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

(11) EP 3 032 845 A1

(12) EUROPEAN PATENT APPLICATION

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

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

(21) Application number: **14197819.7**

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

(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
Designated Extension States:
BA ME

(71) Applicant: **GN ReSound A/S**
2750 Ballerup (DK)

(72) Inventors:
- **Pedersen, Brian Dam**
  DK-4100 Ringsted (DK)
- **Vendelbo, Allan Munk**
  DK-2750 Ballerup (DK)

(74) Representative: **Zacco Denmark A/S**
Arne Jacobsens Allé 15
2300 Copenhagen S (DK)

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

(57) 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. 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.

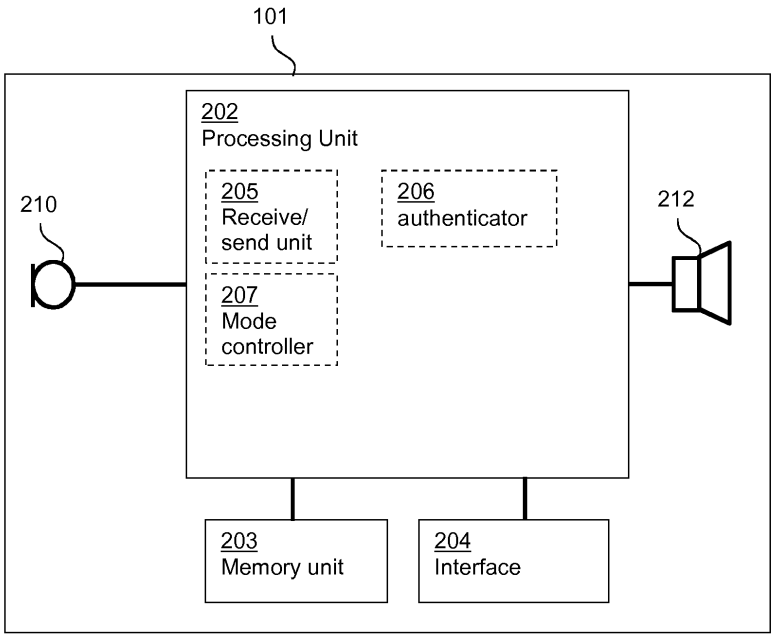

Fig. 2

EP 3 032 845 A1

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.

SUMMARY

[0003] 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.

[0004] 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.

[0005] 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.

[0006] 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.

[0007] The method and apparatus as disclosed provides a secure configuration and/or update of a hearing device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] 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

[0009] 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.

[0010] Throughout, the same reference numerals are used for identical or corresponding parts.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] 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.

[0024] 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.

[0025] 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.

[0026] The processing unit may be configured to authenticate the mode request by authenticating the sender of the mode request.

[0027] The processing unit/hearing device may be configured to authenticate the mode request by verifying integrity of a digital signature of the mode request.

[0028] 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.

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] The mode request may comprise a signature, and to authenticate the mode request may comprise to verify the signature of the mode request.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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,

[0039] 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.

[0040] 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,

[0041] In the method, authenticating the mode request may comprise authenticating the sender of the mode request.

[0042] In the method, the mode request may comprise a digital signature, and authenticating the mode request may comprise verifying the digital signature.

[0043] In the method, authenticating the mode request may comprise verifying integrity of the mode request.

[0044] 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.

[0045] 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,

[0046] 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.

[0047] 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.

[0048] 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.

[0049] 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.

[0050] 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.

[0051] 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.

[0052] 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.

[0053] 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.

[0054] 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.

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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.

[0062] Although particular features have been shown and described, it will be understood that they are not intended to limit the claimed invention, and it will be made obvious to those skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the claimed invention. The specification and drawings are, accordingly to be regarded in an illustrative rather than restrictive sense. The claimed invention is intended to cover all alternatives, modifications and equivalents.

LIST OF REFERENCES

[0063]

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 comprising

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

wherein the processing unit is 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.

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 the mode request is one or more of

- a service mode request,
- a fitting mode request; and
- a debug mode request.

7. 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.

8. 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.

9. 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.

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 generate a session identifier, to transmit the session identifier via the interface and to store the session identifier in the hearing device.

11. 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.

12. A hearing device according to claim 11 as dependent on claim 10, 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.

13. A hearing device according to claim 11, 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.

14. 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 comprising:

    - 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.

