(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 November 2022 (24.11.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/245212 A1

(51) International Patent Classification:
A61N 1/36 (2006.01) *H04L 9/00* (2022.01)
A61N 1/372 (2006.01)

(21) International Application Number:
PCT/NL2022/050273

(22) International Filing Date:
19 May 2022 (19.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

20210100331	19 May 2021 (19.05.2021)	GR
2028563	29 June 2021 (29.06.2021)	NL
2028564	29 June 2021 (29.06.2021)	NL

(71) Applicant: **ERASMUS UNIVERSITY MEDICAL CENTER ROTTERDAM** [NL/NL]; Dr. Molewaterplein 50, 3015 GE Rotterdam (NL).

(72) Inventors: **SIDDIQI, Muhammad Ali**; c/o Dr. Molewaterplein 50, 3015 GE Rotterdam (NL). **STRYDIS, Christos**; c/o Dr. Molewaterplein 50, 3015 GE Rotterdam (NL). **DE ZEEUW, Christiaan Innocentius**; c/o Dr. Molewaterplein 50, 3015 GE Rotterdam (NL).

(74) Agent: **WITMANS, H.A.**; V.O., P.O. Box 87930, 2508 DH Den Haag (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: IMPLANTABLE MEDICAL DEVICE AND CONTROL DEVICE THEREFOR

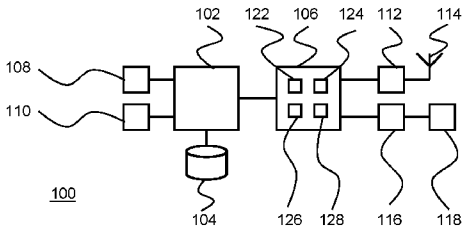


Fig. 1 A

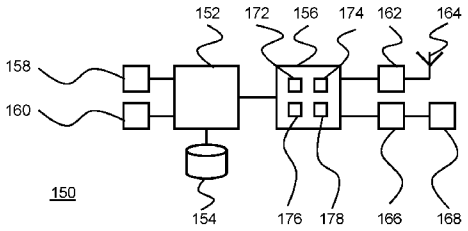


Fig. 1 B

(57) Abstract: In an implantable medical device, a method of communicating with a control device is provided. The method comprises receiving a first data message from the control device via a first physical communication channel, upon receiving the first message, activating a second physical communication channel different from the first physical communication channel and obtaining first authentication data of the control device, based on data provided in the first data message. The method further comprises receiving, via the second physical communication channel, a second message, verifying whether the second message originates from the control device, based on the obtained first authentication data and deactivating the second physical communication channel at the side of the implantable medical device if a result of the verifying is that the second message does not originate from the control device.

WO 2022/245212 A1

[Continued on next page]

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Title: implantable medical device and control device therefor

TECHNICAL FIELD

The various aspects and variations thereof relate to communication between an implantable medical device and a control device.

BACKGROUND

Implantable medical devices may be controlled by means of a control device. Such may be a dedicated device or a generally available device, like a smartphone. The communication may take place using radiofrequency communication or ultrasonic communication. As hacking of devices, causing the implantable medical device to demonstrate unwanted or dangerous behaviour or to drain a battery of the implantable medical device, is possible without the appropriate measures, security measures are provided.

SUMMARY

It is preferred to improve the currently available security measures. To that purpose, a first aspect provides, in an implantable medical device, a method of communicating with a control device. The method comprises receiving a first data message from the control device via a first physical communication channel, upon receiving the first message, activating a second physical communication channel different from the first physical communication channel and obtaining first authentication data of the control device, based on data provided in the first data message. The method further comprises receiving, via the second physical communication channel, a second message, verifying whether the second message originates from the control device, based on the obtained first authentication data.

This method allows for secure coupling of the control device with the implantable medical device. A first connection is made using a first

physical communication channel, for example ultrasound and via that connection, first security data is provided. The security data may be used to enable the control device to authenticate particular data sent to the implantable medical device. For the avoidance of doubt, to authenticate, within the context of this disclosure, is an equivalent of to certify, meaning to modify a message, by modifying data or by appending particular data, such that an origin of data may be verified, based on any action performed by an authentication step. Such action may be signing, encrypting, adding a certificate, other, or a combination thereof.

The data to be certified is certified and received by the implantable medical device. This enables the implantable medical device to verify that the message is received from the control device. This message, with the authenticated data to be verified, is sent via another physical communication channel. This allows for use of a further physical communication channel that may be, in physical nature, less secure as the ranger is wider, after more crucial and more basic security data has been exchanged over for example a physical communication channel that has a shorter range. The communication over the potentially less secure physical communication channel is at higher layers secured by, for example, cryptography, signing, certification, other means of authenticating data or a combination thereof. This allows for improved security and for flexibility of use of communication channels.

The second physical communication channel may be deactivated at the side of the implantable medical device if a result of the verifying is that the second message does not originate from the control device. By shutting down the second physical communication channel upon any verification error, improved security is provided and any further energy consumption is prevented, reducing risks of battery depletion attacks on the implantable medical device.

The method may further comprise sending, upon receiving the first message, via the first physical communication channel, a third message to the control device, the third message comprising second authentication data, wherein the first authentication data is further based on the second authentication data. This may allow for symmetrical key generation, in which a generated key is based on data from the implantable medical device, as well as data from the control device.

The second authentication data may comprise at least one of a medical device identifier identifying the implantable medical device and random medical device data. By including the medical device identifier, fixed data related to the medical device may be used. Such data identifies the applicable device and the data is readily available. Use of random data reduces a risk of spoofing.

The first data message may comprise at least one of a control identifier identifying the control device and random control data and the first authentication data may further be based on at least one of the control identifier and the random control data. By including the medical device identifier, fixed data related to the medical device may be used. Such data identifies the applicable device and the data is readily available. Use of random data reduces a risk of spoofing.

Obtaining first authentication data may comprise generating, by the implantable medical device, a key based on data provided in the first data message. In such case, the key is comprised by the first authentication data. In this disclosure, a key may be a key as known in the narrow definition in encryption and signing, but also as any data in general to indicate authenticity of data or to certify a particular origin of data. An advantage is that such key may be used on a case by case communication, for example on a per-communication session basis.

The first physical communication channel may have a first signal attenuation factor in a gaseous medium and the second physical

communication channel has a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor. This means that the first communications, with first security data, can only be done if the control device and the implantable medical device are very close together. If the implantable medical device is implanted, this may even require contact between the control device and the implantable medical device. This means that data for verifying the authentication over the second physical communication channel may only be transmitted while being noticed by a person in whom the implantable medical device is implanted, reducing a risk of hacking.

The first physical communication channel may be an ultrasonic communication channel and the second physical communication channel may be an electromagnetic communication channel. Firstly, such communication techniques are well known and have been proven. Second, such communication techniques may also transmit power from the control device to the implantable medical device. This may reduce a risk of depletion of a battery of the implantable medical device by continuously hailing the implantable medical device. The energy provided in the signal carrying the first message may be used for processing data in the implantable medical device.

