples, on or more analytes for measurement can be glucose; insulin; acarboxyprothrombin; acylcarnitine; adenine phosphoribosyl transferase; adenosine deaminase; albumin; alpha-fetoprotein; amino acid profiles (arginine (Krebs cycle), histidine/urocanic acid, homocysteine, phenylalanine/tyrosine, tryptophan); andrenostenedione; antipyrine; arabinitol enantiomers; arginase; benzoylecgonine (cocaine); biotinidase; biopterin; c-reactive protein; carnitine; carnosinase; CD4; ceruloplasmin; chenodeoxycholic acid; chloroquine; cholesterol; cholinesterase; conjugated 1-.beta. hydroxy-cholic acid; cortisol; creatine kinase; creatine kinase MM isoenzyme; cyclosporin A; d-penicillamine; de-ethylchloroquine; dehydroepiandrosterone sulfate; DNA (acetylator polymorphism, alcohol dehydrogenase, alpha 1-antitrypsin, cystic fibrosis, Duchenne/Becker muscular dystrophy, glucose-6-phosphate dehydrogenase, hemoglobin A, hemoglobin S, hemoglobin C, hemoglobin D, hemoglobin E, hemoglobin F, D-Punjab, beta-thalassemia, hepatitis B virus, HCMV, HIV-1, HTLV-1, Leber hereditary optic neuropathy, MCAD, RNA, PKU, Plasmodium vivax, sexual differentiation, 21-deoxycortisol); desbutylhalofantrine; dihydropteridine reductase; diptheria/tetanus antitoxin; erythrocyte arginase; erythrocyte protoporphyrin; esterase D; fatty acids/acylglycines; free .beta.-human chorionic gonadotropin; free erythrocyte porphyrin; free thyroxine (FT4); free tri-iodothyronine (FT3); fumarylacetoacetase; galactose/gal-1-phosphate; galactose-1-phosphate uridyltransferase; gentamicin; glucose-6-phosphate dehydrogenase; glutathione; glutathione perioxidase; glycocholic acid; glycosylated hemoglobin; halofantrine; hemoglobin variants; hexosaminidase A; human erythrocyte carbonic anhydrase I; 17-alpha-hydroxyprogesterone; hypoxanthine phosphoribosyl transferase; immunoreactive trypsin; lactate; lead; lipoproteins ((a), B/A-1, .beta.); lysozyme; mefloquine; netilmicin; phenobarbitone; phenyloin; phytanic/pristanic acid;

progesterone; prolactin; prolidase; purine nucleoside phosphorylase; quinine; reverse tri-iodothyronine (rT3); selenium; serum pancreatic lipase; sissomicin; somatomedin C; specific antibodies (adenovirus, anti-nuclear antibody, anti-zeta antibody, arbovirus, Aujeszky's disease virus, dengue virus, Dracunculus medinensis, Echinococcus granulosus, Entamoeba histolytica, enterovirus, Giardia duodenalisa, Helicobacter pylori, hepatitis B virus, herpes virus, HIV-1, IgE (atopic disease), influenza virus, Leishmania donovani, leptospira, measles/mumps/rubella, Mycobacterium leprae, Mycoplasma pneumoniae, Myoglobin, Onchocerca volvulus, parainfluenza virus, Plasmodium falciparum, poliovirus, Pseudomonas aeruginosa, respiratory syncytial virus, rickettsia (scrub typhus), Schistosoma mansoni, Toxoplasma gondii, Trepenoma pallidium, Trypanosoma cruzi/rangeli, vesicular stomatis virus, Wuchereria bancrofti, yellow fever virus); specific antigens (hepatitis B virus, HIV-1); succinylacetone; sulfadoxine; theophylline; thyrotropin (TSH); thyroxine (T4); thyroxine-binding globulin; trace elements; transferrin; UDP-galactose-4-epimerase; urea; uroporphyrinogen I synthase; vitamin A; white blood cells; and zinc protoporphyrin.

[0058] Salts, sugar, protein, fat, vitamins and hormones naturally occurring in blood or interstitial fluids can also constitute analytes, for example. Further, the analyte can be naturally present in the biological fluid, for example, a metabolic product, a hormone, an antigen, an antibody, and the like. Alternatively, the analyte can be introduced into the body such as, for example but not limited to, a contrast agent for imaging, a radioisotope, a chemical agent, a fluorocarbon-based synthetic blood, or a drug or pharmaceutical composition, including but not limited to insulin; ethanol; cannabis (marijuana, tetrahydrocannabinol, hashish); inhalants (nitrous oxide, amyl nitrite, butyl nitrite, chlorohydrocarbons, hydrocarbons); cocaine (crack cocaine); stimulants (amphetamines, methamphetamines, Ritalin, Cylert, Preludin, Didrex, PreState, Voranil, Sandrex, Plegine); depressants (barbituates, methaqualone, tranquilizers such as Valium, Librium, Miltown, Serax, Equanil, Tranxene); hallucinogens (phencyclidine, lysergic acid, mescaline, peyote, psilocybin); narcotics (heroin, codeine, morphine, opium, meperidine, Percocet, Percodan, Tussionex, Fentanyl, Darvon, Talwin, Lomotil); designer drugs (analogs of fentanyl, meperidine, amphetamines, methamphetamines, and phencyclidine, for example, Ecstasy); anabolic steroids; and nicotine. The metabolic products of drugs and pharmaceutical compositions can also be considered analytes. Analytes such as neurochemicals and other chemicals generated within the body can also be analyzed, such as, for example, ascorbic acid, uric acid, dopamine, noradrenaline, 3-methoxytyramine (3MT), 3,4-dihydroxyphenylacetic acid (DOPAC), homovanillic acid (HVA), 5-hydroxytryptamine (5HT), and 5-hydroxyindoleacetic acid (FHIAA).

[0059] Although only a few illustrative embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the illustrative embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of the appended claims and their equivalents.

Claims

1. A method for pairing a wireless physiological condition monitoring system, comprising:

   placing a physiological condition meter (105) in proximity with a physiological condition sensor (110);
   receiving an instruction to initialize communication between the physiological condition meter (105) and the physiological condition sensor (110);
   in response to the instruction and the physiological condition meter (105) being in proximity with the physiological condition sensor (110), generating a secret key at one of the physiological condition meter (105) and the physiological condition sensor (110) and transmitting the secret key to the other one of the physiological condition meter (105) and the physiological condition sensor (110) via a first communication link to provide a shared key that is shared between the physiological condition meter (105) and the physiological condition sensor (110); and
   transmitting measurement data to the physiological condition meter (105) from a physiological condition sensor (110) via a second communication link that is different from the first communication link the second communication link providing a secure wireless link based on the secret key.

2. The method of claim 1, wherein the secret key is generated using a random process, and/or further comprising encrypting the data using the secret key.

3. The method recited in claim 1, further comprising:

   receiving operational information from the physiological condition sensor (110) at the physiological condition meter (105) via the first communication link, the operational information comprising at least one of battery status, expiration data, and spoilage of the physiological condition sensor (110); and
   determining if the physiological condition meter (105) can transmit the secret key to the physiological condition sensor (110) based on the operational information, and/or
   further comprising actuating the physiological

condition sensor (110) based on the received instruction.

4. The method of claim 1, wherein the physiological condition sensor (110) comprises memory for storing the secret key that is programmable a single instance, and/or
further comprising verifying if the physiological condition meter (105) and the physiological condition sensor (110) have identical secret keys.