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

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

17. Method according to any of claims 14-16, wherein authenticating the mode request comprises verifying integrity of the mode request.

18. Method according to any of claims 14-17, wherein when the hearing device is in a service mode, the method comprises:

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

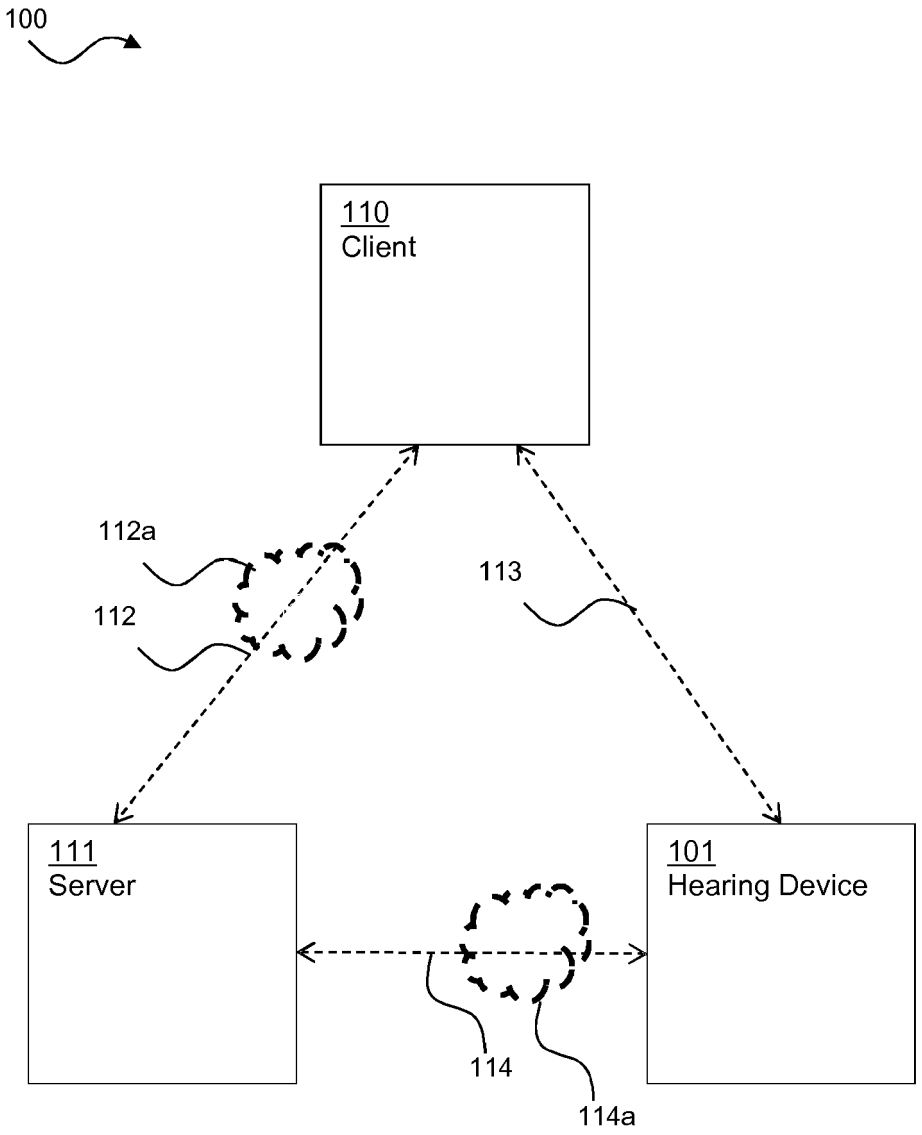
100
110
Client
112a
112
113
111
Server
101
Hearing Device
114
114a