A second aspect provides, in a control device arranged to control an implantable medical device, a method of communicating with the implantable medical device. The method comprises sending a first data message to the implantable medical device over a first physical communication channel, obtaining first authentication data based on data provided in the first data message, generating second data message, authenticating the second data message using the first authentication data and sending the authenticated second data message to the implantable medical device over a second physical communication channel, the second

physical communication channel being different from the first physical communication channel.

By requiring the control device to use the first authentication data received over the first physical communication channel for communication on the second physical communication channel, security is improved, as two types of channels are required. Different physical communication channels are, in the context of this disclosure, to be understood as relying on different physical principles, like mechanical vibrations versus electromagnetic waves.

The method may further comprise receiving, from the implantable medical device, over the first physical communication channel, a third message, the third message comprising second authentication data, wherein the first authentication data may further be based on the second authentication data. In this case, security is further improved by requiring the control device to use also data from the implantable medical device for generating or otherwise obtaining the first authentication data.

The second authentication data may comprise at least one of a medical device identifier identifying the implantable medical device and random medical device data. Use of randomised data may reduce a risk of spoofing and the medical device identifier is readily available data.

The first data message may comprise at least one of a control identifier identifying the control device and random control data; and the first authentication data may further be based on at least one of the control identifier and the random control data. Use of randomised data may reduce a risk of spoofing and the medical device identifier is readily available data.

A third aspect provides an implantable medical device arranged for communicating with a control device. The implantable medical device comprises a first transceiver arranged to receive, via a first physical communication channel, a first message from a control device, a second transceiver arranged to receive, via a second physical communication

channel, a second message and a processing unit. The processing unit is arranged to activate, upon receiving the first message, the second physical communication channel, by activating the second transceiver, obtain first authentication data of the control device, based on data provided in the first data message, verify whether the second message originates from the control device, based on the obtained first authentication data and deactivate the second physical communication channel at the side of the implantable medical device if a result of the verifying is that the second message does not originate from the control device.

A fourth aspect provides a control device arranged to control an implantable medical device. The control device comprises a first transceiver arranged to send, via a first physical communication channel, a first data message to the implantable medical device, a second transceiver arranged to send, via a second physical communication channel, a second data message to the implantable medical device, the second physical communication channel being different from the first physical communication channel and a processing unit. The processing unit is arranged to obtain first authentication data based on the first data message, generate the second data message, authenticate the second data message using the first authentication data and send the authenticated second data message to the implantable medical device by means of the second transceiver.

Additionally, it may be preferred to improve the currently available security measures. To that purpose, a fifth aspect provides, in a control device for an implantable medical device, a method of communicating with the implantable medical device. The method comprises sending a first data message to the implantable medical device, via a first physical communication channel, receiving, via the first physical communication channel, from the implantable medical device, a second data message comprising a first key, obtaining, upon receiving the first key, a second key related to the first key. The method further comprises sending a

third data message to the implantable medical device, via a second physical communication channel different from the first physical communication channel, the third data message being authenticated with the second key.

By providing the first key over the first physical communication channel and subsequently verifying communication over the second physical channel with a different but related key, two keys are used, of which the second key has not been available over any communication channel. Hence, the second key cannot be obtained using eavesdropping.

Furthermore, this may allow for use of short-term second keys, based on a long-term first key. This may improve efficiency.

This method allows for secure coupling of the control device with the implantable medical device. A first connection is made using a first physical communication channel, for example ultrasound and via that connection, first security data is provided. The security data may be used to enable the control device to authenticate particular data sent to the implantable medical device. For the avoidance of doubt, to authenticate, within the context of this disclosure, is an equivalent of to certify, meaning to modify a message, by modifying data or by appending particular data, such that an origin of data may be verified, based on any action performed by an authentication step. Such action may be signing, encrypting, adding a certificate, other, or a combination thereof.

The data to be certified is certified and received by the implantable medical device. This enables the implantable medical device to verify that the message is received from the control device. This message, with the authenticated data to be verified, is sent via another physical communication channel. This allows for use of a further physical communication channel that may be, in physical nature, less secure as the ranger is wider, after more crucial and more basic security data has been exchanged over for example a physical communication channel that has a shorter range. The communication over the potentially less secure physical

communication channel is at higher layers secured by, for example, cryptography, signing, certification, other means of authenticating data or a combination thereof. This allows for improved security and for flexibility of use of communication channels.

In this disclosure, a key may be a key as known in the narrow definition in encryption and signing, but also as any data in general to indicate authenticity of data or to certify a particular origin of data. An advantage is that such key may be used on a case by case communication, for example on a per-communication session basis.

Preferably, both the first physical communication channel and the second physical communication channel are two-way communication channels. As such, both the control device and the implantable medical device comprise transceivers for both the first physical communication channel and the second physical communication channel, rather than only a receiver or a transmitter, respectively.

The first physical communication channel may have a first signal attenuation factor in a gaseous medium and the second physical communication channel has a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor. This means that the first communications, with first security data, can only be done if the control device and the implantable medical device are very close together. If the implantable medical device is implanted, this may even require contact between the control device and the implantable medical device. This means that data for verifying the authentication over the second physical communication channel may only be transmitted while being noticed by a person in whom the implantable medical device is implanted, reducing a risk of hacking.

The first physical communication channel may be an ultrasonic communication channel and the second physical communication channel may be an electromagnetic communication channel. Firstly, such

communication techniques are well known and have been proven. Second, such communication techniques may also transmit power from the control device to the implantable medical device. This may reduce a risk of depletion of a battery of the implantable medical device by continuously hailing the implantable medical device. The energy provided in the signal carrying the first message may be used for processing data in the implantable medical device.

At least one of the first data message may comprise a first payload and the second message may comprise a second payload and the third data message may be based on at least one of the first payload and the second payload. This may allow for symmetrical key generation, in which a generated key is based on data from the implantable medical device, as well as data from the control device, because data for generating keys is available at both side of the communication, in particular if the second key is generated based on at least one of the first payload and the second payload.

At least one of the payload and the second payload comprises random data; this may reduce the risk of spoofing.

The first message may comprise a control identifier related to the control device, the second message may comprise a medical device identifier related to the implantable medical device; and the second key may be generated further based on at least one of the control identifier and the medical device identifier. As such, an additional advantage is provided that readily available data is used, based on unique identifiers on both sides of the communication.

A sixth aspect provides, in an implantable medical device, a method of communicating with a control device. The method comprises receiving, via a first physical communication channel, a first message from the control device, sending, via the first physical communication channel, upon receiving the first message, a second message to the control device, the

second message comprising a first key and obtaining a second key related to the first key. The method further comprises receiving a third message from the control device via a second physical communication channel different from the first physical communication channel; and verifying whether the third message has been authenticated with the second key.

