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

(11) **EP 3 032 845 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
05.02.2020 Bulletin 2020/06

(51) Int Cl.:
H04R 25/00 *(2006.01)*

(21) Application number: **14197819.7**

(22) Date of filing: **12.12.2014**

(54) **Hearing device configured to authenticate a mode request and related method**

Hörgerät mit Authentifizierung einer Anforderung zum Betriebsartwechsel und zugehöriges Verfahren

Dispositif d'aide auditive apte à authentifier une demande de changer un mode de service et procédé associé

(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

(43) Date of publication of application:
15.06.2016 Bulletin 2016/24

(73) Proprietor: **GN Hearing A/S**
2750 Ballerup (DK)

(72) Inventors:
- **Pedersen, Brian Dam**
2750 Ballerup (DK)
- **Vendelbo, Allan Munk**
2750 Ballerup (DK)

(74) Representative: **Aera A/S**
Gammel Kongevej 60, 18th floor
1850 Frederiksberg C (DK)

(56) References cited:
US-A1- 2005 069 161
US-A1- 2007 230 711
US-A1- 2008 165 994
US-A1- 2014 211 972
US-B1- 8 437 860

EP 3 032 845 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present disclosure relates to a hearing device and in particular to hearing device and related method for configuration or operation of a hearing device.

BACKGROUND

[0002] The functionality of a hearing device becomes increasingly advanced. Wireless communication between a hearing device and external devices, such as hearing device fitting apparatus, remote controllers, tablets and smart phones, has evolved. Typically, a wireless communication interface of a hearing device uses open standard-based interface. However, this poses many challenges in terms of security. A hearing device may assume any incoming data as legitimate, and may allow memory to be written or changed by an unauthorized party. Any such attacks may result in a malfunction of the hearing aid, or a battery exhaustion attack.

[0003] US 2005/0069161 relates to a method and apparatus for improving interference suppression processing and control in hearing aids communicating with a mobile station over a short-range wireless network. The hearing aid includes an acoustic echo canceller to suppress acoustic echo from the input audio signals. The mobile station also includes an echo canceller, and may include one or more switching circuits to bypass the echo canceller when the mobile station communicates with the hearing aid via the short-range wireless network.

[0004] US 2008/0165994 relates to a hearing aid device enabled with a Bluetooth transceiver, allowing the user to communicate with linked, Bluetooth enabled mobile radio or telephone. Mobile phone receives a communication, encodes it in accordance with the Bluetooth protocol and links with the transceiver, which is housed with the hearing aid.

[0005] US 2014/0211972 relates to a method of fitting a hearing aid connected to a mobile terminal. The method may include acquiring location information of a location of the mobile terminal, transmitting the location information to a server, receiving, from the server, information about at least one recommended fitting parameter model adapted to hearing conditions of the location and hearing characteristics of a user of the hearing aid, and displaying the information about the at least one recommended fitting parameter model. The method may also include receiving a fitting parameter model selected by the user from among the at least one recommended fitting parameter model, and controlling the hearing aid to function according to the received fitting parameter model.

[0006] US2007/0230711 shows a system of a fitting device and several hearing aids which can be fitted by the fitting device. An identification procedure which is executed before a wireless link is established between the fitting device and the hearing aids makes sure that only a desired hearing aid is fitted.

SUMMARY

[0007] There is a need for a hearing device with reduced risk of a third party accessing any part of the hearing device. In particular there is a need for a hearing device that is protected against unauthorized modification of the hearing device and operation thereof.

[0008] Disclosed is a hearing device comprising a processing unit configured to compensate for hearing loss of a user of the hearing device, a memory, and an interface. The processing unit/hearing device may be configured to receive a mode request via the interface; authenticate the mode request; and place the hearing device into the requested mode if authentication of the mode request succeeds.

[0009] Also disclosed is a method for configuration of a hearing device comprising a processing unit configured to compensate for hearing loss of a user of the hearing device, a memory, and an interface. The method may comprise receiving a mode request via the interface; authenticating the mode request; and placing the hearing device into the requested mode if authentication of the mode request succeeds.

[0010] The method and hearing device as disclosed provide secure configuration of the hearing device, such as secure access to the memory of the hearing device. It is an advantage of the present disclosure that the hearing device can only be configured or updated by authorized parties. The disclosed hearing device thus has the advantage of detecting and preventing any modification by unauthorized parties. The hearing device disclosed herein is advantageously protected against attacks such as spoofing attacks, man-in-the-middle attacks, and/or replay-attacks.

[0011] The method and apparatus as disclosed provides a secure configuration and/or update of a hearing device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The above and other features and advantages will become readily apparent to those skilled in the art by the following detailed description of exemplary embodiments thereof with reference to the attached drawings, in which:

- Fig. 1 schematically illustrates an exemplary architecture according to this disclosure,
- Fig. 2 schematically illustrates an exemplary hearing device,
- Fig. 3 schematically illustrates an exemplary signalling diagram,
- Fig. 4 schematically illustrates an exemplary signalling diagram, and
- Fig. 5 schematically illustrates a flowchart of an exemplary method

DETAILED DESCRIPTION

[0013] Various embodiments are described hereinafter with reference to the figures. Like reference numerals refer to like elements throughout. Like elements will, thus, not be described in detail with respect to the description of each figure. It should also be noted that the figures are only intended to facilitate the description of the embodiments. They are not intended as an exhaustive description of the claimed invention or as a limitation on the scope of the claimed invention. In addition, an illustrated embodiment needs not have all the aspects or advantages shown. An aspect or an advantage described in conjunction with a particular embodiment is not necessarily limited to that embodiment and can be practiced in any other embodiments even if not so illustrated, or if not so explicitly described.

[0014] Throughout, the same reference numerals are used for identical or corresponding parts.

[0015] It is an object of the present disclosure to provide a hearing device, and a method which seeks to mitigate, alleviate, or eliminate one or more of the above-identified deficiencies in the art and disadvantages singly or in any combination.

[0016] The present disclosure provides improved security of a hearing device. Security comprise assessing threats, vulnerabilities and attacks and developing appropriate safeguards and countermeasures to protect against threats and attacks.

[0017] The hearing device comprises a processing unit. The processing unit is configured to compensate for hearing loss or other hearing disability of a user of the hearing device.

[0018] The hearing device may be operated in one or more modes. The one or more modes may include a first mode and/or a second mode. The one or more modes may include a third mode and/or a fourth mode. The one or more modes may include a default mode.

[0019] The first mode may be a service mode. A service mode may be characterized in that a firmware part of the memory can be written in the service mode. The firmware part of the memory may be write-protected in at least one other mode of the hearing device.

[0020] The second mode may be a fitting mode. A fitting mode may be characterized in that a fitting part of the memory can be read and/or written in the fitting mode. A fitting mode may be characterized in that a firmware part of the memory is write-protected. The fitting part of the memory may comprise fitting data, such as hearing loss parameters, compressor parameters, filter coefficients, and/or gain coefficients.