5. The method of claim 1, wherein the first communication link is selected from at least one of an electrical connection, a wireless connection, an inductive coupling connection, an optical connection, and a near field communication (NFC) link formed when the physiological condition meter (105) and the physiological condition sensor (110) are proximate to each other.

6. The method of claim 5, wherein the secure wireless link is a radio frequency (RF) link, and the NFC link is an inductive link and the range of the secure wireless link exceeds the range of the NFC link, and the physiological condition meter (105) and the physiological condition sensor (110) are proximate when placed within approximately 20 centimeters.

7. The method of claim 1, further comprising the steps of:

after placing the physiological condition meter (105) in proximity with the physiological condition sensor (110), energizing an inductive element (208, 308) in the physiological condition meter (105), and inducing a current in an inductive element (208, 308) in the physiological condition sensor (110); and
further comprising the step of
storing energy in the physiological condition sensor (110) from the induced current, or
when the physiological condition meter (105) inductive element (208, 308) induces the current in the inductive element (208, 308) of the physiological condition sensor (110), sending the instruction to initialize communication between the physiological condition meter (105) and the physiological condition sensor (110).

8. A wireless physiological condition monitoring system, comprising:

a physiological condition sensor (110) adapted to measure physiological condition of a user and transmitting the measured physiological condition data using a secure wireless link based on a secret key; and
a physiological condition meter (105) adapted to receive the measured physiological condition data via the secure wireless link based on the secret key and displaying the physiological condition data to the user,
wherein, in response to an instruction provided when the physiological condition sensor (110) and the physiological condition meter (105) are in proximity to each other, the secret key is generated and transmitted using another communication link that is different from the secure wireless link.

9. The wireless physiological condition monitoring system of claim 8, wherein the secret key is generated using a random process, and/or
the physiological condition sensor (110) includes a one-time programmable memory for storing the secret key, and/or
the physiological condition sensor (110) encrypts the measured physiological condition data using the secret key and the physiological condition meter (105) decrypts the received encrypted data using the secret key.

10. The wireless physiological condition monitoring system of claim 8, wherein the other communication link is a near field communication (NFC) link formed when the physiological condition meter (105) and the physiological condition sensor (110) are proximate to each other, and/or the secure link is a radio frequency (RF) link, and/or
the NFC link is an inductive link and the range of the secure wireless link exceeds the range of the NFC link, and/or
the physiological condition meter (105) and the physiological condition sensor (110) are proximate when placed within approximately 20 centimeters.

11. The wireless physiological condition monitoring system of claim 8, wherein the physiological condition meter (105) receives operational information of the physiological condition sensor (110) via the other communication link and determines if the physiological condition meter (105) can transmit the secret key to the physiological condition sensor (110) based on the operational information, and/or
the physiological condition sensor (110) is actuated based on the received instruction.

12. The wireless physiological condition monitoring system of claim 8, wherein the physiological condition sensor (110) comprises a first inductive element (208, 308) adapted to provide an inductive link between the first inductive element (208, 308) and a second inductive element (208, 308) in the physiological condition meter (105), and
wherein the instruction is generated and sent in response to an induced current of one of the inductive

elements (208, 308) induced by energization in the other of the inductive elements (208, 308), or wherein the physiological condition sensor (110) comprises an energy storage element, and the energy storage element is adapted to be charged by an induced current in the first inductive element (208, 308), the induced current being induced by energization of the second inductive element (208, 308).

13. The method of claim 1 wherein the first communication link is a wireless inductive link and further comprising the steps of:

in response to the instruction, transmitting the secret key via the wireless inductive link;
receiving the secret key via the wireless inductive link;
encrypting the measurement data to be transmitted between the physiological condition sensor (110) and physiological condition meter (105); and
transmitting the encrypted data between the physiological condition sensor (110) and the physiological condition meter (105) via the secure wireless link.

14. A physiological condition sensor (110) for measuring physiological condition in a physiological condition monitoring system, comprising:

a sensor (310) for measuring physiological condition of a user and generating physiological condition measurement data;
a connection (308) for providing a secret key to the physiological condition meter (105) via a first communication link if the secret key is generated by the physiological condition sensor (110) and for receiving the secret key from a physiological condition meter (105) if the secret key is generated by the physiological condition meter (105), wherein the physiological condition sensor (110) is placed in proximity with the physiological condition meter (105) before the secret key is generated in response to an instruction to initialize communication between the physiological condition meter (105) and the physiological condition sensor (110);
a controller (300) for encrypting the physiological condition measurement data using the secret key; and
a transmitter (304) for transmitting the encrypted physiological condition measurement data to the physiological condition meter (105) via a second communication link that is different from the first communication link, the second communication link providing a secure wireless link based on the secret key.

15. A physiological condition meter (105) for measuring physiological condition in a physiological condition monitoring system, comprising:

a controller (200) for receiving an instruction to provide a secret key to a physiological condition sensor (110) if the secret key is generated by the physiological condition meter (105), wherein the controller (200) generates a secret key based on the instruction;
a connection (208) for transmitting the secret key to the physiological condition sensor (110) if the secret key is generated by the physiological condition meter (105) and for receiving the secret key from the physiological condition sensor (110) if the secret key is generated by the physiological condition sensor (110) via a first communication link, wherein the physiological condition meter (105) is placed in proximity with the physiological condition sensor (110) to transmit the secret key before the secret key is generated in response to the instruction;
a receiver (204) for receiving the secret key from the physiological condition sensor (110) if the secret key is generated by the physiological condition sensor (110), and for receiving encrypted physiological condition measurement data via a second communication link that is different from the first communication link, the second communication link providing a secure wireless link based on the secret key, wherein the controller (200) decrypts the encrypted physiological condition measurement data using the secret key; and
a display to display a user's physiological condition level using the physiological condition measurement data.

Patentansprüche

1. Verfahren zum Koppeln eines drahtlosen Systems zur Überwachung von physiologischen Zuständen, mit den Schritten:

Platzieren eines Messgeräts (105) für physiologische Zustände in der Nähe eines Sensors (110) für physiologische Zustände;
Empfangen eines Befehls zum Initialisieren der Kommunikation zwischen dem Messgerät (105) für physiologische Zustände und dem Sensor (110) für physiologische Zustände;
in Reaktion auf den Befehl und die Nähe des Messgeräts (105) für physiologische Zustände zu dem Sensor (110) für physiologische Zustände, Erzeugen eines geheimen Schlüssels in dem Messgerät (105) für physiologische Zustände oder dem Sensor (110) für physiologi-

sche Zustände, und Senden des geheimen Schlüssels an die andere Einrichtung, nämlich das Messgerät (105) für physiologische Zustände und den Sensor (110) für physiologische Zustände, über eine erste Kommunikationsverbindung, um einen gemeinsamen Schlüssel bereitzustellen, der dem Messgerät (105) für physiologische Zustände und dem Sensor (110) für physiologische Zustände gemeinsam ist; und
Senden von Messdaten an das Messgerät (105) für physiologische Zustände von einem Sensor (110) für physiologische Zustände über eine zweite Kommunikationsverbindung, welche von der ersten Kommunikationsverbindung verschieden ist, wobei die zweite Kommunikationsverbindung eine sichere drahtlose Verbindung auf der Basis des geheimen Schlüssels bereitstellt.

2. Verfahren nach Anspruch 1, bei welchem der geheime Schlüssel unter Verwendung eines Zufallsprozesses erzeugt wird, und/oder ferner mit dem Schritt des Verschlüsselns der Daten unter Verwendung des geheimen Schlüssels.