By requiring the control device to use the first authentication data received over the first physical communication channel for communication on the second physical communication channel, security is improved, as two types of channels are required. Different physical communication channels are, in the context of this disclosure, to be understood as relying on different physical principles, like mechanical vibrations versus electromagnetic waves.

At least one of the first data message may comprise a first payload and the second message may comprise a second payload and the third data message may be based on at least one of the first payload and the second payload. This may allow for symmetrical key generation, in which a generated key is based on data from the implantable medical device, as well as data from the control device, because data for generating keys is available at both side of the communication, in particular if the second key is generated based on at least one of the first payload and the second payload.

At least one of the payload and the second payload may comprise random data. This may reduce a risk of spoofing.

The first message may comprise a control identifier related to the control device, the second message may comprise a medical device identifier related to the implantable medical device; and the second key may be generated further based on at least one of the control identifier and the medical device identifier. As such, an additional advantage is provided that readily available data is used, based on unique identifiers on both sides of the communication.

The first physical communication channel may have a first signal attenuation factor in a gaseous medium and the second physical communication channel may have a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor.

This means that the first communications, with first security data, can only be done if the control device and the implantable medical device are very close together. If the implantable medical device is implanted, this may even require contact between the control device and the implantable medical device. This means that data for verifying the authentication over the second physical communication channel may only be transmitted while being noticed by a person in whom the implantable medical device is implanted, reducing a risk of hacking.

The first physical communication channel may be an ultrasonic communication channel and the second physical communication channel may be an electromagnetic communication channel.

Firstly, such communication techniques are well known and have been proven. Second, such communication techniques may also transmit power from the control device to the implantable medical device. This may reduce a risk of depletion of a battery of the implantable medical device by continuously hailing the implantable medical device. The energy provided in the signal carrying the first message may be used for processing data in the implantable medical device.

The method may further comprise, if the verifying fails, deactivating the second physical communication channel. By shutting down the second physical communication channel upon any verification error, improved security is provided and any further energy consumption is prevented, reducing risks of battery depletion attacks on the implantable medical device.

A seventh aspect provides a control device for an implantable medical device. The control device comprises a first transceiver arranged to send a first data message to the implantable medical device, via a first physical communication channel and receive, via the first physical communication channel, from the implantable medical device, a second data message comprising a first key. The device further comprises a processing unit arranged to generate, upon receiving the first key and based on the first key, a second key and authenticate a third data message with the second key. The device also comprises a second transceiver arranged to send the third data message to the implantable medical device, via a second physical communication channel different from the first physical communication channel.

A eighth aspect provides an implantable medical device. The device comprises a first transceiver arranged to receive, via a first physical communication channel, a first message from a control device and send, via the first physical communication channel, upon receiving the first message, a second message to the control device, the second message comprising a first key. The device further comprises a processing unit arranged to generate, upon receiving the first key and based on the first key, a second key. The device also comprises a second transceiver arranged to receive a third message from the control device via a second physical communication channel different from the first physical communication channel. In this device, the processing unit is further arranged to verify whether the third message has been authenticated with the second key.

BRIEF DESCRIPTION OF THE DRAWINGS

The various aspects and variations thereof will now be elucidated in further detail in conjunction with drawings. In the drawings:

Figure 1 A: shows an implantable medical device;

Figure 1 B: shows a control device;

Figure 2 A: shows a first part of a flowchart; and

Figure 2 B: shows a second part of a flowchart.

DETAILED DESCRIPTION

Figure 1 A shows an implantable medical device 100. The implantable medical device 100 comprises a central processing unit 102, coupled to a memory module 104 as a data storage unit and to a communication processor 106. The memory module 104 may be volatile or non-volatile, magnetic, electronic, other, or a combination thereof. The memory module 104 is arranged to store data acquired by the implantable medical device 100, for example related to a body in which the implantable medical device 100 may be implanted.

Furthermore, the memory module 104 is arranged to store code readable and executable by the central processing unit 102, the communication processor 106 and other parts of the implantable medical device 100. With such code, the various part of the implantable medical device 100 may be programmed to execute methods described above and below.

The central processing unit 102 is further coupled to a sensor module 108 and an actuator module 110. The sensor module 108 may be an electrical sensor, capable of measuring at least one of voltages, currents and electrical power, a magnetic sensor, a mechanic sensor capable of measuring motion, acceleration, force, stress, other or a combination thereof. The actuator module 110 may be an electrical, mechanical, magnetic or other type of sensor or combination thereof. For example, the actuator module 110 may provide electrical pulses - currents, voltages or both - to muscles of a body, like a heart.

As shown by Figure 1A, the communication processor 106 is programmed, either hardwired or softwired by means of code, to comprise a random number unit 122 arranged to generate random numbers, a key

generation unit 124 arranged to generate a key, an authentication unit 126 arranged to authenticate data, using for example a key and a verification unit 128 to verify an authentication for particular data.

A key may be understood as any type of data object that may be used to authenticate data and to verify the authentication. Authentication may be any type of process to generate a data object, in conjunction with a key, which generated data may be used to verify an origin of the data to be authenticated. Authentication may be executed by means of signing, encrypting, hashing, compressing, other, or a combination thereof. Verification of data may be executed using data identical or similar to data used for authentication or other data, to verify that the authentication to be verified matches with a verification data object, like a key.

The communication processor 106 is connected to an RF module 112 as an RF transceiver that is in turn connected to an antenna 114. The RF module 112 is arranged to modulate a radio frequency electromagnetic signal with data provided by the communication processor 106. Furthermore, the RF module is arranged to demodulate a radio frequency electromagnetic signal received by means of the antenna 114 to obtain data. Radio frequency may be between 100 kHz and 10 GHz; preferably, standardised spectra for near-field radio frequency data communication are used.

The communication processor 106 is further connected to an acoustic driver 116 as an ultrasonic transceiver that is in turn connected to an ultrasonic transducer 118. The acoustic driver 116 is arranged to modulate an ultrasonic signal with data provided by the communication processor and provide the modulated signal to the ultrasonic transducer 108 for generating a modulated acoustic signal. Furthermore, the acoustic driver 116 is arranged to demodulate an ultrasonic signal received by means of the ultrasonic transducer 118 to obtain data. Ultrasonic sound may be defined

as sound - mechanical vibrations - having a frequency of at least 20 kHz, in particular at least 500 MHz, at least 1 MHz or at least 2 MHz.

Figure 1 B shows a control device 150 arranged to control the implantable medical device 100. The control device 150 comprise a central processing unit 152, coupled to a memory module 154 as a data storage unit and to a communication processor 156. The memory module 154 may be volatile or non-volatile, magnetic, electronic, other, or a combination thereof. The memory module 154 is arranged to store data acquired by the implantable medical device 100, for example related to a body in which the implantable medical device 100 may be implanted.

Furthermore, the memory module 154 is arranged to store code readable and executable by the central processing unit 152, the communication processor 156 and other parts of the control device 150. With such code, the various part of the control device 150 may be programmed to execute methods described above and below.