[0021] The third mode may be a debug mode. A debug mode may be characterized in that a debug part of the memory can be read and/or written in the fitting mode. A debug mode may be characterized in that a fitting part of the memory can be read and/or written in the debug mode. A debug mode may be characterized in that a firmware part of the memory can be read and/or written in the debug mode. The debug part of the memory may be read-protected and/or write-protected in at least one other mode of the hearing device, such as in the default mode and/or the fitting mode.

[0022] The default mode may be a boot mode. A boot mode may be characterized in that the hearing device is operated according to operating parameters set during booting and/or in response to user input, e.g. program selection, volume up/down, etc. The default mode may be characterized in that the firmware part (or at least a part thereof) and/or the fitting part of the memory (or at least a part thereof) is write-protected and/or read-protected in the default mode. The default mode may be characterized in that the debug part of the memory (or at least a part thereof) is read-protected and/or write-protected in the default mode.

[0023] The hearing device comprises a memory. The memory may be embedded in the processing unit and/or be employed in a memory unit connected to the processing unit. The memory may comprise a first memory part. The first memory part may be a firmware part of the memory. The firmware part of the memory may be configured to be accessed in the service mode e.g. to be written to and/or read from in the service mode. The firmware part of the memory may additionally be configured to be accessed in the debug mode. The memory may comprise a second memory part. The second memory part may be a fitting part of the memory. The fitting part of the memory may be configured to be accessed in the fitting mode e.g. to be written to and/or read from in the fitting mode. The fitting part of the memory may additionally be configured to be accessed in the service mode and/or the debug mode. The memory may comprise a third memory part. The third memory part may be a debug part of the memory. The debug part of the memory may be configured to be accessed in the debug mode e.g. to be written to or read from in the debug mode.

[0024] The hearing device may comprise an interface configured for enabling communication between the hearing device and another device. The interface may comprise a wireless transceiver, e.g. configured for wireless communication at frequencies in the range from 2.4 to 2.5 GHz. The wireless transceiver may be a Bluetooth Low Energy transceiver. The interface may comprise a connector for forming a wired connection to the hearing device. The interface may form a connection to one or more other devices such as a tablet and/or a smart phone and/or a fitting device.

[0025] The processing unit/hearing device is configured to receive a mode request via the interface. The mode request may comprise a mode identifier indicative of the requested mode. The mode request may be a service mode request, e.g. the mode identifier is indicative of a first/service mode. The mode request may be a fitting mode request, e.g. the mode identifier is indicative of a second/fitting mode. The mode request may be a debug mode request, e.g. the mode identifier is indicative of a third/debug mode. Accordingly, the mode request may

be one of a service mode request, a fitting mode request, and a debug mode request.

[0026] The mode request may comprise a sender identifier indicative of the mode request sender. The mode request may comprise a certificate, such as a digital signature, for certifying the mode request sender. This allows for direct authentication of the mode request. The mode request may comprise a session identifier, e.g. an encrypted session identifier.

[0027] The hearing device may be paired with a sender of the mode request prior to receipt of the mode request. In the pairing, the hearing device and the sending/client device device may have exchanged one or more of hearing device identifier, sender identifier, session identifier, etc.

[0028] The processing unit/hearing device is configured to authenticate the mode request and to place the hearing device into the requested mode if authentication of the mode request succeeds. The processing unit may be configured to place the hearing device into a mode different from the requested mode, such as the default mode, if authentication of the mode request fails.

[0029] The hearing device disclosed herein has the advantage of verifying integrity of received mode requests and/or senders thereof, detecting any alteration and disregard altered mode requested. The hearing device disclosed herein may advantageously allow access to specific parts of the memory only with authenticated parties, such as an authenticated fitting device, an authenticated accessory device, an authenticated external device and/or an authenticated server.

[0030] The processing unit may be configured to authenticate the mode request by authenticating the sender of the mode request.

[0031] The processing unit/hearing device may be configured to authenticate the mode request by verifying integrity of a digital signature of the mode request.

The processing unit may be configured to authenticate the mode request by verifying integrity of the mode request. The mode request may comprise a message authentication code. To verify integrity of the mode request may comprise to verify the message authentication code, e.g. with a session identifier stored in the hearing device. The mode request may comprise a digital signature or certificate. To verify integrity of the mode request may comprise verifying the digital signature or certificate.

[0032] The processing unit/hearing device may be configured to send a mode response. For example, to place the hearing device into the requested mode if authentication of the mode request succeeds may comprise sending a mode response. The processing unit/hearing device may be configured to generate and/or send a mode response in response to the mode request. The processing unit may be configured to obtain and/or store a session identifier (may also be denoted session key) and include the session identifier and/or an encrypted version thereof in the mode response. To obtain the session identifier may comprise to generate the session identifier, e.g. as a random or pseudo-random number. Thus the hearing device and/or the processing unit may comprise a number generator, e.g. configured to generate a random or pseudo-random number as a session identifier. By using a unique session identifier or session identifier from a large number of available session identifiers, the processing power requirements in the hearing device may be reduced. Further, simple encryption is facilitated and replay-attacks are prevented.

[0033] The processing unit may be configured to encrypt the session identifier, optionally based on a hearing device key. The session identitier may be a session key in the form of a symmetric key. A symmetric session key may provide a lightweight processing of the security algorithms on the processing unit, such as lightweight encryption, lightweight decryption, lightweight integrity protection, etc. The hearing device key may be a symmetric key or a public key of a private-public key pair. The hearing device key may be stored in a permanent memory of the hearing device, e.g. during manufacture or during a fitting session.

[0034] The mode response may comprise the encrypted session key. The session response may comprise a hearing device identifier and/or the session key. Thus, the processing unit may be configured to send a hearing device identifier and/or the session key in the mode response. A mode response comprising a hearing device identifier may enable the sender of the mode request to obtain the hearing device key, either from a database or by requesting the hearing device key from the manufacturer, which in turn enables the sender of the mode request to decrypt an encrypted session identifier/key and use the session identifier when sending data to the hearing device.

[0035] The mode request may be received in a session. The processing unit/hearing devic may be configured to terminate the session if authentication of the mode request fails.

[0036] The mode request may comprise a signature, and to authenticate the mode request may comprise to verify the signature of the mode request.

[0037] The processing unit may be configured to obtain, e.g. generate a session identifier, e.g. upon receipt of the mode request or when the hearing device is in a service mode, a fitting mode, or a debug mode. The processing unit may be configured to encrypt the session identifier, e.g. with a hearing device key. The processing unit may be configured to transmit the session identifier or the encrypted session identifier via the interface, e.g. as a part of the mode response or a session setup message. The processing unit may be configured to store the session identifier in the hearing device.