3. Verfahren nach Anspruch 1, ferner mit den folgenden Schritten:

Empfangen von Betriebsinformationen von dem Sensor (110) für physiologische Zustände durch das Messgerät (105) für physiologische Zustände über die erste Kommunikationsverbindung, wobei die Betriebsinformationen den Batteriezustand und/oder Ablaufdaten und/oder Verschlechterung des Sensors (110) für physiologische Zustände; und
Feststellen, basierend auf den Betriebsinformationen, ob das Messgerät (105) für physiologische Zustände den geheimen Schlüssel an den Sensor (110) für physiologische Zustände senden kann, und/oder
ferner mit dem Schritt des Betätigens des Sensors (110) für physiologische Zustände basierend auf dem empfangenen Befehl.

4. Verfahren nach Anspruch 1, bei welchem der Sensor (110) für physiologische Zustände einen einmal programmierbaren Speicher zum Speichern des geheimen Schlüssels aufweist, und/oder
ferner mit dem Schritt des Prüfens, ob das Messgerät (105) für physiologische Zustände und der Sensor (110) für physiologische Zustände identische geheime Schlüssel aufweisen.

5. Verfahren nach Anspruch 1, bei welchem die erste Kommunikationsverbindung unter einer elektrischen Verbindung und/oder einer drahtlosen Verbindung und/oder einer Induktionskopplungsverbindung und/oder einer optischen Verbindung und/oder einer Nahfeldkommunikationsverbindung (NFC) gewählt ist, welche gebildet wird, wenn das Messgerät (105) für physiologische Zustände und der Sensor (110) für physiologische Zustände einander nah sind.

6. Verfahren nach Anspruch 5, bei welchem die sichere drahtlose Verbindung eine Funkfrequenzverbindung (RF) ist, und die NFC-Verbindung eine induktive Verbindung ist, und die Reichweite der sicheren drahtlosen Verbindung die Reichweite der NFC-Verbindung übertrifft, und das Messgerät (105) für physiologische Zustände und der Sensor (110) für physiologische Zustände einander nah sind, wenn sie innerhalb von ungefähr 20 Zentimetern platziert sind.

7. Verfahren nach Anspruch 1, ferner mit den folgenden Schritten:

nach dem Platzieren des Messgeräts (105) für physiologische Zustände in der Nähe des Sensors (110) für physiologische Zustände, Bestromen eines induktiven Elements (208, 308) in dem Messgerät (105) für physiologische Zustände und Induzieren eines Stroms in ein induktives Element (208, 308) in dem Sensor (110) für physiologische Zustände; und
ferner mit dem folgenden Schritt:

Speichern von Energie in dem Sensor (110) für physiologische Zustände aus dem induzierten Strom, oder
wenn das induktive Element (208,308) des Messgeräts (105) für physiologische Zustände einen Strom in dem induktiven Element (208, 308) des Sensors (110) für physiologische Zustände induziert, Senden des Befehls zum Initialisieren der Kommunikation zwischen dem Messgerät (105) für physiologische Zustände und dem Sensor (110) für physiologische Zustände.

8. Drahtloses System zur Überwachung von physiologischen Zuständen, mit:

einem Sensor (110) für physiologische Zustände, der zum Messen des physiologischen Zustands eines Benutzers geeignet ist und die gemessenen Daten des physiologischen Zustands unter Verwendung einer sicheren drahtlosen Verbindung auf der Basis eines geheimen Schlüssels sendet; und
einem Messgerät (105) für physiologische Zustände, das zum Empfangen der gemessenen Daten des physiologischen Zustands über die sichere drahtlose Verbindung auf der Basis des

geheimen Schlüssels geeignet ist, und dem Benutzer die Daten des physiologischen Zustands anzeigt,
wobei, in Reaktion auf einen Befehl, der gegeben wird, wenn der Sensor (110) für physiologische Zustände und das Messgerät (105) für physiologische Zustände einander nahe sind, der geheime Schlüssel erzeugt wird und unter Verwendung einer anderen Kommunikationsverbindung, die von der sicheren drahtlosen Verbindung verschieden ist, gesendet wird.

9. Drahtloses System zur Überwachung von physiologischen Zuständen nach Anspruch 8, bei welchem der geheime Schlüssel unter Verwendung eines Zufallsprozesses erzeugt wird, und/oder
der Sensor (110) für physiologische Zustände einen einmal programmierbaren Speicher zum Speichern des geheimen Schlüssels aufweist; und/oder
der Sensor (110) für physiologische Zustände die gemessenen Daten des physiologischen Zustands unter Verwendung des geheimen Schlüssels verschlüsselt, und das Messgerät (105) für physiologische Zustände die empfangenen verschlüsselten Daten unter Verwendung des geheimen Schlüssels entschlüsselt.

10. Drahtloses System zur Überwachung von physiologischen Zuständen nach Anspruch 8, bei welchem die andere Kommunikationsverbindung eine Nahfeldkommunikationsverbindung (NFC) ist, welche gebildet wird, wenn das Messgerät (105) für physiologische Zustände und der Sensor (110) für physiologische Zustände einander nah sind, und/oder die sichere Verbindung eine Funkfrequenzverbindung (RF) ist, und/oder
die NFC-Verbindung eine induktive Verbindung ist und die Reichweite der sicheren drahtlosen Verbindung die Reichweite der NFC-Verbindung übertrifft, und/oder
das Messgerät (105) für physiologische Zustände und der Sensor (110) für physiologische Zustände einander nah sind, wenn sie innerhalb von ungefähr 20 Zentimetern platziert sind.

11. Drahtloses System zur Überwachung von physiologischen Zuständen nach Anspruch 8, bei welchem das Messgerät (105) für physiologische Zustände Betriebsinformationen von dem Sensor (110) für physiologische Zustände über die andere Kommunikationsverbindung empfängt und auf der Basis der Betriebsinformationen feststellt, ob das Messgerät (105) für physiologische Zustände den geheimen Schlüssel an den Sensor (110) für physiologische Zustände senden kann, und/oder
der Sensor (110) für physiologische Zustände auf der Basis des empfangenen Befehls betätigt wird.

12. Drahtloses System zur Überwachung von physiologischen Zuständen nach Anspruch 8, bei welchem der Sensor (110) für physiologische Zustände ein erstes induktives Element (208, 308) aufweist, das geeignet ist, eine induktive Verbindung zwischen dem ersten induktiven Element (208, 308) und einem zweiten induktiven Element (208, 308) in dem Messgerät (105) für physiologische Zustände zu bilden, und
wobei der Befehl in Reaktion auf einen induzierten Strom eines der induktiven Elemente (208, 308), der durch Bestromen in dem anderen der induktiven Elemente (208, 308) induziert wird, erzeugt und gesendet wird, oder wobei der Sensor (110) für physiologische Zustände ein Energiespeicherelement aufweist, und das Energiespeicherelement geeignet ist, durch einen induzierten Strom in dem ersten induktiven Element (208, 308), wobei der induzierte Strom durch Bestromen des zweiten induktiven Elements (208, 308) induziert wird.