The central processing unit 152 is further coupled to an input module 158 and an output module 160. The input module 158 may be a keyboard, a touchscreen, a mouse, a data network connector, a microphone, a touchpad, other or a combination thereof. The output module 160 may be an electronic display screen, a touchscreen, a speaker, a data network connector, an array of light sources, other, or combination thereof.

As shown by Figure 1 B, the communication processor 156 is programmed, either hardwired or softwired by means of code, to comprise a random number unit 172 arranged to generate random numbers, a key generation unit 174 arranged to generate a key, an authentication unit 176 arranged to authenticate data, using for example a key and a verification unit 178 to verify an authentication for particular data. A key may be understood as any type of data object that may be used to authenticate data.

Authentication may be any type of process to generate a data object, in conjunction with a key. Authentication may be executed by means

of signing, encrypting, hashing, compressing, other, or a combination thereof. Verification of data may be executed using data identical or similar to data used for authentication or other data, to verify that the authentication to be verified matches with a verification data object, like a key.

The communication processor 156 is connected to an RF module 162 as an RF transceiver that is in turn connected to an antenna 164. The RF module 162 is arranged to modulate a radio frequency electromagnetic signal with data provided by the communication processor 156. Furthermore, the RF module is arranged to demodulate a radio frequency electromagnetic signal received by means of the antenna 164 to obtain data. Radio frequency may be between 100 kHz and 10 GHz; preferably, standardised spectra for near-field radio frequency data communication are used.

The communication processor 156 is further connected to an acoustic driver 166 as an ultrasonic transceiver that is in turn connected to an ultrasonic transducer 168. The acoustic driver 166 is arranged to modulate an ultrasonic signal with data provided by the communication processor and provide the modulated signal to the ultrasonic transducer 158 for generating a modulated acoustic signal. Furthermore, the acoustic driver 166 is arranged to demodulate an ultrasonic signal received by means of the ultrasonic transducer 168 to obtain data. Ultrasonic sound may be defined as sound - mechanical vibrations - having a frequency of at least 20 kHz, in particular at least 500 MHz, at least 1 MHz or at least 2 MHz.

The various components of the two devices described above may be integrated in one or more semiconductor dies, provided with one or more discrete components, other, or a combination thereof. The various components may be powered by means of an internal or external battery.

The implantable medical device 100 may be controlled by means of the control device. A first flowchart 200 shown by Figure 2 A and a second

flowchart 200' shown by Figure 2 B show a procedure for communication between the implantable medical device 100 and the control device 150. Parts shown at the left may be executed by the control device 150 and parts on the right may be executed by the implantable medical device 100, unless indicated otherwise. Below, a list is provided with brief summaries of the parts of the first flowchart 200 and the second flowchart 200'.

202	start procedure
204	create control nonce
206	create control message
208	send message to medical device over acoustic
210	receive message over acoustic
212	create IMD nonce
214	obtain long term key
216	create IMD message
218	send IMD message over acoustic
220	receive IMD message over acoustic
222	get key
224	get nonces and identifiers
226	generate short-term key
228	activate RF
230	generate message
232	authenticate message with short term key
234	send message over RF
236	receive message over RF
238	verify authentication of message
240	verified?
242	generate message
244	authenticate message with short term key
246	send message over RF

248 receive message over RF
250 verify authentication of message
252 verified?
254 communicate between devices
256 communication ended
258 sleep
260 generate nonce
262 send continuation message over RF
264 receive continuation message over RF
266 wake up
268 generate nonce
270 send continuation confirmation over RF
272 receive continuation confirmation over RF
274 generate short term key
276 generate message
278 authenticate message
280 send continuation verification
282 receive continuation verification
284 verify continuation verification
286 verified?
288 send continuation verification return
290 receive continuation verification return
292 verify continuation verification return
294 verified?
296 deactivate RF
298 end

The procedure starts in a terminator 202 and continues to step 204, in which the random number unit 172 of the control device 150 generates a control nonce as a random number. In step 206, a control

message is generated, comprising the nonce and an identifier of the control device 150. In step 208, the control message is sent by the control device 150 by means of the acoustic driver 166 and the ultrasonic transducer 168.

In step 210, the implantable medical device 100 receives the ultrasonic signal with the control message by means of the ultrasonic transducer 118 and the acoustic driver 116 of the implantable medical device 100. The demodulated data is provided to the communication processor 106 of the implantable medical device 100.

The energy in the signal received by means of the ultrasonic transducer 118 and the acoustic driver 116 may be stored in a battery or other energy storage module of the implantable medical device 100 and used for communication or other data processing by the implantable medical device.

Upon receiving the data in the control message, the communication processor 106 of the implantable medical device 100 and the random number unit 122 thereof creates a medical device nonce as a random number in step 212. In step 214, the communication processor 106 obtains a long-term key. The long-term key may be obtained from the memory module 106, may be generated by the central processing unit 102, may be generated by the communication processor 106 or may be obtained otherwise.

In step 216, a medical device message is generated comprising the medical device nonce, an identifier of the implantable medical device 100 and the obtained long-term key. The message is sent to the control device 150 in step 218, using the acoustic driver 116 and the ultrasonic transducer 118, analogous to the sending of the control message as discussed above. The medical device message is received by the control device 150 by means of the ultrasonic transducer 168 and the acoustic driver 166 analogous to the receiving of the control message as discussed above in step 220.

The key in the medical device message is obtained by the communication processor 156 of the control device 150 in step 222. In step 224, the key generation unit 174 of the control device 150 obtains at least one of the received long-term key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100 and generates based thereon a short-term key in step 226 in accordance with a particular algorithm, which may be pre-determined.

Likewise, in step 224', the key generation unit 124 of the implantable medical device 100 obtains at least one of the received key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 150 and generates based thereon a short-term key in step 226' in accordance with a particular algorithm, which may be pre-determined and which may be the same as used in step 226. Hence, the key generated in step 226 may be the same as the key generated in step 226'. In step 228, the implantable medical device 100 activates the RF module 112 and opens a communication channel at a radio frequency.

Subsequently, the communication processor 256 of the control device 150 generates in step 230a data object which may be based on at least one of the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100, other, or a combination thereof. In step 232, the authentication unit 126 authenticates the data object thus generated. The authenticated data object is sent as a message to the implantable medical device 100 by means of the RF module 162 and the antenna 164 of the control device 150 in step 234.

The message thus sent in step 236 is received by the implantable medical device 100 by means of its antenna 114, its RF module 112 and its communication processor 106. In step 238, the verification unit 128 of the implantable medical device 100 verifies whether the data received is

authenticated with an appropriate key. The energy in the RF signal received may be used for this processing or other processing and/or may be stored in a battery or another energy storage module comprised by the implantable medical device.

In step 238, the key generated in step 226' above may be used to this purpose. In step 240, the procedure branches to step 296 if the verification fails, in which step 296 the RF communication channel is closed by the communication processor 106 and the RF module 112 of the implantable medical device 100. Subsequently, the procedure ends in terminator 298.