[0038] The processing unit may be configured to receive data via the interface, e.g. when the hearing device is in a mode, e.g. the service mode, the fitting mode and/or the debug mode. The processing unit may be configured to authenticate the received data, e.g. when the hearing device is in one or more modes, e.g. the service

mode, the fitting mode and/or the debug mode. The processing unit may be configured to store hearing device data in a part of the memory based on the received data if authentication of the data succeeds. For example, when the hearing device is in a service mode, the processing unit may store hearing device data, such as e.g. firmware, based on the received data in the firmware part of the memory. In an exemplary hearing device, the processing unit may, when the hearing device is in a fitting mode, store hearing device data (fitting data) based on the received data in the fitting part of the memory. In an exemplary hearing device, the processing unit may, when the hearing device is in a debug mode, store hearing device data (debug data) based on the received data in the debug part of the memory.

[0039] The processing unit may be configured to authenticate the received data by verifying integrity of the received data. Verifying integrity of the received data may be based on the session identifier stored in the hearing device. The received data may comprise a message authentication code. To verify integrity of the received data may comprise to verify the message authentication code, e.g. with the stored session identifier. The received data may comprise a digital signature. To verify integrity of the received data may comprise verifying the digital signature.

[0040] The data may comprise a session identifier, and to authenticate the data may comprise to compare the session identifier of received data with the session identifier stored in the hearing device.

[0041] The data may be received in a session. The processing unit may be configured to terminate the session if authentication of the received data fails, e.g. the processing unit may be configured to terminate the session if integrity of the received data is corrupted, i.e. verification of the integrity fails. The processing unit may be configured to place the hearing device in another mode, such as the default mode, if authentication of the received data fails,

[0042] The hearing device/processing unit may be configured to receive a mode exit request and to place the hearing device in another mode, such as the default mode, e.g. if an authentication of the mode exit request succeeds. For example, a client device may send a mode exit request when fitting or transfer of firmware is done.

[0043] The disclosed method provides secure configuration and/or update of a hearing device. The method may comprise placing the hearing device into a default mode if authentication of the mode request fails. The method may comprise determining if operation in default mode fails, and switching to service mode if operating the hearing device in default mode fails,

[0044] In the method, authenticating the mode request may comprise authenticating the sender of the mode request.

[0045] In the method, the mode request may comprise a digital signature, and authenticating the mode request may comprise verifying the digital signature.

[0046] In the method, authenticating the mode request may comprise verifying integrity of the mode request.

[0047] The method may comprise receiving data via the interface, e.g. when the hearing device is in one or more modes, e.g. the service mode, the fitting mode and/or the debug mode. The method may comprise authenticating the received data, e.g. when the hearing device is in one or more modes, e.g. the service mode, the fitting mode and/or the debug mode. The method may comprise storing hearing device data in a part of the memory based on the received data if authentication of the data succeeds. For example, when the hearing device is in a service mode, the method may comprise storing hearing device data (firmware) based on the received data in the firmware part of the memory. In an exemplary method, the method may, when the hearing device is in a fitting mode, comprise storing hearing device data (fitting data) based on the received data in the fitting part of the memory. In an exemplary method, the method may, when the hearing device is in a debug mode, comprise storing hearing device data (debug data) based on the received data in the debug part of the memory. The method may comprise placing the hearing device in another mode, such as the default mode, if authenticating the received data fails.

[0048] The processing unit may be configured to operate the hearing device in default mode, and switch to service mode if operating the hearing device in default mode fails,

[0049] Fig. 1 schematically illustrates an exemplary architecture 100 according to this disclosure. The architecture 100 comprises a hearing device 101, a client device 110, and a server device 111. The client device 110 may comprise a computing device acting as a client, a fitting device, a handheld device, a relay, a tablet, a personal computer, a mobile phone, and/or USB dongle plugged into a personal computer. The server device 111 may comprise a computing device configured to act as a server, i.e. to serve requests from the client device 110 and/or from the hearing device 101. The server device 111 may be controlled by the hearing device manufacturer.

[0050] The hearing device 101 may be connected to the client device 110 via a communication link 113, such as a bidirectional communication link and/or a wireless communication link. The wireless communication link may be carried over a short-range communication system, such as Bluetooth, Bluetooth low energy, IEEE 802.11, Zigbee. The hearing device 101 may be connected to the client device 110 over a network.

[0051] The hearing device 101 may be connected to the server device 111 via a communication link 114 over a network 114a, such as a bidirectional and/or wireless communication link over a network.

[0052] The client device 110 may be connected to the server device 111 via a communication link 112 over a network 112a, such as a bidirectional and/or wireless communication link over a network. In an embodiment, the network 112a may be the Internet.

[0053] Fig. 2 schematically illustrates an exemplary hearing device 101. The exemplary hearing device 101 comprises a processing unit 202 configured to compensate for hearing loss of a user of the hearing device 101. The exemplary hearing device 101 comprises a memory and an interface 204. The memory is in Fig. 1 illustrated in the form of a memory unit 203 external to the processing unit 202. The memory may in other exemplary hearing devices be at least partly embedded in the processing unit 202 and/or in the memory unit 203.

[0054] The processing unit 202 is configured to receive a mode request via the interface 204. Hence, the processing unit 202 comprises a receive/send unit 205 configured to send and/or receive via the interface 204. The receive/send unit 205 is configured to send and receive via the interface 204 to/from an external device, such as a server device, a client device, a fitting device, an accessory, a relay device, a smart phone. The processing unit 202 is configured to authenticate the mode request. Hence, the processing unit 202 may comprise an authenticator 206 configured to authenticate the mode request. The processing unit 202 is configured to place the hearing device into the requested mode, such as a service mode, a fitting mode or debug mode, if authentication of the mode request succeeds. Hence the processing unit 202 comprises a mode controller configured to place the hearing device into the requested mode, e.g. based on an output from the authenticator 206. In the hearing aid in Fig. 2, the processing unit 202 is configured to place the hearing device into a default mode if authentication of the mode request fails, the default mode comprising booting the hearing device and operating the hearing device according to operating parameters set during booting. In an embodiment, the operating parameters set during booting may be stored in a non-volatile part of the memory unit 203. In an embodiment, the operating parameters set during booting may comprise a default setting enabling the hearing aid to function according to a default setting programmed during production of the hearing device.

[0055] The hearing device comprises a microphone 210 for receiving a sound signal and converting it into converted sound signal. The converted sound signal may be an electrical and digital version of the sound signal. The processing unit is configured to receive and process the converted sound signal into a processed sound signal according to a hearing loss of a user of the hearing device. The processed sound signal may be compressed and/or amplified or the like. The hearing device further comprises an output transducer/loudspeaker, known as a receiver 212. The receiver 212 is configured to receive the processed sound signal and convert it to an output sound signal for reception by an eardrum of the user.