13. Verfahren nach Anspruch 1, bei welchem die erste Kommunikationsverbindung eine drahtlose induktive Verbindung ist, und ferner mit den folgenden Schritten:

Senden des geheimen Schlüssels über die drahtlose induktive Verbindung in Reaktion auf den Befehl;
Empfangen des geheimen Schlüssels über die drahtlose induktive Verbindung;
Verschlüsseln der zwischen dem Sensor (110) für physiologische Zustände und dem Messgerät (105) für physiologische Zustände zu sendenden Messdaten; und
Senden der verschlüsselten Daten zwischen dem Sensor (110) für physiologische Zustände und dem Messgerät (105) für physiologische Zustände über die sichere drahtlose Verbindung.

14. Sensor (110) für physiologische Zustände zum Messen von physiologischen Zuständen in einem System zur Überwachung von physiologischen Zuständen, mit:
einem Sensor (310) zum Messen des physiologischen Zustands eines Benutzers und zum Erzeugen von Messdaten des physiologischen Zustands:

einer Verbindung (308) zum Liefern eines geheimen Schlüssels an das Messgerät (105) für physiologische Zustände über die erste Kommunikationsverbindung, wenn der geheime Schlüssel von dem Sensor (110) für physiologische Zustände erzeugt wird, und zum Empfangen des geheimen Schlüssels von einem Messgerät (105) für physiologische Zustände, wenn der geheime Schlüssel durch das Messgerät

(105) für physiologische Zustände erzeugt wird, wobei der Sensor (110) für physiologische Zustände in der Nähe des Messgeräts (105) für physiologische Zustände platziert wird, bevor der geheime Schlüssel in Reaktion auf einen Befehl zum Initialisieren der Kommunikation zwischen dem Messgerät (105) für physiologische Zustände und dem Sensor (110) für physiologische Zustände erzeugt wird;
einer Steuerung (300) zum Verschlüsseln der Messdaten des physiologischen Zustands unter Verwendung des geheimen Schlüssels; und
einem Sender (304) zum Senden der Messdaten des physiologischen Zustands an das Messgerät (105) für physiologische Zustände über eine zweite Kommunikationsverbindung, die von der ersten Kommunikationsverbindung verschieden ist, wobei die zweite Kommunikationsverbindung eine sichere drahtlose Verbindung auf der Basis des geheimen Schlüssels bereitstellt.

15. Messgerät (105) für physiologische Zustände zum Messen von physiologischen Zuständen in einem System zur Überwachung von physiologischen Zuständen, mit:

einer Steuerung (200) zum Empfangen eines Befehls zum Liefern eines geheimen Schlüssels an einen Sensor (110) für physiologische Zustände, wenn der geheime Schlüssel von dem Messgerät (105) für physiologische Zustände erzeugt wird, wobei die Steuerung (200) einen geheimen Schlüssel auf der Basis des Befehls erzeugt;
einer Verbindung (208) zum Senden des geheimen Schlüssels an den Sensor (110) für physiologische Zustände, wenn der geheime Schlüssel von dem Messgerät (105) für physiologische Zustände erzeugt wird, und zum Empfangen des geheimen Schlüssels von dem Sensor (110) für physiologische Zustände über die erste Kommunikationsverbindung, wenn der geheime Schlüssel von dem Sensor (110) für physiologische Zustände erzeugt wird, wobei das Messgerät (105) für physiologische Zustände zum Senden des geheimen Schlüssels in der Nähe des Sensors (110) für physiologische Zustände platziert wird, bevor der geheime Schlüssel in Reaktion auf den Befehl erzeugt wird;
einem Empfänger (204) zum Empfangen des geheimen Schlüssels von dem Sensor (110) für physiologische Zustände, wenn der geheime Schlüssel von dem Sensor (110) für physiologische Zustände erzeugt wird, und zum Empfangen verschlüsselter Messdaten des physiologischen Zustands über eine zweite Kommunikationsverbindung, die von der ersten Kommunikationsverbindung verschieden ist, wobei die zweite Kommunikationsverbindung eine sichere drahtlose Verbindung auf der Basis des geheimen Schlüssels bereitstellt, wobei die Steuerung (200) die verschlüsselten Messdaten des physiologischen Zustands unter Verwendung des geheimen Schlüssels entschlüsselt; und
einer Anzeige zum Anzeigen eines physiologischen Zustandslevels eines Benutzers unter Verwendung der Messdaten des physiologischen Zustands.

Revendications

1. Procédé d'appariement d'un système de surveillance d'état physiologique sans fil, comprenant le fait :

de placer un dispositif de mesure d'état physiologique (105) à proximité d'un capteur d'état physiologique (110) ;
de recevoir une instruction pour initialiser une communication entre le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) ;
en réponse à l'instruction et au fait que le dispositif de mesure d'état physiologique (105) est à proximité du capteur d'état physiologique (110), de générer une clé secrète au niveau de l'un du dispositif de mesure d'état physiologique (105) et du capteur d'état physiologique (110) et de transmettre la clé secrète à l'autre du dispositif de mesure d'état physiologique (105) et du capteur d'état physiologique (110) via une première liaison de communication pour fournir une clé partagée qui est partagée entre le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) ; et
de transmettre des données de mesure au dispositif de mesure d'état physiologique (105) à partir d'un capteur d'état physiologique (110) via une deuxième liaison de communication qui est différente de la première liaison de communication, la deuxième liaison de communication fournissant une liaison sans fil sécurisée sur la base de la clé secrète.

2. Procédé de la revendication 1, dans lequel la clé secrète est générée en utilisant un processus aléatoire, et/ou comprenant en outre le fait de crypter les données en utilisant la clé secrète.

3. Procédé selon la revendication 1, comprenant en outre le fait :

de recevoir des informations opérationnelles à partir du capteur d'état physiologique (110) au niveau du dispositif de mesure d'état physiolo-

gique (105) via la première liaison de communication, les informations opérationnelles comprenant au moins l'un(e) d'un état de batterie, d'une date d'expiration et de la détérioration du capteur d'état physiologique (110) ; et
de déterminer si le dispositif de mesure d'état physiologique (105) peut transmettre la clé secrète au capteur d'état physiologique (110) sur la base des informations opérationnelles, et/ou comprenant en outre le fait d'actionner le capteur d'état physiologique (110) sur la base de l'instruction reçue.

4. Procédé de la revendication 1, dans lequel le capteur d'état physiologique (110) comprend une mémoire pour stocker la clé secrète qui est programmable pour une seule instance, et/ou
comprenant en outre le fait de vérifier si le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) ont des clés secrètes identiques.

5. Procédé de la revendication 1, dans lequel la première liaison de communication est choisie parmi au moins l'une d'une connexion électrique, d'une connexion sans fil, d'une connexion de couplage inductif, d'une connexion optique et d'une liaison de communication en champ proche (NFC) formée lorsque le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) sont proches l'un de l'autre.

6. Procédé de la revendication 5, dans lequel la liaison sans fil sécurisée est une liaison radiofréquence (RF), et la liaison NFC est une liaison inductive et la portée de la liaison sans fil sécurisée dépasse la portée de la liaison NFC, et le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) sont proches lorsqu'ils sont placés à environ 20 centimètres.

7. Procédé de la revendication 1, comprenant en outre les étapes qui consistent :

après avoir placé le dispositif de mesure d'état physiologique (105) à proximité du capteur d'état physiologique (110), à exciter un élément inductif (208, 308) dans le dispositif de mesure d'état physiologique (105) et à induire un courant dans un élément inductif (208, 308) dans le capteur d'état physiologique (110) ; et
comprenant en outre l'étape qui consiste
à stocker de l'énergie dans le capteur d'état physiologique (110) à partir du courant induit, ou
lorsque l'élément inductif (208, 308) du dispositif de mesure d'état physiologique (105) induit le courant dans l'élément inductif (208, 308) du capteur d'état physiologique (110), à envoyer l'instruction pour initialiser une communication entre le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110).