If the verification in step 238 is successful, the procedure branches in step 240 to step 242 in which a data object is generated by the communication processor 106 of the implantable medical device based on at least one of the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100. In step 244, the authentication unit 176 authenticates the data object thus generated. The authenticated data object is sent as a message to the control device 150 by means of the RF module 112 and the antenna 114 of the implantable medical device 100 in step 246.

The message thus sent is received by the control device 150 by means of its antenna 164, its RF module 162 and its communication processor 156 in step 248. In step 250, the verification unit 178 of the control device 150 verifies whether the data received is authenticated with an appropriate key. In step 250, the key generated in step 226 above may be used to this purpose. In step 252, the procedure branches to step 296 if the verification fails, in which step 296 the RF communication channel is closed by the communication processor 156 and the RF module 162 of the control device 150. Subsequently, the procedure ends in terminator 298.

If the verification in step 250 is successful, the procedure branches in step 252 to step 254 and step 254' in which the control device

150 and the implantable medical device 100 exchange data. Generally, the control device 150 will provide instruction to the implantable medical device 100 how the central processing unit 102 is to control the actuator module. Additionally, or alternatively, instructions may be provided to provide the control device 150 with data acquired by means of the sensor module 108 and/or to acquire data using the sensor module 108.

In this regular data exchange as well , the messages may be encrypted in the form of "Authenticated Encryption", in which both Encryption and Message Authentication Code (MAC) may be used in order to provide data confidentiality and authentication, respectively, for example, the standardized Galois Counter Mode (GCM) block-cipher mode of operation, Encrypt-then-MAC (EtM), other, or a combination thereof. A MAC code of every message sent during regular-data-exchange may be verified as discussed in conjunction with step 250. If any such verification check fails, the process branches to step 296 as well and the RF module 162 will be switched off. Additionally, or alternatively, an established pairing between the implantable medical device 100 and the control device may be reset.

During communication, both in step 256 and step 256', the control device 150 and the implantable medical device check whether the communication continues or has ended. The communication may be ended explicitly, by means of a termination instruction or implicitly, by not sending any data anymore. Upon any end of the communication, the procedure enters in waiting step 258. In the waiting step 258, both devices may be in a low-power state or sleeping state.

In step 260, the control device 150 is activated, for example following user input as discussed above. Following activation, with an instruction to be sent to the implantable medical device 100, a nonce is generated by the random number unit 172, which may be based on an instruction of the central processing unit 152. In step 262, the nonce thus

generated is sent by the control device 150 as discussed above, via the RF module 162. The identifier of the control device 150 may be sent along, as well as a specific instruction to resume communication.

The data thus sent in step 262, is received in step 264 as a continuation message by means of the RF module 112 of the implantable medical device 100. In step 266, the implantable medical device 100 wakes up as a result of receiving the message. Energy in the received signal may be used for the waking up. In step 268, the random number unit 122 generates a nonce and in step 270, the nonce is sent to the control unit 150, which may be accompanied by an identifier of the implantable medical device 100. The data message thus generated and sent is received by the control device 150 in step 272.

In step 274, the key generation unit 172 of the control device 150 generates a short-term key, based on at least the long-term key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100. Next, the communication processor 156 generates a data object based on at least one of the short-term key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100 in step 276. In step 278, the authentication unit 176 authenticates the data object thus generated.

Likewise, in step 274', the key generation unit 122 of the implantable medical device 100 generated a short-term key, based on at least the long-term key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100. Next, the communication processor 106 generates a data object based on at least one of the short-term key, the control nonce, the medical device nonce, the identifier of the control device 150 and the identifier of the implantable medical device 100 in step 276'. In step 278', the authentication unit 126 authenticates the data object thus generated.

In step 280, the authenticated data object generated by the communication processor 156 of the control device as discussed above is sent to the implantable medical device 150 by means of the RF module 112 as a continuation confirmation message. The continuation confirmation message is received by the RF module 112 of the implantable medical device 100 in step 282 and the authentication is verified in step 284. The verification may be executed using the key generated in step 274. If the verification fails, the procedure branches to step 296 as discussed above. Additionally, the control device 150 may be unpaired with the implantable medical device 100, which means that for further contact between the two devices, the pairing using ultrasonic data communication may have to be executed again, as discussed above.

If the verification in step 284 is successful, the procedure continues to step 288 via branch 286, in which the data object generated in step 276' and authenticated in step 278' is sent to the control device as a continuation verification return message, via the RF module 112 and the communication processor 106. The continuation verification return message thus sent is received by the control device in step 290, by means of the RF module 162.

In step 292, the authentication of the continuation verification return message is verified in step 292, which may be executed by means of the key generated in step 274' discussed above. If the verification fails, the procedure branches to step 296 as discussed above via step 294. Additionally, the control device 150 may be unpaired with the implantable medical device 100, which means that for further contact between the two devices, the pairing using ultrasonic data communication may have to be executed again. If the verification is successful, the procedure branches back to step 254 and step 254', in which communication is resumed as discussed above.

The various aspects and variations thereof relate to the following numbered implementations:

Claims

1. In an implantable medical device, a method of communicating with a control device, the method comprising:

receiving a first data message from the control device via a first physical communication channel;

upon receiving the first message, activating a second physical communication channel different from the first physical communication channel;

obtaining first authentication data of the control device, based on data provided in the first data message;

receiving, via the second physical communication channel, a second message; and

verifying whether the second message originates from the control device, based on the obtained first authentication data.

2. The method according to claim 1, further comprising deactivating the second physical communication channel at the side of the implantable medical device if a result of the verifying is that the second message does not originate from the control device

3. The method according to any of the preceding claims, further comprising sending, upon receiving the first message, via the first physical communication channel, a third message to the control device, the third message comprising second authentication data;

wherein the first authentication data is further based on the second authentication data.

4. The method according to claim 3, wherein the second authentication data comprises at least one of a medical device

identifier identifying the implantable medical device and random medical device data.

5. The method according to any of the preceding claims, wherein:
the first data message comprises at least one of a control identifier identifying the control device and random control data; and
the first authentication data is further based on at least one of the control identifier and the random control data.

6. Method according to any of the preceding claims, wherein obtaining first authentication data comprises generating, by the implantable medical device, a key based on data provided in the first data message.

7. Method according to any of the preceding claims, wherein the verifying comprises at least one of verifying a signature of the second message and subjecting at least part of the second message to a decryption operation.

8. The method according to any of the preceding claims, wherein the first physical communication channel has a first signal attenuation factor in a gaseous medium and the second physical communication channel has a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor.

9. The method of any one of the preceding claims, wherein the first physical communication channel is an ultrasonic communication channel and the second physical communication channel is an electromagnetic communication channel.

10. The method according to claim 9, wherein the ultrasonic communication channel has a frequency higher than 500 kHz, preferably higher than 1 MHz.

11. The method according to claim 9 or claim 10, wherein the electromagnetic communication channel has a frequency between 100 kHz and 10 GHz.