[0056] Fig. 3 shows an exemplary signalling diagram 300 between a hearing device 101, and a client device 110. In an embodiment, the client device may be in the form of a fitting device. The hearing device 101 receives a fitting mode request 301 via the interface 204 from the client device 110, the mode request comprising a digital signature and a mode identifier. The digital signature may be a signature according to the Digital Signature Standard or other suitable standards, such as RSA. for digital signatures known in the art.. The hearing device 101 authenticates the mode request by verifying the digital signature. In the illustrated signalling diagram 300, the authentication succeeds, and the processing unit places the hearing device in the fitting mode including sending a fitting mode response 302 to the client device via the interface 204. In the fitting mode of hearing device 101, a firmware part of the memory is write-protected and a fitting mode part of the memory is write-enabled.

[0057] Upon receipt of the fitting mode response 302, the client device 110 sends data 303 to the hearing device 101 which receives the data and authenticates the received data 303, e.g. by use of digital signature or a session identifier/key as described earlier. If authentication of data 303 succeeds, the processing unit 202 derives hearing device data (fitting data) from the data 303 and stores hearing device data (fitting data) in a fitting part of the memory. If authentication of data 303 fails, the processing unit 202 places the hearing device in default mode.

[0058] When the fitting data have been transferred, the client device may send a mode exit request and the hearing device is configured to optionally authenticate the mode exit request and to place the hearing device in the default mode, optionally if authentication of the mode exit request succeeds.

[0059] In another embodiment, the client device may be in the form of a smart phone or a tablet and may comprise software configured to provide the functionality of a fitting device.

[0060] Fig. 4 shows an exemplary signalling diagram 300' where a client device 110 is used for updating firmware of the hearing device 101, and a client device 110 in the form of a fitting device. The hearing device 101 receives a service mode request 304 via the interface 204 from the client device 110. The hearing device 101 authenticates the service mode request. In the illustrated signalling diagram 300', the authentication succeeds, and the processing unit 202 places the hearing device in the service mode including sending a service mode response 305 to the client device via the interface 204. In the service mode of hearing device 101, the processing unit 202 is allowed to write to a firmware part of the memory.

[0061] Upon receipt of the service mode response 305, the client device 110 sends data 306 to the hearing device 101 which receives the data and authenticates the received data 306, e.g. by use of digital signature or a session identifier/key as described earlier. Before sending data to the hearing device, the client device 110 may correspond with a server device 111 as illustrated with dotted arrows 307, 308, e.g. in order to determine the data 306 to be sent to the hearing device. If authentication of data 306 succeeds, the processing unit 202 derives

hearing device data (firmware data) from the data 306 and stores hearing device data (firmware data) in a firmware part of the memory. If authentication of data 306 fails, the processing unit 202 may place the hearing device in default mode and/or terminate the session.

[0062] When the firmware has been transferred, the client device may send a mode exit request and the hearing device is configured to optionally authenticate the mode exit request and place the hearing device in the default mode, optionally if authentication of the mode exit request succeeds.

[0063] Fig. 5 illustrates an exemplary flowchart of a method 400, e.g. for configuration of a hearing device, such as hearing device 101, comprising a processing unit configured to compensate for hearing loss of a user of the hearing device, a memory, and an interface. The method 400 comprises receiving 401 a mode request via the interface and authenticating 402 the mode request. Authenticating 402 the mode request comprises authenticating the sender of the mode request and verifying integrity of the mode request. If authentication of the mode request succeeds 404, the method proceeds to placing 403 the hearing device into the requested mode. If authentication of the mode request fails 404, the method optionally proceeds to placing 405 the hearing device into a default mode. After placing the hearing device in the requested mode, the method optionally proceeds to receiving 408 data via the interface, authenticating 410 the received data; and storing 412 hearing device data in a part of the memory corresponding to the requested mode and based on the received data if authentication of the data succeeds. If authenticating 410 the received data fails, the method may proceed to placing 405 the hearing device in default mode or another mode and/or terminating the session. Upon storing, the method 400 optionally comprises to evaluate 414 whether a mode exit request has been received. If so, the method proceeds to placing 405 the hearing device in default mode. If not, the method proceeds to receiving 408 data.

[0064] The use of the terms "first", "second", "third" and "fourth", etc. does not imply any particular order, but are included to identify individual elements. Moreover, the use of the terms first, second, etc. does not denote any order or importance, but rather the terms first, second, etc. are used to distinguish one element from another. Note that the words first and second are used here and elsewhere for labelling purposes only and are not intended to denote any specific spatial or temporal ordering. Furthermore, the labelling of a first element does not imply the presence of a second element and vice versa.

[0065] Although particular features have been shown and described, it will be understood that they are not intended to limit the claimed invention.

LIST OF REFERENCES

[0066]

100 architecture
101 hearing device
111 server device
202 processing unit
203 memory unit
204 interface
205 receive/send unit
206 authenticator
207 mode controller
210 microphone
212 receiver
300, 300' signalling diagram
301 fitting mode request
302 fitting mode response
303 data
304 service mode request
305 service mode response
306 data
307 firmware request
308 firmware response
400 method for configuration of a hearing device
401 receiving mode request
402 authenticating mode request
403 placing hearing device in requested mode
404 authentication ok?
405 placing hearing device in default mode
408 receiving data via the interface
410 authenticating the received data
412 storing hearing device data
414 evaluating if mode exit request has been received

Claims

1. A hearing device (101) comprising

- a processing unit (202) configured to compensate for hearing loss of a user of the hearing device;
- a memory (203); and
- an interface (204),

wherein the processing unit (202) is configured to:

- receive a mode request via the interface, wherein the mode request is one or more of a service mode request for a service mode, a fitting mode request; and a debug mode request, wherein the service mode is **characterized in that** a firmware part of the memory (203) is writable;
- authenticate the mode request; and
- place the hearing device into the requested mode if authentication of the mode request succeeds.

2. A hearing device according to claim 1, wherein the

processing unit is configured to place the hearing device into a default mode if authentication of the mode request fails.

3. A hearing device according to claim 2, wherein the default mode comprises booting the hearing device and operating the hearing device according to operating parameters set during booting.

4. A hearing device according to any of claims 1-3, wherein the processing unit is configured to authenticate the mode request by authenticating the sender of the mode request.

5. A hearing device according to any of the preceding claims, wherein the processing unit is configured to authenticate the mode request by verifying integrity of the mode request.

6. A hearing device according to any of the preceding claims, wherein to place the hearing device into the requested mode if authentication of the mode request succeeds comprises sending a mode response.

7. A hearing device according to any of the preceding claims, wherein the mode request is received in a session and the processing unit is configured to terminate the session if authentication of the mode request fails.

8. A hearing device according to any of the preceding claims, wherein the mode request comprises a signature, and wherein to authenticate the mode request comprises to verify the signature of the mode request.

9. A hearing device according to any of the preceding claims, wherein when the hearing device is in a service mode, the processing unit is configured to generate a session identifier, to transmit the session identifier via the interface and to store the session identifier in the hearing device.

10. A hearing device according to any of the preceding claims, wherein when the hearing device is in a service mode, the processing unit is configured to receive data via the interface, wherein the processing unit is configured to authenticate the received data and store hearing device data in a part of the memory based on the received data if authentication of the data succeeds.