8. Système de surveillance d'état physiologique sans fil, comprenant :

un capteur d'état physiologique (110) adapté pour mesurer l'état physiologique d'un utilisateur et transmettre les données d'état physiologique mesuré en utilisant une liaison sans fil sécurisée sur la base d'une clé secrète ; et
un dispositif de mesure d'état physiologique (105) adapté pour recevoir les données d'état physiologique mesuré via la liaison sans fil sécurisée sur la base de la clé secrète et pour afficher les données d'état physiologique à l'utilisateur,
dans lequel, en réponse à une instruction fournie lorsque le capteur d'état physiologique (110) et le dispositif de mesure d'état physiologique (105) sont à proximité l'un de l'autre, la clé secrète est générée et transmise en utilisant une autre liaison de communication qui est différente de la liaison sans fil sécurisée.

9. Système de surveillance d'état physiologique sans fil de la revendication 8, dans lequel la clé secrète est générée en utilisant un processus aléatoire, et/ou le capteur d'état physiologique (110) comporte une mémoire programmable une seule fois pour stocker la clé secrète, et/ou
le capteur d'état physiologique (110) crypte les données d'état physiologique mesuré en utilisant la clé secrète et le dispositif de mesure d'état physiologique (105) décrypte les données cryptées reçues en utilisant la clé secrète.

10. Système de surveillance d'état physiologique sans fil de la revendication 8, dans lequel l'autre liaison de communication est une liaison de communication en champ proche (NFC) formée lorsque le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) sont proches l'un de l'autre, et/ou la liaison sécurisée est une liaison radiofréquence (RF), et/ou
la liaison NFC est une liaison inductive et la portée de la liaison sans fil sécurisée dépasse la portée de la liaison NFC, et/ou
le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) sont proches lorsqu'ils sont placés à environ 20 centimètres.

11. Système de surveillance d'état physiologique sans fil de la revendication 8, dans lequel le dispositif de mesure d'état physiologique (105) reçoit des informations opérationnelles du capteur d'état physiolo-

gique (110) via l'autre liaison de communication et détermine si le dispositif de mesure d'état physiologique (105) peut transmettre la clé secrète au capteur d'état physiologique (110) sur la base des informations opérationnelles, et/ou
le capteur d'état physiologique (110) est actionné sur la base de l'instruction reçue.

12. Système de surveillance d'état physiologique sans fil de la revendication 8, dans lequel le capteur d'état physiologique (110) comprend un premier élément inductif (208, 308) adapté pour fournir une liaison inductive entre le premier élément inductif (208, 308) et un deuxième élément inductif (208, 308) dans le dispositif de mesure d'état physiologique (105), et
dans lequel l'instruction est générée et envoyée en réponse à un courant induit de l'un des éléments inductifs (208, 308) induit par excitation dans l'autre des éléments inductifs (208, 308), ou
dans lequel le capteur d'état physiologique (110) comprend un élément de stockage d'énergie, et l'élément de stockage d'énergie est adapté pour être chargé par un courant induit dans le premier élément inductif (208, 308), le courant induit étant induit par excitation du deuxième élément inductif (208, 308).

13. Procédé de la revendication 1, dans lequel la première liaison de communication est une liaison inductive sans fil et comprenant en outre les étapes qui consistent :

en réponse à l'instruction, à transmettre la clé secrète via la liaison inductive sans fil ;
à recevoir la clé secrète via la liaison inductive sans fil ;
à crypter les données de mesure à transmettre entre le capteur d'état physiologique (110) et le dispositif de mesure d'état physiologique (105) ; et
à transmettre les données cryptées entre le capteur d'état physiologique (110) et le dispositif de mesure d'état physiologique (105) via la liaison sans fil sécurisée.

14. Capteur d'état physiologique (110) pour mesurer l'état physiologique dans un système de surveillance d'état physiologique, comprenant :

un capteur (310) pour mesurer l'état physiologique d'un utilisateur et générer des données de mesure d'état physiologique ;
une connexion (308) pour fournir une clé secrète au dispositif de mesure d'état physiologique (105) via une première liaison de communication si la clé secrète est générée par le capteur d'état physiologique (110) et pour recevoir la clé secrète à partir d'un dispositif de mesure d'état physiologique (105) si la clé secrète est générée par le dispositif de mesure d'état physiologique (105), où le capteur d'état physiologique (110) est placé à proximité du dispositif de mesure d'état physiologique (105) avant que la clé secrète ne soit générée en réponse à une instruction pour initialiser une communication entre le dispositif de mesure d'état physiologique (105) et le capteur d'état physiologique (110) ;
un dispositif de commande (300) pour crypter les données de mesure d'état physiologique en utilisant la clé secrète ; et
un émetteur (304) pour transmettre les données de mesure d'état physiologique cryptées au dispositif de mesure d'état physiologique (105) via une deuxième liaison de communication qui est différente de la première liaison de communication, la deuxième liaison de communication fournissant une liaison sans fil sécurisée sur la base de la clé secrète.

15. Dispositif de mesure d'état physiologique (105) pour mesurer l'état physiologique dans un système de surveillance d'état physiologique, comprenant :

un dispositif de commande (200) pour recevoir une instruction pour fournir une clé secrète à un capteur d'état physiologique (110) si la clé secrète est générée par le dispositif de mesure d'état physiologique (105), où le dispositif de commande (200) génère une clé secrète sur la base de l'instruction ;
une connexion (208) pour transmettre la clé secrète au capteur d'état physiologique (110) si la clé secrète est générée par le dispositif de mesure d'état physiologique (105) et pour recevoir la clé secrète à partir du capteur d'état physiologique (110) si la clé secrète est générée par le capteur d'état physiologique (110) via une première liaison de communication,
dans lequel le dispositif de mesure d'état physiologique (105) est placé à proximité du capteur d'état physiologique (110) pour transmettre la clé secrète avant que la clé secrète ne soit générée en réponse à l'instruction ;
un récepteur (204) pour recevoir la clé secrète à partir du capteur d'état physiologique (110) si la clé secrète est générée par le capteur d'état physiologique (110), et pour recevoir des données de mesure d'état physiologique cryptées via une deuxième liaison de communication qui est différente de la première liaison de communication, la deuxième liaison de communication fournissant une liaison sans fil sécurisée sur la base de la clé secrète,
dans lequel le dispositif de commande (200) décrypte les données de mesure d'état physiologique cryptées en utilisant la clé secrète ; et
un dispositif d'affichage pour afficher le niveau

d'état physiologique d'un utilisateur en utilisant les données de mesure d'état physiologique.