12. In a control device arranged to control an implantable medical device, a method of communicating with the implantable medical device, the method comprising:

sending a first data message to the implantable medical device over a first physical communication channel;

obtaining first authentication data based on data provided in the first data message;

generating second data message;

authenticating the second data message using the first authentication data;

sending the authenticated second data message to the implantable medical device over a second physical communication channel, the second physical communication channel being different from the first physical communication channel.

13. The method according to claim 12, further comprising receiving, from the implantable medical device, over the first physical communication channel, a third message, the third message comprising second authentication data;

wherein the first authentication data is further based on the second authentication data.

14. The method according to claim 13, wherein the second authentication data comprises at least one of a medical device

identifier identifying the implantable medical device and random medical device data.

15. The method according to any of claims 12 to 14, wherein:
the first data message comprises at least one of a control identifier identifying the control device and random control data; and
the first authentication data is further based on at least one of the control identifier and the random control data.

16. Method according to any one of the claims 12 to 15, wherein obtaining first authentication data comprises generating, by the control device, a key based on data provided in the first data message.

17. Method according to any of the claims 12 to 16, wherein the authenticating comprises at least one of adding signature to the second message and subjecting at least part of the second message to an encryption operation.

18. The method according to any of the claims 10 to 17, wherein the first physical communication channel has a first signal attenuation factor in a gaseous medium and the second physical communication channel has a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor.

19. The method of any one of the claims 12 to 18, wherein the first physical communication channel is an ultrasonic communication channel and the second physical communication channel is an electromagnetic communication channel.

20. The method according to claim 19, wherein the ultrasonic communication channel has a frequency higher than 500 kHz, preferably higher than 1 MHz.

21. The method according to claim 19 or claim 20, wherein the electromagnetic communication channel has a frequency between 100 kHz and 10 GHz.

22. An implantable medical device arranged for communicating with a control device, the implantable medical device comprising:
a first transceiver arranged to receive, via a first physical communication channel, a first message from a control device;
a second transceiver arranged to receive, via a second physical communication channel, a second message;
a processing unit arranged to:
activate, upon receiving the first message, the second physical communication channel, by activating the second transceiver;
obtain first authentication data of the control device, based on data provided in the first data message;
verify whether the second message originates from the control device, based on the obtained first authentication data;
deactivate the second physical communication channel at the side of the implantable medical device if a result of the verifying is that the second message does not originate from the control device.

23. A control device arranged to control an implantable medical device, the control device comprising
a first transceiver arranged to send, via a first physical communication channel, a first data message to the implantable medical device;

a second transceiver arranged to send, via a second physical communication channel, a second data message to the implantable medical device, the second physical communication channel being different from the first physical communication channel;

a processing unit arranged to:

obtain first authentication data based on the first data message;

generate the second data message;

authenticate the second data message using the first authentication data; and

send the authenticated second data message to the implantable medical device by means of the second transceiver.

24. In a control device for an implantable medical device, a method of communicating with the implantable medical device, the method comprising:

sending a first data message to the implantable medical device, via a first physical communication channel;

receiving, via the first physical communication channel, from the implantable medical device, a second data message comprising a first key;

obtaining, upon receiving the first key, a second key related to the first key;

sending a third data message to the implantable medical device, via a second physical communication channel different from the first physical communication channel, the third data message being authenticated with the second key.

25. The method according to claim 24, wherein the first physical communication channel has a first signal attenuation factor in a gaseous medium and the second physical communication channel has a second signal attenuation factor in the gaseous medium, the

first signal attenuation factor being higher than the second signal attenuation factor.

26. The method of any one of the claims 24 to 25, wherein the first physical communication channel is an ultrasonic communication channel and the second physical communication channel is an electromagnetic communication channel.

27. The method according to claim 26, wherein the ultrasonic communication channel has a frequency higher than 500 kHz, preferably higher than 1 MHz.

28. The method according to claim 26 or claim 27, wherein the electromagnetic communication channel has a frequency between 100 kHz and 10 GHz.

29. The method according to any one of the preceding claims 24 to 28, wherein:

at least one of the first data message comprises a first payload and the second message comprises a second payload; and

the third data message is based on at least one of the first payload and the second payload.

30. The method according to claim 29, wherein the second key is generated based on at least one of the first payload and the second payload.

31. The method according to any one of claims 29 and 30, wherein at least one of the payload and the second payload comprises random data.

32. The method according to any of the claims 24 to 31, wherein:
the first message comprises a control identifier related to the control device;
the second message comprises a medical device identifier related to the implantable medical device; and
the second key is generated further based on at least one of the control identifier and the medical device identifier.

33. The method according to any one of the claims 24 to 32, wherein the authenticating is performed by at least one of signing and encrypting.

34. In an implantable medical device, a method of communicating with a control device, the method comprising:
receiving, via a first physical communication channel, a first message from the control device;
sending, via the first physical communication channel, upon receiving the first message, a second message to the control device, the second message comprising a first key;
obtaining a second key related to the first key;
receiving a third message from the control device via a second physical communication channel different from the first physical communication channel; and
verifying whether the third message has been authenticated with the second key.

35. The method according to claim 34, wherein:
at least one of the first data message comprises a first payload and the second message comprises a second payload; and
the third data message is based on at least one of the first payload and the second payload.

36. The method according to claim 35, wherein the second key is generated based on at least one of the first payload and the second payload.

37. The method according to any one of claims 35 and 36, wherein at least one of the payload and the second payload comprises random data.

38. The method according to any of the claims 34 to 37, wherein:
the first message comprises a control identifier related to the control device;
the second message comprises a medical device identifier related to the implantable medical device; and
the second key is generated further based on at least one of the control identifier and the medical device identifier.

39. The method according to any one of the claims 34 to 38, wherein the authenticating is performed by at least one of signing and encrypting.

40. The method according to any one of the claims 34 to 39, wherein the first physical communication channel has a first signal attenuation factor in a gaseous medium and the second physical communication channel has a second signal attenuation factor in the gaseous medium, the first signal attenuation factor being higher than the second signal attenuation factor.

41. The method of any one of the claims 34 and to 40, wherein the first physical communication channel is an ultrasonic communication channel and the second physical communication channel is an electromagnetic communication channel.

42. The method according to claim 41, wherein the ultrasonic communication channel has a frequency higher than 500 kHz, preferably higher than 1 MHz.

43. The method according to claim 41 or claim 42, wherein the electromagnetic communication channel has a frequency between 100 kHz and 10 GHz.

44. The method according to any of the claim 34 to 43, further comprising, if the verifying fails, deactivating the second physical communication channel.

45. A control device for an implantable medical device, the control device comprising:
a first transceiver arranged to:
send a first data message to the implantable medical device, via a first physical communication channel and
receive, via the first physical communication channel, from the implantable medical device, a second data message comprising a first key;
a processing unit arranged to:
generate, upon receiving the first key and based on the first key, a second key; and
authenticate a third data message with the second key;
a second transceiver arranged to send the third data message to the implantable medical device, via a second physical communication channel different from the first physical communication channel.