11. A hearing device according to claim 10 as dependent on claim 9, wherein the data comprises a session identifier, and wherein to authenticate the data comprises to compare the received session identifier with the session identifier stored in the hearing device.

12. A hearing device according to claim 10, wherein the data is received in a session and the processing unit is configured to terminate the session if authentication of the received data fails.

13. Method (400) for configuration of a hearing device comprising a processing unit configured to compensate for hearing loss of a user of the hearing device, a memory, and an interface, the method comprising:

receiving (401) a mode request via the interface, wherein the mode request is one or more of a service mode request for updating firmware data, a fitting mode request; and
a debug mode request;

- authenticating (402) the mode request; and
- placing (403) the hearing device into the requested mode if authentication of the mode request succeeds.

14. Method according to claim 13, the method comprising placing (405) the hearing device into a default mode if authentication of the mode request fails.

15. Method according to any of claims 13-14, wherein authenticating the mode request comprises authenticating the sender of the mode request.

16. Method according to any of claims 13-15, wherein authenticating the mode request comprises verifying integrity of the mode request.

17. Method according to any of claims 13-16, wherein when the hearing device is in a service mode, the method comprises:

- receiving (408) data via the interface,
- authenticating (410) the received data; and
- storing (412) hearing device data in a part of the memory based on the received data if authentication of the data succeeds.

Patentansprüche

1. Hörgerät (101), umfassend

- eine Verarbeitungseinheit (202), die konfiguriert ist, um Hörverlust eines Benutzers des Hörgeräts zu kompensieren;
- einen Speicher (203); und
- eine Schnittstelle (204),

wobei die Verarbeitungseinheit (202) konfiguriert ist, um:

- eine Betriebsartanforderung über die Schnittstelle zu empfangen, wobei die Betriebsartanforderung eines oder mehreres von einer Servicebetriebsartanforderung für eine Servicebetriebsart, einer Anpassungsbetriebsartanforderung; und einer Debug-Betriebsartanforderung ist, wobei die Servicebetriebsart **dadurch gekennzeichnet ist, dass** ein Firmwareteil des Speichers (203) beschreibbar ist;
- die Betriebsartanforderung zu authentifizieren; und
- das Hörgerät in die angeforderte Betriebsart zu versetzen, wenn die Authentifizierung der Betriebsartanforderung erfolgreich ist.

2. Hörgerät nach Anspruch 1, wobei die Verarbeitungseinheit konfiguriert ist, um das Hörgerät in eine Standardbetriebsart zu versetzen, wenn Authentifizierung der Betriebsartanforderung fehlschlägt.

3. Hörgerät nach Anspruch 2, wobei die Standardbetriebsart ein Starten des Hörgeräts und ein Betreiben des Hörgeräts gemäß während des Startens festgelegten Betriebsparametern umfasst.

4. Hörgerät nach einem der Ansprüche 1 bis 3, wobei die Verarbeitungseinheit konfiguriert ist, um die Betriebsartanforderung zu authentifizieren, indem der Absender der Betriebsartanforderung authentifiziert wird.

5. Hörgerät nach einem der vorhergehenden Ansprüche, wobei die Verarbeitungseinheit konfiguriert ist, um die Betriebsartanforderung zu authentifizieren, indem die Integrität der Betriebsartanforderung verifiziert wird.

6. Hörgerät nach einem der vorhergehenden Ansprüche, wobei das Versetzen des Hörgeräts in die angeforderte Betriebsart das Senden einer Betriebsartantwort umfasst, wenn die Authentifizierung der Betriebsartanforderung erfolgreich ist.

7. Hörgerät nach einem der vorhergehenden Ansprüche, wobei die Betriebsartanforderung in einer Sitzung empfangen wird und die Verarbeitungseinheit konfiguriert ist, um die Sitzung zu beenden, wenn Authentifizierung der Betriebsartanforderung fehlschlägt.

8. Hörgerät nach einem der vorhergehenden Ansprüche, wobei die Betriebsartanforderung eine Signatur umfasst und wobei das Authentifizieren der Betriebsartanforderung das Verifizieren der Signatur der Betriebsartanforderung umfasst.

9. Hörgerät nach einem der vorhergehenden Ansprüche, wobei, wenn sich das Hörgerät in einer Servicebetriebsart befindet, die Verarbeitungseinheit konfiguriert ist, um eine Sitzungskennung zu generieren, um die Sitzungskennung über die Schnittstelle zu übertragen und die Sitzungskennung im Hörgerät zu speichern.

10. Hörgerät nach einem der vorhergehenden Ansprüche, wobei, wenn sich das Hörgerät in einer Servicebetriebsart befindet, die Verarbeitungseinheit konfiguriert ist, um Daten über die Schnittstelle zu empfangen, wobei die Verarbeitungseinheit konfiguriert ist, um die empfangenen Daten zu authentifizieren und Hörgerätedaten in einem Teil des Speichers auf der Grundlage der empfangenen Daten zu speichern, wenn die Authentifizierung der Daten erfolgreich ist.

11. Hörgerät nach Anspruch 10 in Abhängigkeit von Anspruch 9, wobei die Daten eine Sitzungskennung umfassen und wobei das Authentifizieren der Daten ein Vergleichen der empfangenen Sitzungskennung mit der Sitzungskennung umfasst, die im Hörgerät gespeichert ist.

12. Hörgerät nach Anspruch 10, wobei die Daten in einer Sitzung empfangen werden und die Verarbeitungseinheit konfiguriert ist, um die Sitzung zu beenden, wenn Authentifizierung der empfangenen Daten fehlschlägt.

13. Verfahren (400) zur Konfiguration eines Hörgeräts, das eine Verarbeitungseinheit, die konfiguriert ist, um Hörverlust eines Benutzers des Hörgeräts zu kompensieren, einen Speicher und eine Schnittstelle umfasst, wobei das Verfahren umfasst: Empfangen (401) einer Betriebsartanforderung über die Schnittstelle, wobei die Betriebsartanforderung eines oder mehreres von einer Servicebetriebsartanforderung zum Aktualisieren von Firmwaredaten, einer Anpassungsbetriebsartanforderung und einer Debug-Betriebsartanforderung ist;

- Authentifizieren (402) der Betriebsartanforderung; und
- Versetzen (403) des Hörgeräts in die angeforderte Betriebsart, wenn die Authentifizierung der Betriebsartanforderung erfolgreich ist.

14. Verfahren nach Anspruch 13, wobei das Verfahren das Versetzen (405) des Hörgeräts in eine Standardbetriebsart umfasst, wenn die Authentifizierung der Betriebsartanforderung fehlschlägt.

15. Verfahren nach einem der Ansprüche 13 bis 14, wobei das Authentifizieren der Betriebsartanforderung das Authentifizieren des Absenders der Betriebsartanforderung umfasst.

16. Verfahren nach einem der Ansprüche 13 bis 15, wobei das Authentifizieren der Betriebsartanforderung das Verifizieren der Integrität der Betriebsartanforderung umfasst.