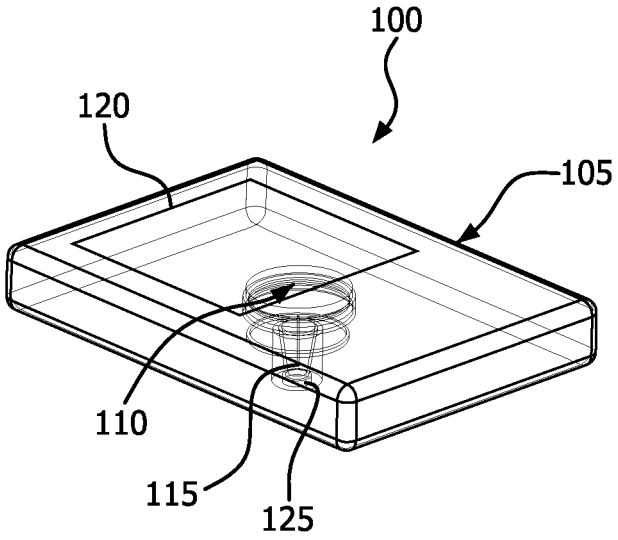
100
120
105
110
115
125

FIG. 1

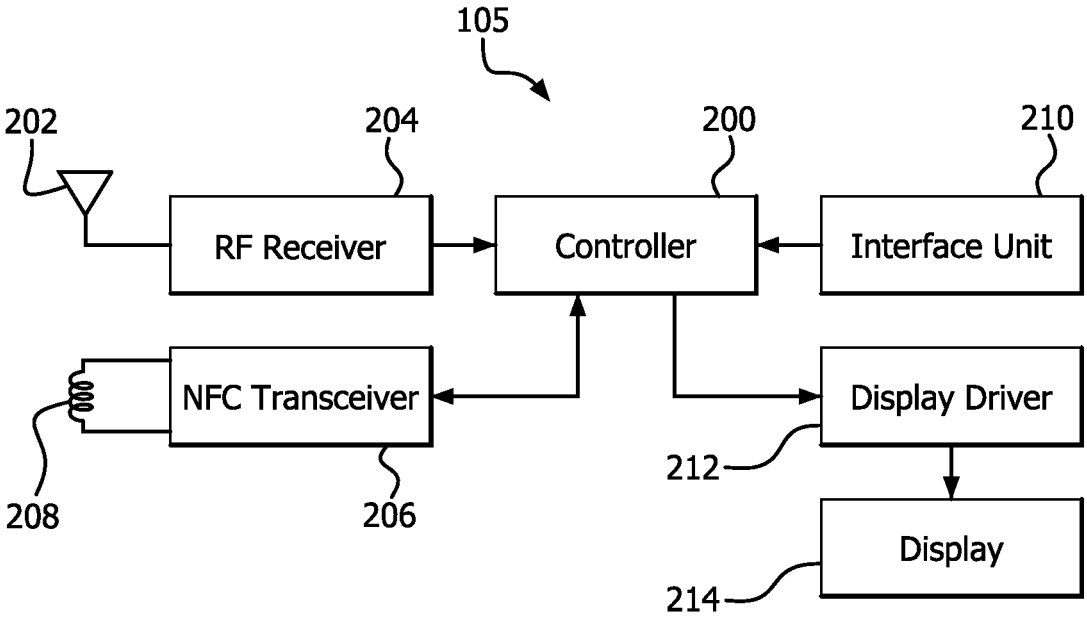
105
202
204
200
210
RF Receiver
Controller
Interface Unit
NFC Transceiver
Display Driver
212
208
206
Display
214

FIG. 2

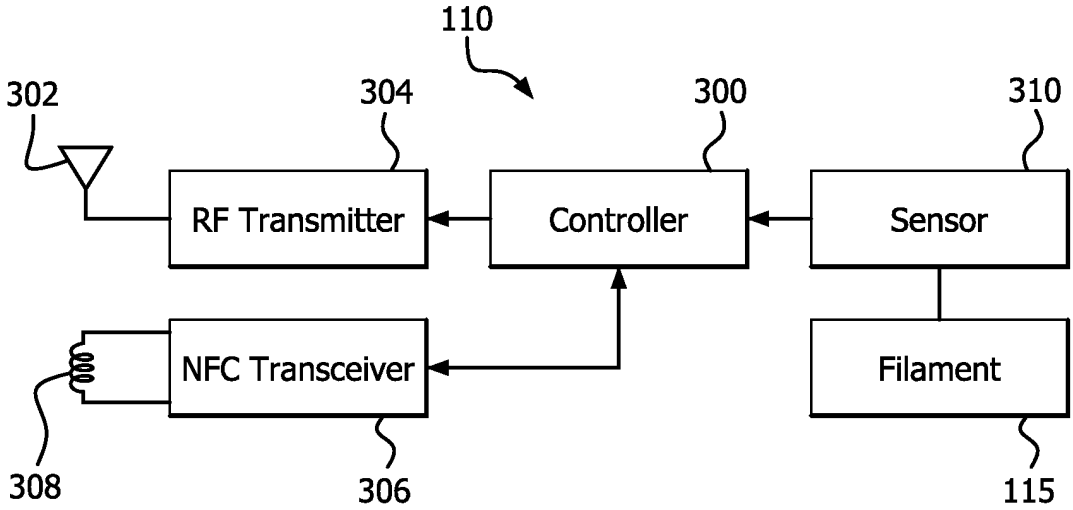
110
302
304
300
310
RF Transmitter
Controller
Sensor
NFC Transceiver
Filament
308
306
115

FIG. 3

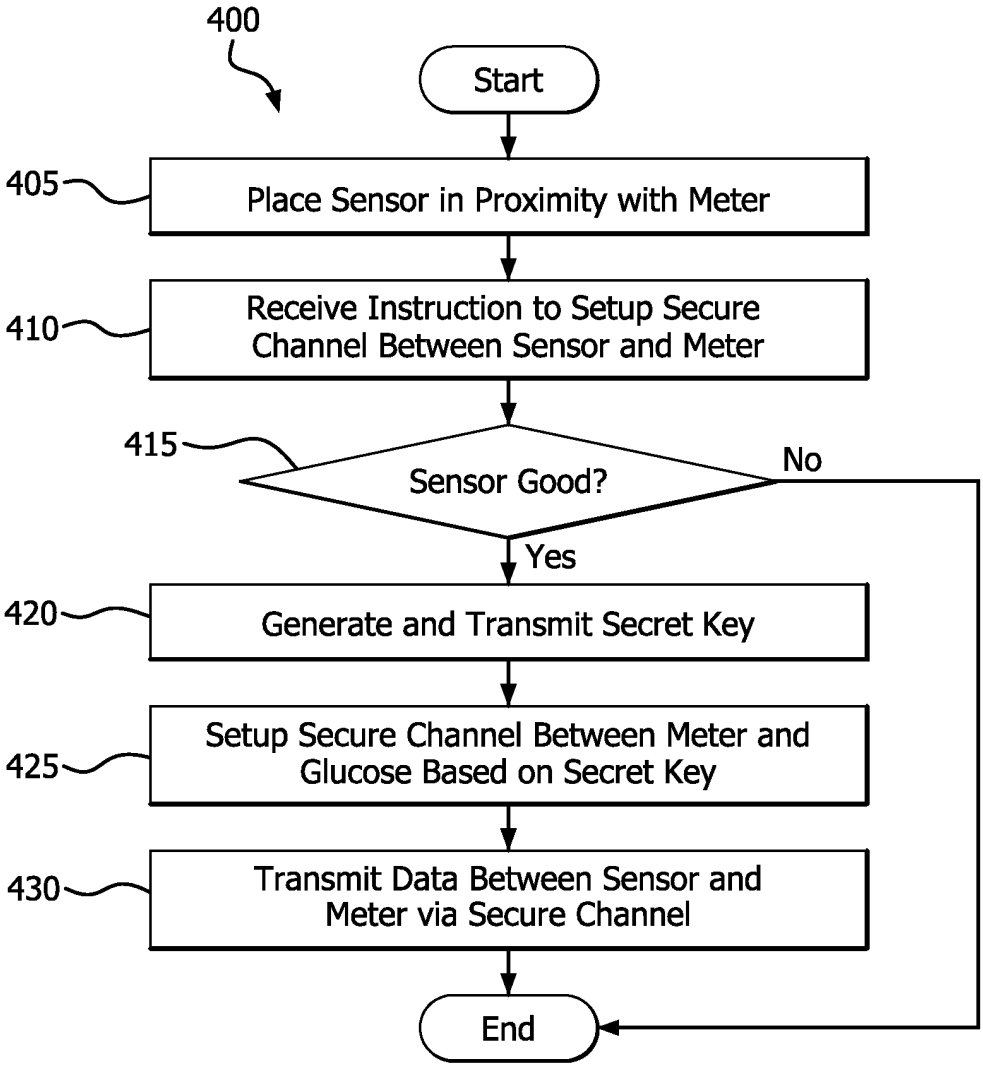
400
Start
405
Place Sensor in Proximity with Meter
410
Receive Instruction to Setup Secure Channel Between Sensor and Meter
415
Sensor Good?
No
Yes
420
Generate and Transmit Secret Key
425
Setup Secure Channel Between Meter and Glucose Based on Secret Key
430
Transmit Data Between Sensor and Meter via Secure Channel
End