46. An implantable medical device comprising:
a first transceiver arranged to:

receive, via a first physical communication channel, a first message from a control device;

send, via the first physical communication channel, upon receiving the first message, a second message to the control device, the second message comprising a first key;

a processing unit arranged to generate, upon receiving the first key and based on the first key, a second key;

a second transceiver arranged to receive a third message from the control device via a second physical communication channel different from the first physical communication channel; and

wherein the processing unit is further arranged to verify whether the third message has been authenticated with the second key.

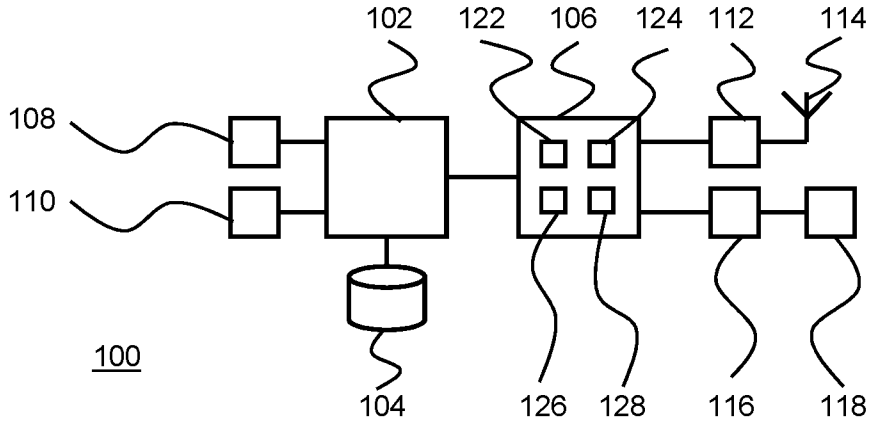

102
122
106
124
112
114
108
110
100
104
126
128
116
118

Fig. 1 A

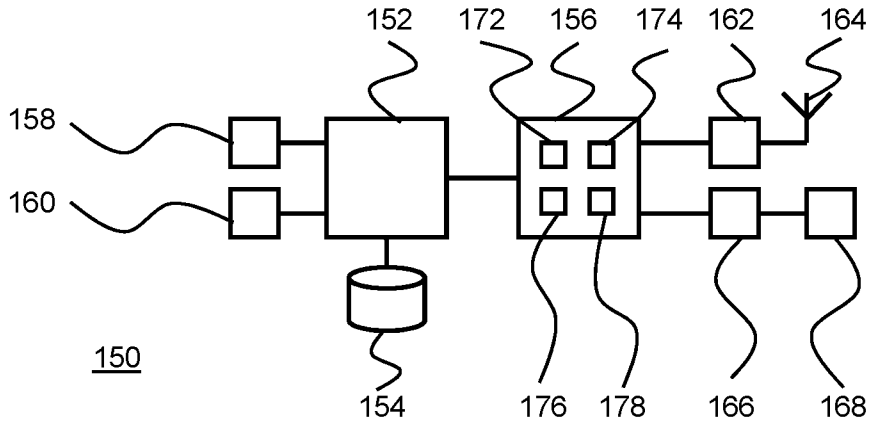

152
172
156
174
162
164
158
160
150
154
176
178
166
168

Fig. 1 B

Fig 2 A

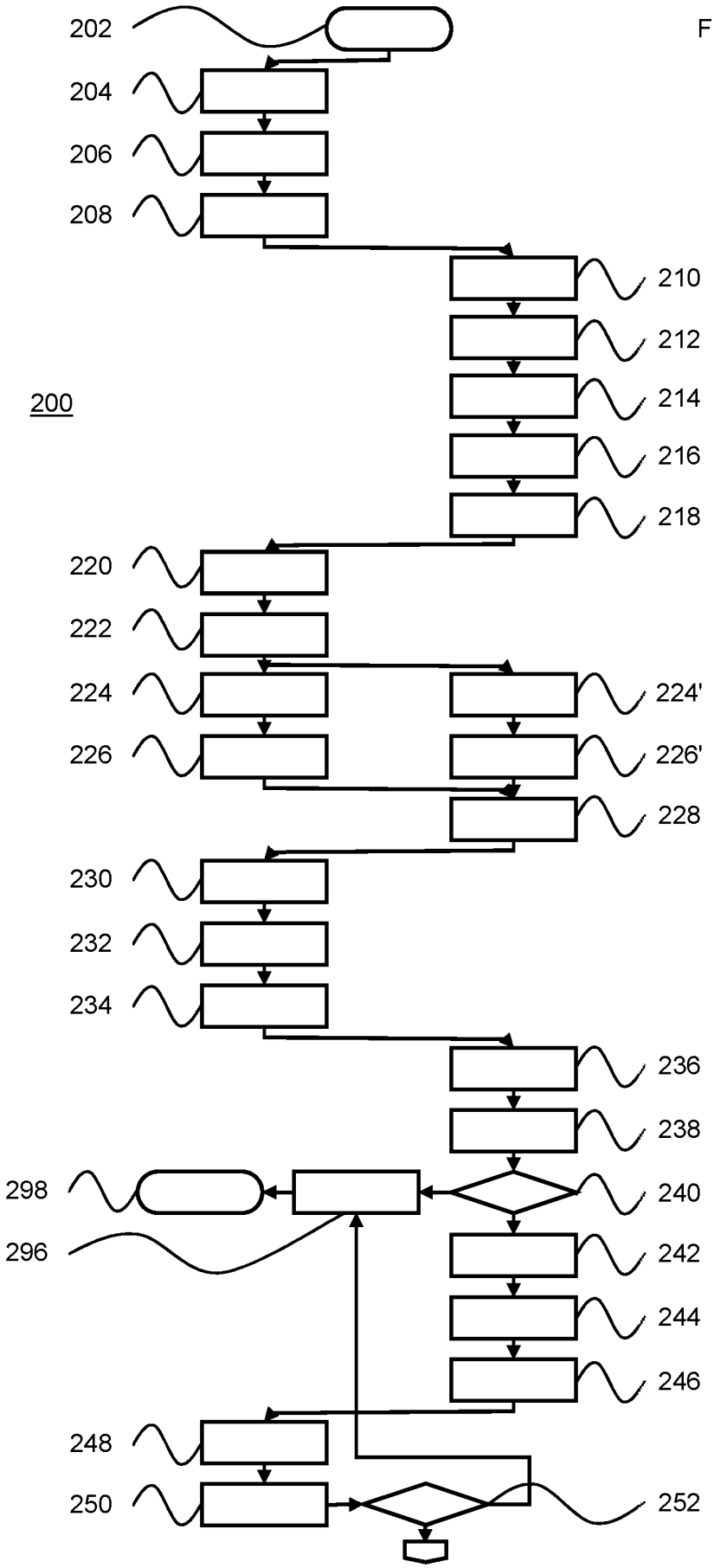
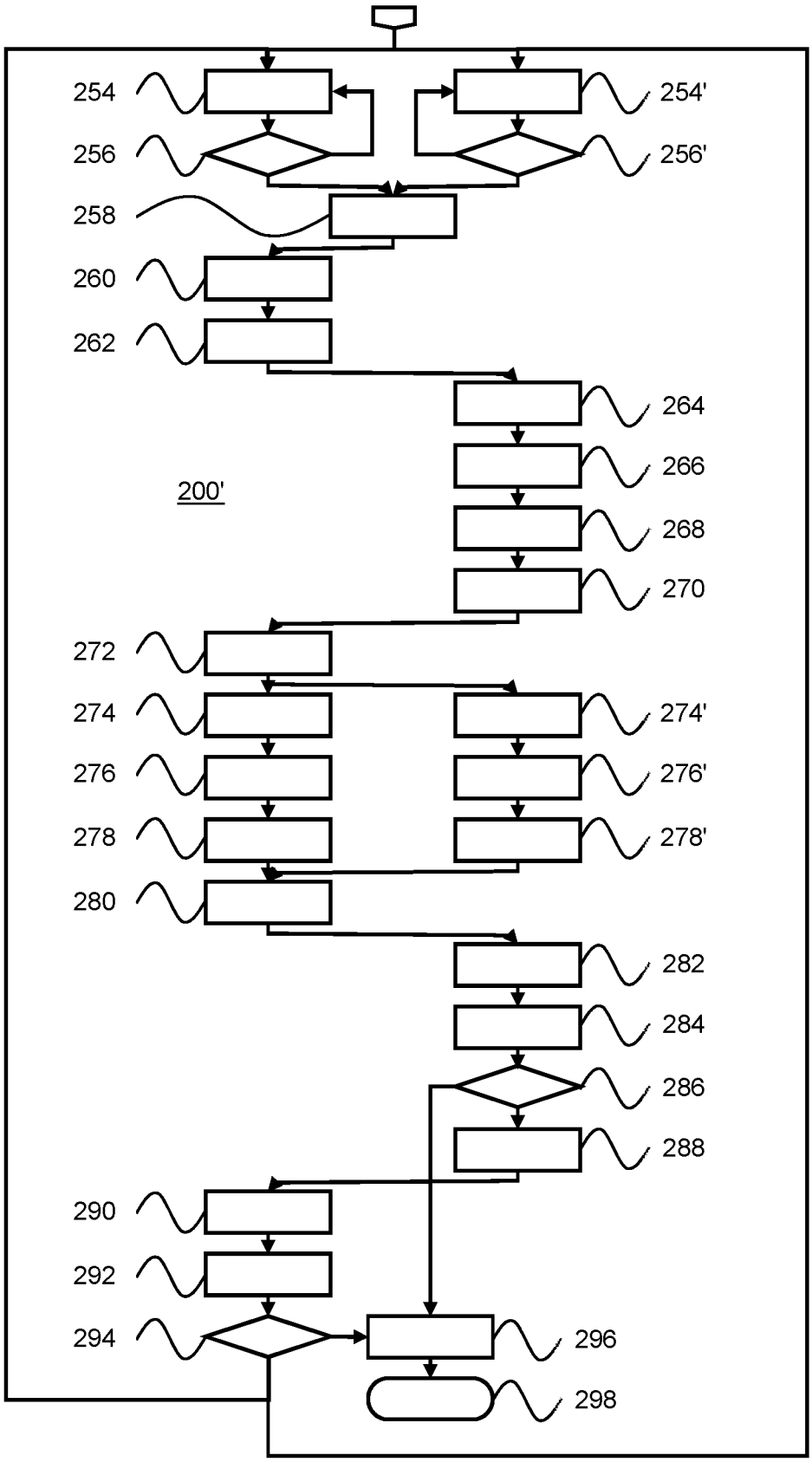

202
204
206
208
210
212
200
214
216
218
220
222
224
224'
226
226'
228
230
232
234
236
238
298
240
296
242
244
246
248
250
252

Fig 2 B


254
254'
256
256'
258
260
262
264
266
200'
268
270
272
274
274'
276
276'
278
278'
280
282
284
286
288
290
292
294
296
298

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2022/050273

A. CLASSIFICATION OF SUBJECT MATTER
INV. A61N1/36 A61N1/372 H04L9/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
A61N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/266221 A1 (CASTELLUCCIA CLAUDE [FR] ET AL) 18 October 2012 (2012-10-18)	24,25, 28, 32-34, 38-40, 43-46
Y	paragraphs [0014] - [0055], [0061] - [0064], [0075] - [0081]; figures 1-2; table 1	27, 29-31, 35-37,42
A		1-23,26, 41
A	US 2019/201702 A1 (MI BIN [US] ET AL) 4 July 2019 (2019-07-04) paragraphs [0018] - [0054], [0073] - [0076]; figures 1-5, 9	1-23

-/--

[x] Further documents are listed in the continuation of Box C.