17. Verfahren nach einem der Ansprüche 13 bis 16, wobei, wenn sich das Hörgerät in einer Servicebetriebsart befindet, das Verfahren umfasst:

- Empfangen (408) von Daten über die Schnittstelle,
- Authentifizieren (410) der empfangenen Daten; und
- Speichern (412) von Hörgerätedaten in einem Teil des Speichers auf der Grundlage der empfangenen Daten, wenn die Authentifizierung der Daten erfolgreich ist.

Revendications

1. Prothèse auditive (101) comprenant :

- une unité de traitement (202) configurée pour compenser la perte d'audition d'un utilisateur de la prothèse auditive ;
- une mémoire (203) ; et
- une interface (204),

dans laquelle l'unité de traitement (202) est configurée pour :

- recevoir une requête de mode via l'interface, dans laquelle la requête de mode est une ou plusieurs d'une requête de mode service pour un mode service, d'une requête de mode ajustement ; et d'une requête de mode débogage, dans laquelle le mode service est **caractérisé en ce qu'**une partie de micrologiciel de la mémoire (203) est inscriptible ;
- authentifier la requête de mode ; et
- placer la prothèse auditive dans le mode requis si l'authentification de la requête de mode réussit.

2. Prothèse auditive selon la revendication 1, dans laquelle l'unité de traitement est configurée pour placer la prothèse auditive en mode défaut si l'authentification de la requête de mode échoue.

3. Prothèse auditive selon la revendication 2, dans laquelle le mode défaut comprend l'amorçage de la prothèse auditive et le fonctionnement de la prothèse auditive selon les paramètres de fonctionnement définis durant l'amorçage.

4. Prothèse auditive selon l'une quelconque des revendications 1 à 3, dans laquelle l'unité de traitement est configurée pour authentifier la requête de mode par authentification de l'expéditeur de la requête de mode.

5. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle l'unité de traitement est configurée pour authentifier la requête de mode par vérification de l'intégrité de la requête de mode.

6. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle le placement de la prothèse auditive dans le mode requis si l'authentification de la requête de mode réussit comprend l'envoi d'une réponse de mode.

7. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle la requête de mode est reçue dans une session et l'unité de traitement est configurée pour mettre un terme à la session si l'authentification de la requête de mode échoue.

8. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle la requête de mode comprend une signature, et dans laquelle l'authentification de la requête de mode comprend la vérification de la signature de la requête de mode.

9. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle lorsque la prothèse auditive se trouve dans un mode service, l'unité de traitement est configurée pour générer un identifiant de session, pour transmettre l'identifiant de session via l'interface et pour stocker l'identifiant de session dans la prothèse auditive.

10. Prothèse auditive selon l'une quelconque des revendications précédentes, dans laquelle lorsque la prothèse auditive est en mode service, l'unité de traitement est configurée pour recevoir des données via l'interface, dans laquelle l'unité de traitement est configurée pour authentifier les données reçues et stocker les données de prothèse auditive dans une partie de la mémoire sur la base des données reçues si l'authentification des données réussit.

11. Prothèse auditive selon la revendication 10 lorsqu'elle dépend de la revendication 9, dans laquelle les données comprennent un identifiant de session, et dans laquelle l'authentification des données comprend la comparaison de l'identifiant de session reçu à l'identifiant de session stocké dans la prothèse auditive.

12. Prothèse auditive selon la revendication 10, dans laquelle les données sont reçues dans une session et l'unité de traitement est configurée pour mettre un

terme à la session si l'authentification des données reçues échoue.

13. Procédé (400) de configuration d'une prothèse auditive comprenant une unité de traitement configurée pour compenser la perte auditive d'un utilisateur de la prothèse auditive, une mémoire et une interface, le procédé comprenant :
la réception (401) d'une requête de mode via l'interface, dans laquelle la requête de mode est une ou plusieurs d'une requête de mode service pour mettre à jour les données de micrologiciel, une requête de mode ajustement ; et une requête de mode débogage ;

- l'authentification (402) de la requête de mode ; et
- le placement (403) de la prothèse auditive dans le mode requis si l'authentification de la requête de mode réussit.

14. Procédé selon la revendication 13, le procédé comprenant le placement (405) de la prothèse auditive dans un mode défaut si l'authentification de la requête de mode échoue.

15. Procédé selon l'une quelconque des revendications 13 et 14, dans lequel l'authentification de la requête de mode comprend l'authentification de l'expéditeur de la requête de mode.

16. Procédé selon l'une quelconque des revendications 13 à 15, dans lequel l'authentification de la requête de mode comprend la vérification de l'intégrité de la requête de mode.

17. Procédé selon l'une quelconque des revendications 13 à 16, dans lequel lorsque la prothèse auditive est en mode service, le procédé comprend :

- la réception (408) de données via l'interface,
- l'authentification (410) des données reçues ; et
- le stockage (412) des données de prothèse auditive dans une partie de la mémoire sur la base des données reçues si l'authentification des données réussit.

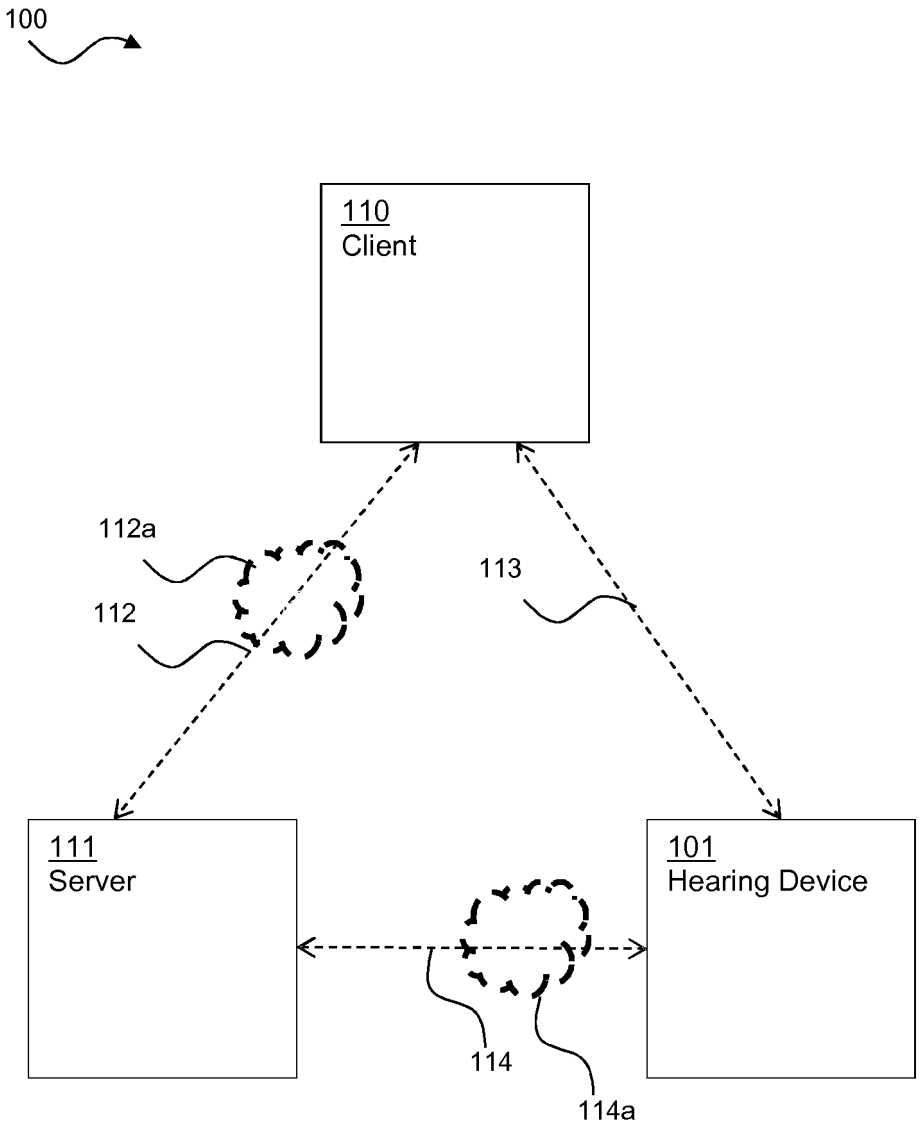
100
110
Client
112a
112
113
111
Server
101
Hearing Device
114
114a