FIG. 4

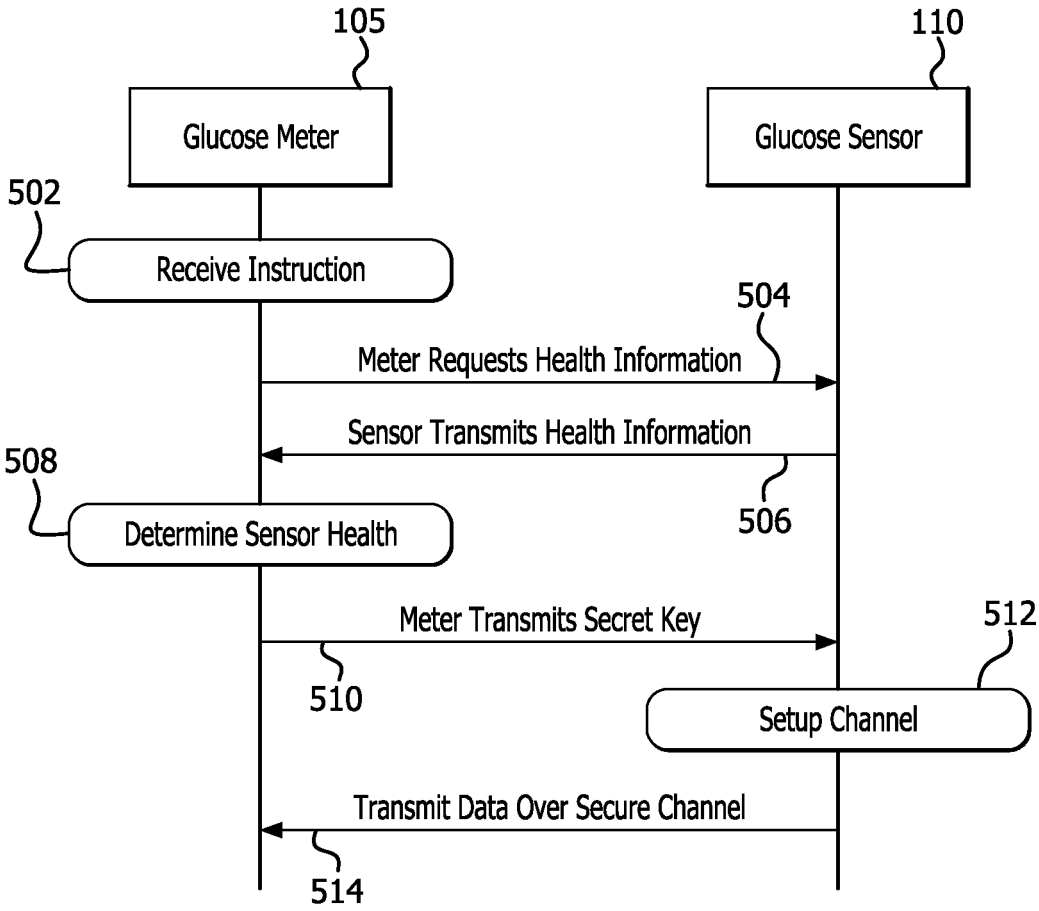
105
110
Glucose Meter
Glucose Sensor
502
Receive Instruction
504
Meter Requests Health Information
Sensor Transmits Health Information
508
506
Determine Sensor Health
Meter Transmits Secret Key
512
510
Setup Channel
Transmit Data Over Secure Channel
514

FIG. 5

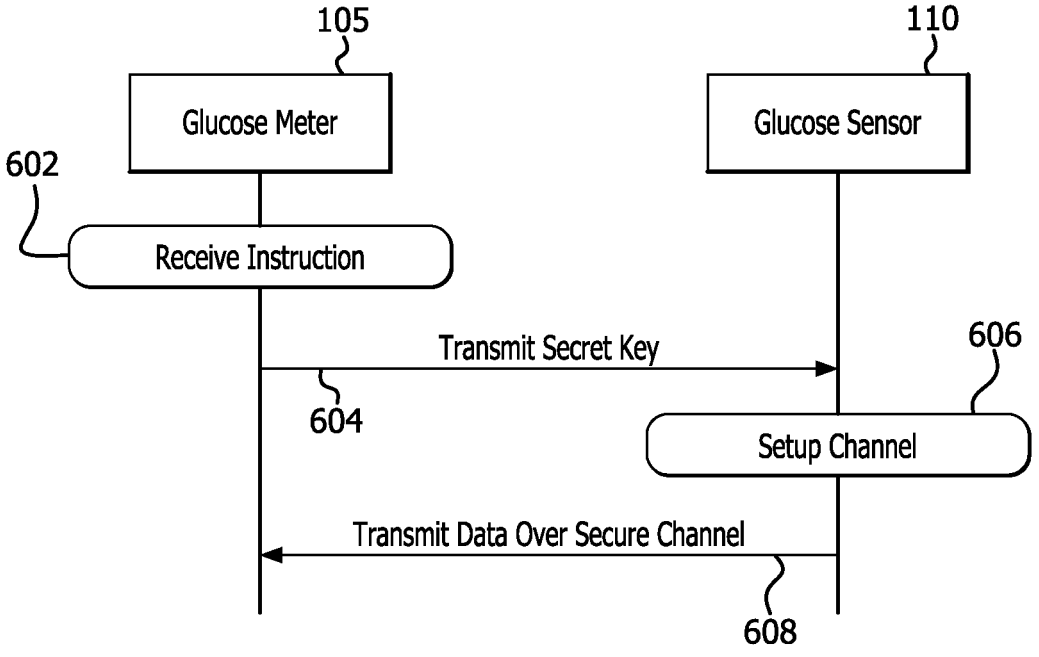
105
110
Glucose Meter
Glucose Sensor
602
Receive Instruction
Transmit Secret Key
606
604
Setup Channel
Transmit Data Over Secure Channel
608