[x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2022	08/11/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Lahorte, Philippe

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2020/101301 A1 (PALTI YORAM [IL]) 2 April 2020 (2020-04-02) paragraphs [0034] - [0068], [0099] - [0100]; figures 3-4	27,42 1-23
A	US 2004/260363 A1 (ARX JEFFREY A VON [US] ET AL) 23 December 2004 (2004-12-23) paragraphs [0010] - [0039]; figures 1-2	1-46
Y	US 2015/341785 A1 (YOUNG CHAO-WEN [US] ET AL) 26 November 2015 (2015-11-26) paragraphs [0015] - [0020], [0044] - [0056]; figures 1-7	29-31, 35-37

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NL2022/050273

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims;; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-23

An implantable medical device and a control device, arranged for communicating with each other, and corresponding communication methods. A contribution to the art seems to reside in the the use of authentication data to perform identity verification of the devices.

---

2. claims: 24-46

An implantable medical device and a control device, arranged for communicating with each other, and corresponding communication methods. A contribution to the art seems to reside in two-way acoustic communication to facilitate selective use of an electromagnetic communication channel.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NL2022/050273

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012266221 A1	18-10-2012	EP 2315465 A1	27-04-2011
		EP 2491736 A1	29-08-2012
		US 2012266221 A1	18-10-2012
		WO 2011047493 A1	28-04-2011
US 2019201702 A1	04-07-2019	US 2019201702 A1	04-07-2019
		US 2021370075 A1	02-12-2021
		WO 2019136233 A1	11-07-2019
US 2020101301 A1	02-04-2020	US 2020101301 A1	02-04-2020
		WO 2018185703 A1	11-10-2018
US 2004260363 A1	23-12-2004	EP 1635907 A1	22-03-2006
		JP 4680187 B2	11-05-2011
		JP 2007524456 A	30-08-2007
		US 2004260363 A1	23-12-2004
		US 2007118188 A1	24-05-2007
		WO 2005000397 A1	06-01-2005
US 2015341785 A1	26-11-2015	NONE	