Fig. 1

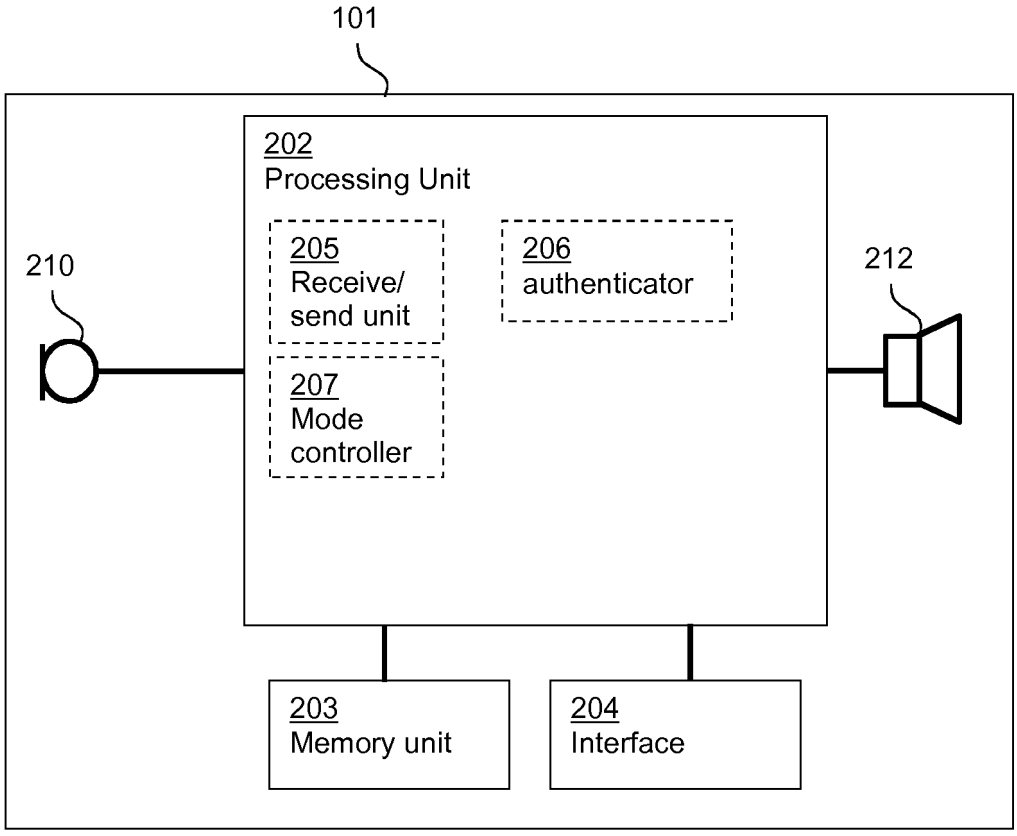
101
202
Processing Unit
205
Receive/
send unit
206
authenticator
207
Mode
controller
210
212
203
Memory unit
204
Interface