FIG. 6

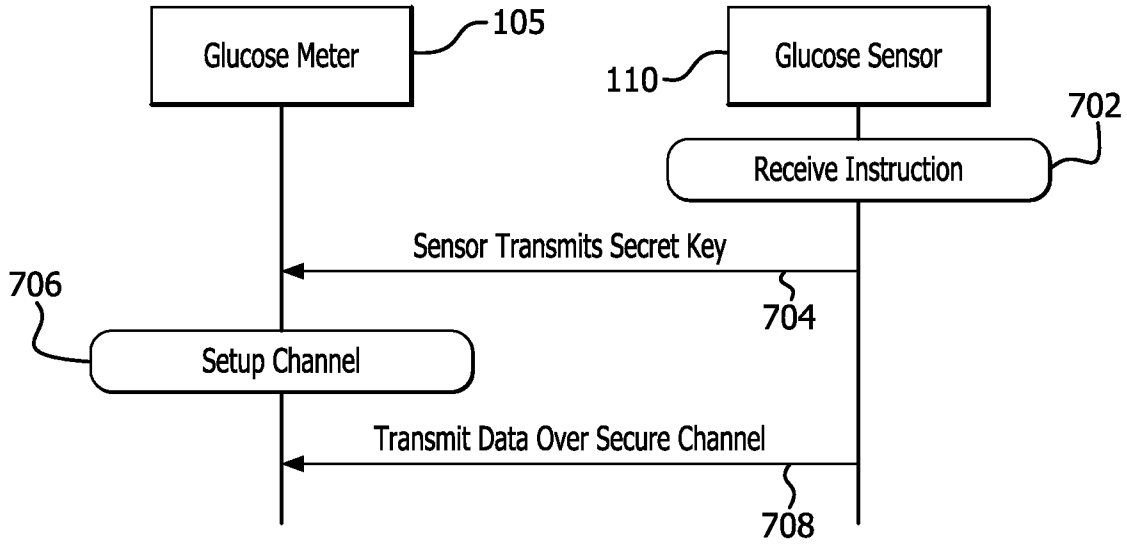
Glucose Meter
105
110
Glucose Sensor
702
Receive Instruction
Sensor Transmits Secret Key
706
704
Setup Channel
Transmit Data Over Secure Channel
708

FIG. 7

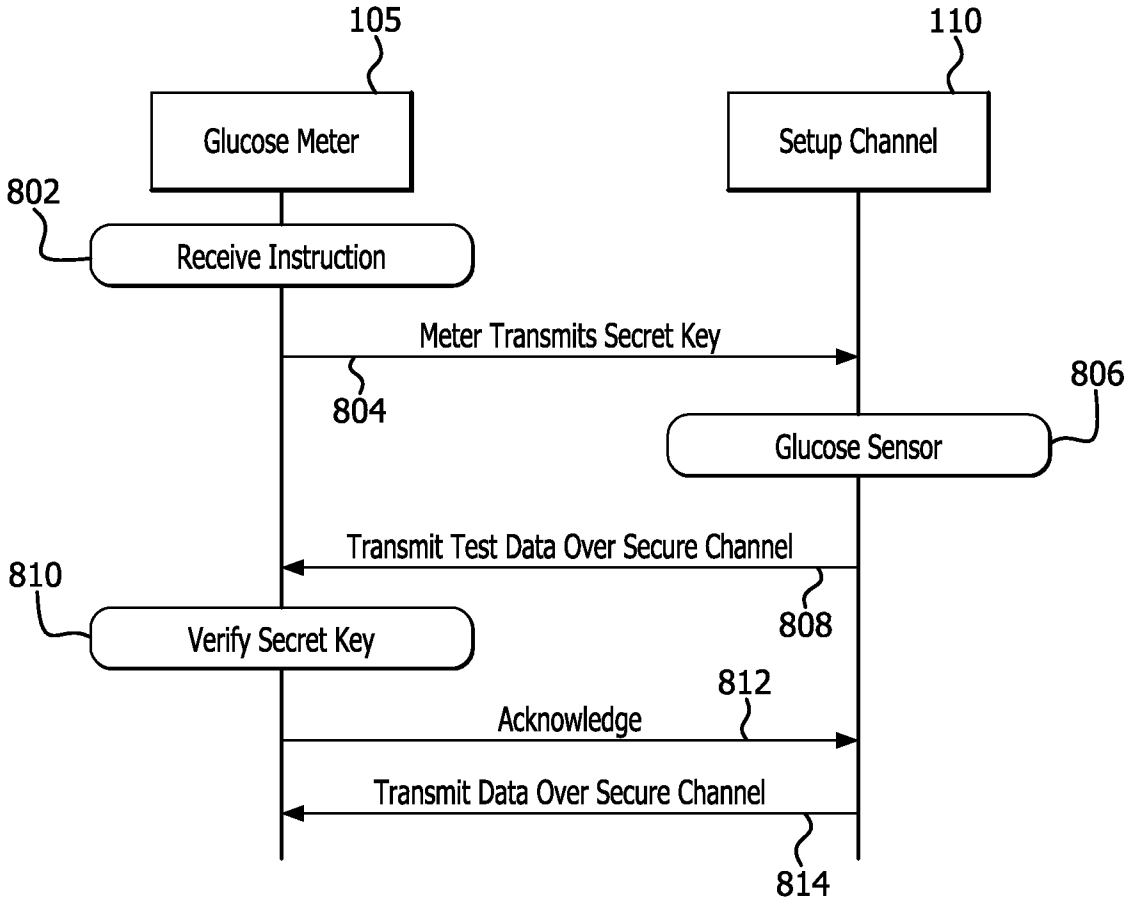
105
110
Glucose Meter
Setup Channel
802
Receive Instruction
Meter Transmits Secret Key
804
806
Glucose Sensor
Transmit Test Data Over Secure Channel
810
808
Verify Secret Key
812
Acknowledge
Transmit Data Over Secure Channel
814

FIG. 8

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2009153710 A2 **[0006]**
- US 20100045425 A1 **[0007]**
- US 20040266449 A1 **[0008]**
- WO 2009004578 A2 **[0009]**

专利名称(译)	近场遥测链路，用于在生理状态监测系统中传递共享秘密以建立安全的射频通信链路		
公开(公告)号	EP2791782A4	公开(公告)日	2015-10-21
申请号	EP2012857131	申请日	2012-12-14
[标]申请(专利权)人(译)	贝克顿·迪金森公司		
申请(专利权)人(译)	流式细胞Dickinson公司		
当前申请(专利权)人(译)	流式细胞Dickinson公司		
[标]发明人	YARGER MICHAEL PETISCE JAMES DIRESTA ELLEN BURNS DEBORAH MASON DAVID		
发明人	YARGER, MICHAEL PETISCE, JAMES DIRESTA, ELLEN BURNS, DEBORAH MASON, DAVID		
IPC分类号	G06F7/04 A61B5/00 A61B5/145 G06F19/00 H04W4/00 H04W12/04 H04W12/06		
CPC分类号	A61B5/002 A61B5/02438 A61B5/14532 A61B5/7275 A61B5/742 G08C17/02 G16H15/00 G16H40/67 G16H50/20 G16H50/30 H04W4/80 Y02A90/26 A61B5/72 G06F19/00 G06F19/3456 G16H20/10 G16H20/60		
优先权	61/576309 2011-12-15 US		
其他公开文献	EP2791782A1 EP2791782B1		
外部链接	Espacenet		

摘要(译)

生理状况监测系统（例如，连续血糖监测系统）包括生理状况计量器和生理状况传感器。生理状况测量仪和生理状况传感器被放置在附近以使用近场无线链路交换秘密密钥，该近场无线链路用于加密数据以保护射频（RF）无线信道。