Fig. 2

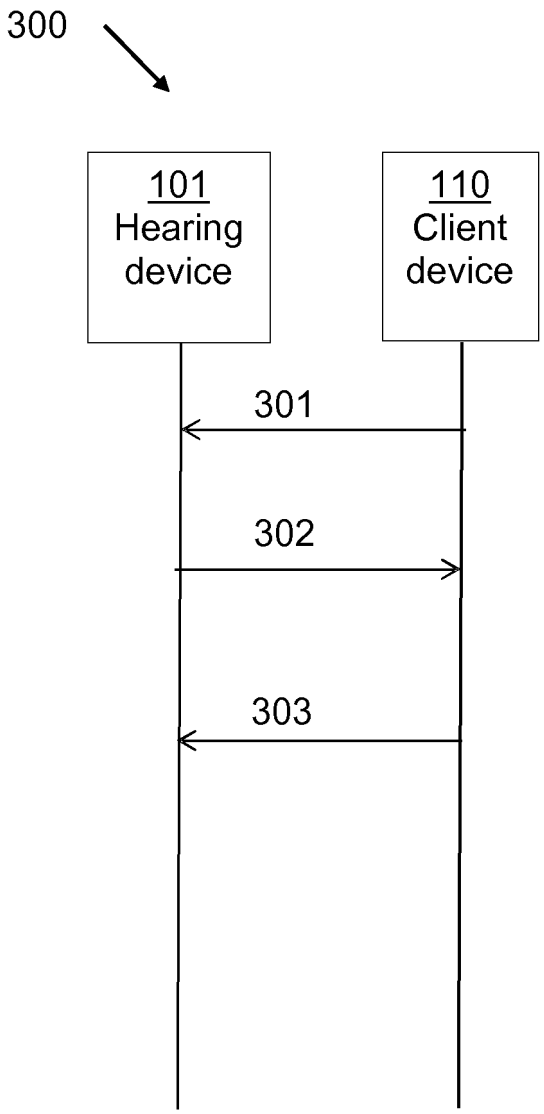

Fig. 3

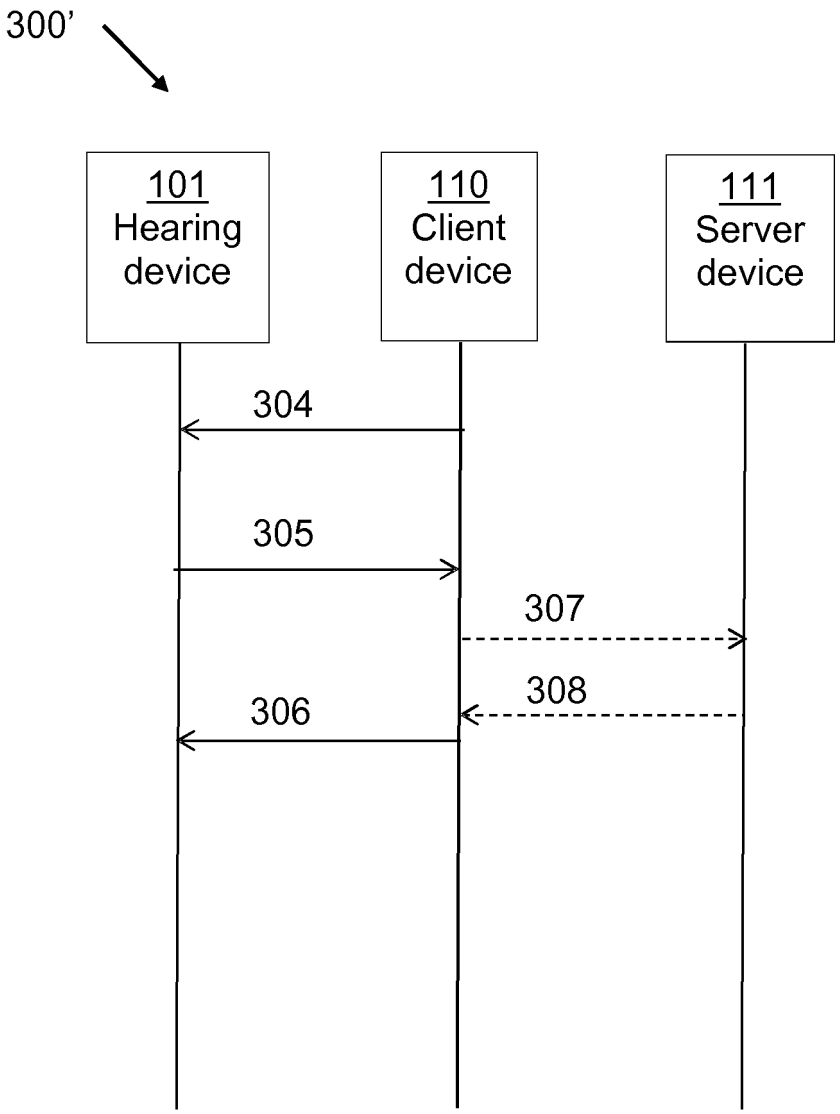
300'
101
Hearing device
110
Client device
111
Server device
304
305
307
308
306

Fig. 4

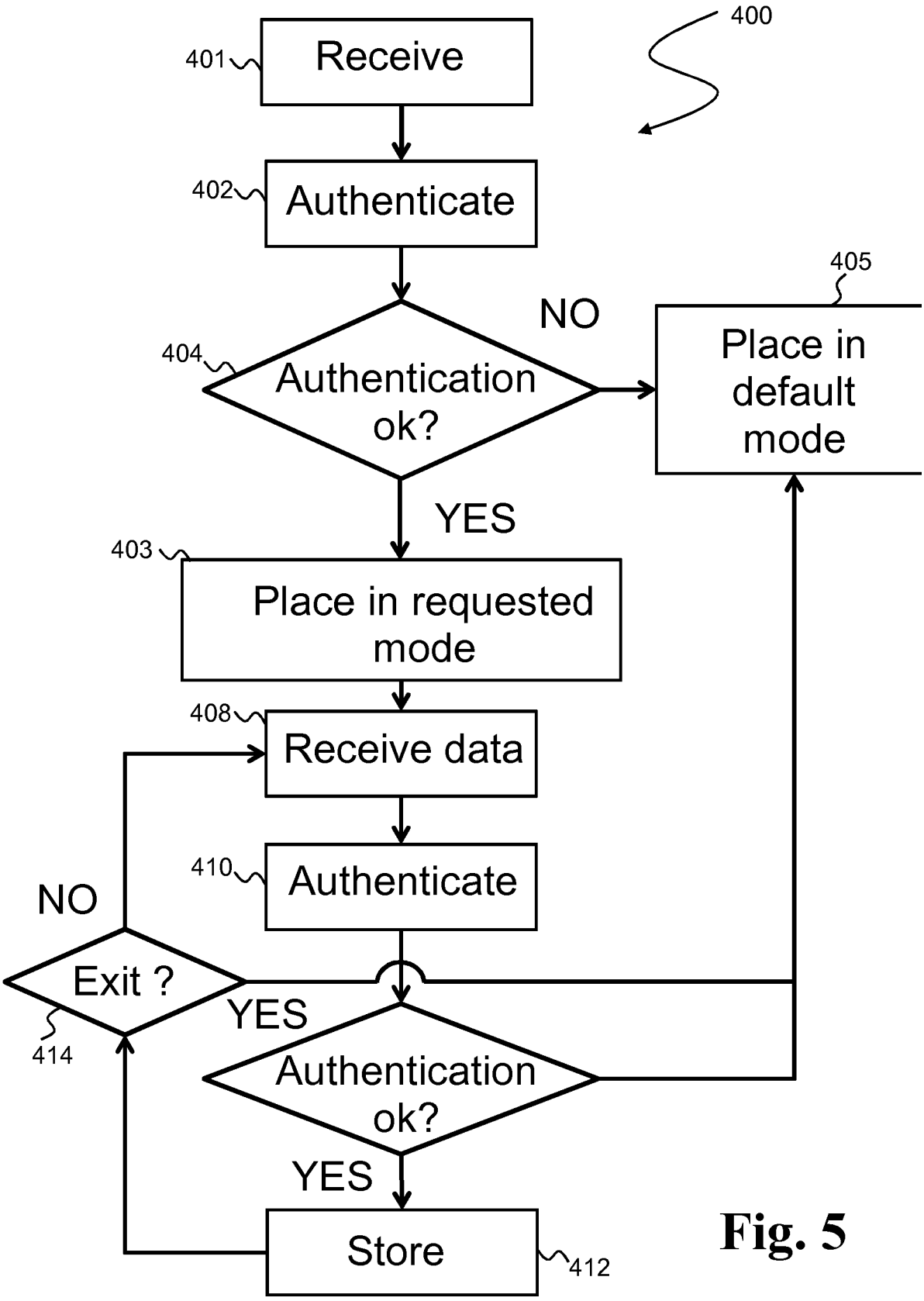
400
401
Receive
402
Authenticate
404
Authentication ok?
NO
405
Place in default mode
YES
403
Place in requested mode
408
Receive data
410
Authenticate
NO
Exit ?
414
YES
Authentication ok?
YES
Store
412

Fig. 5

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

- US 20050069161 A **[0003]**
- US 20080165994 A **[0004]**
- US 20140211972 A **[0005]**
- US 20070230711 A **[0006]**