Fig. 1

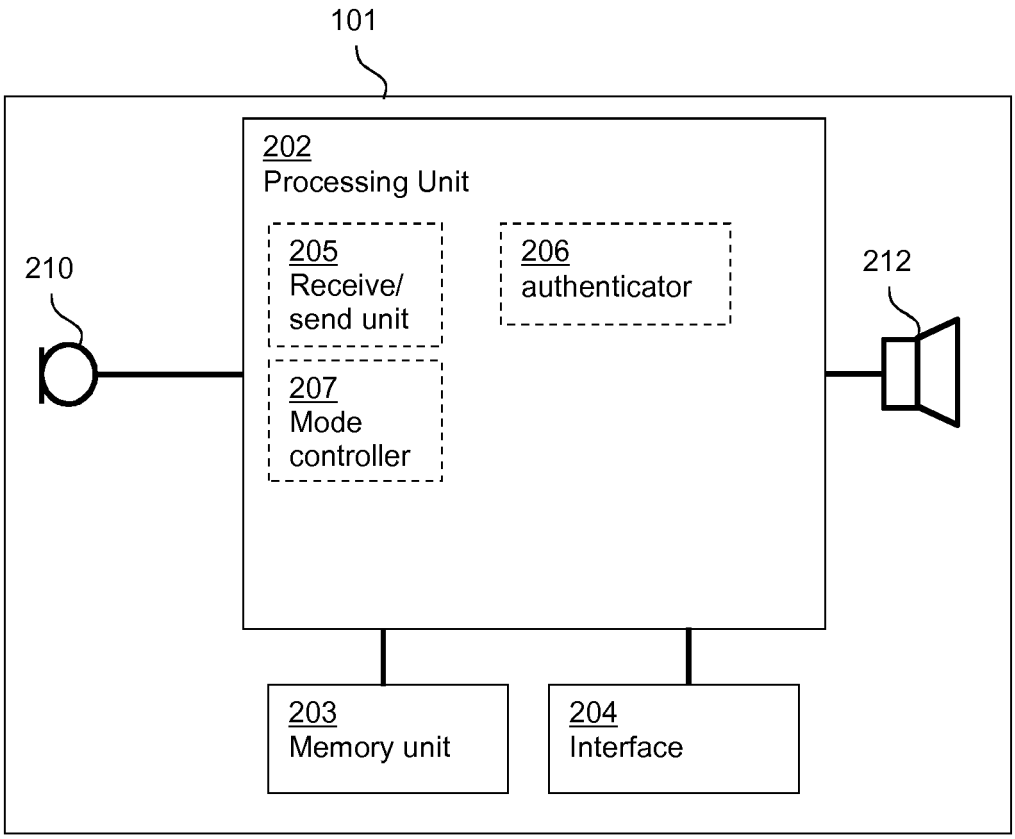
101
202
Processing Unit
205
Receive/
send unit
206
authenticator
207
Mode
controller
210
212
203
Memory unit
204
Interface

Fig. 2

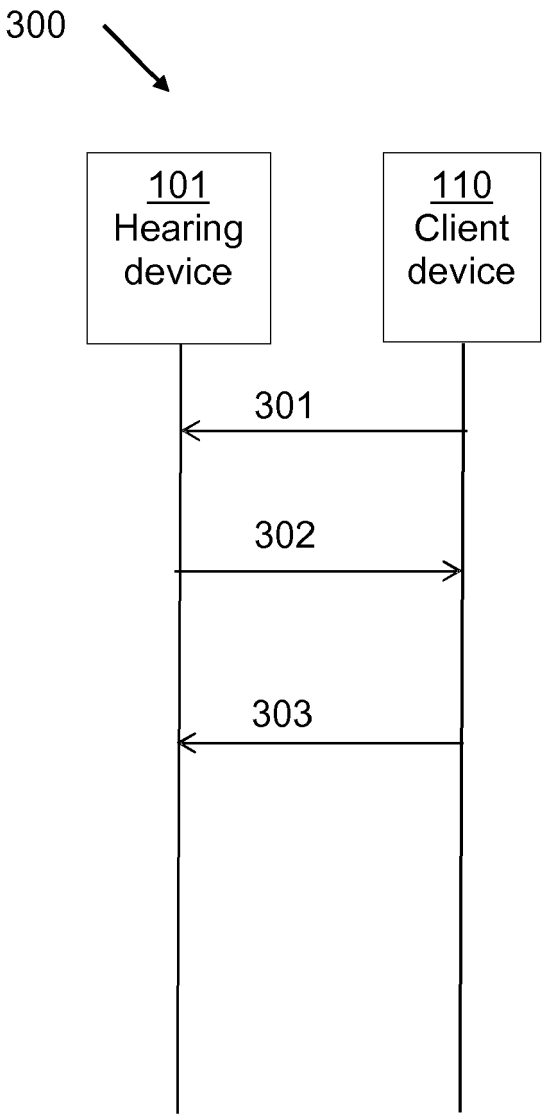

Fig. 3

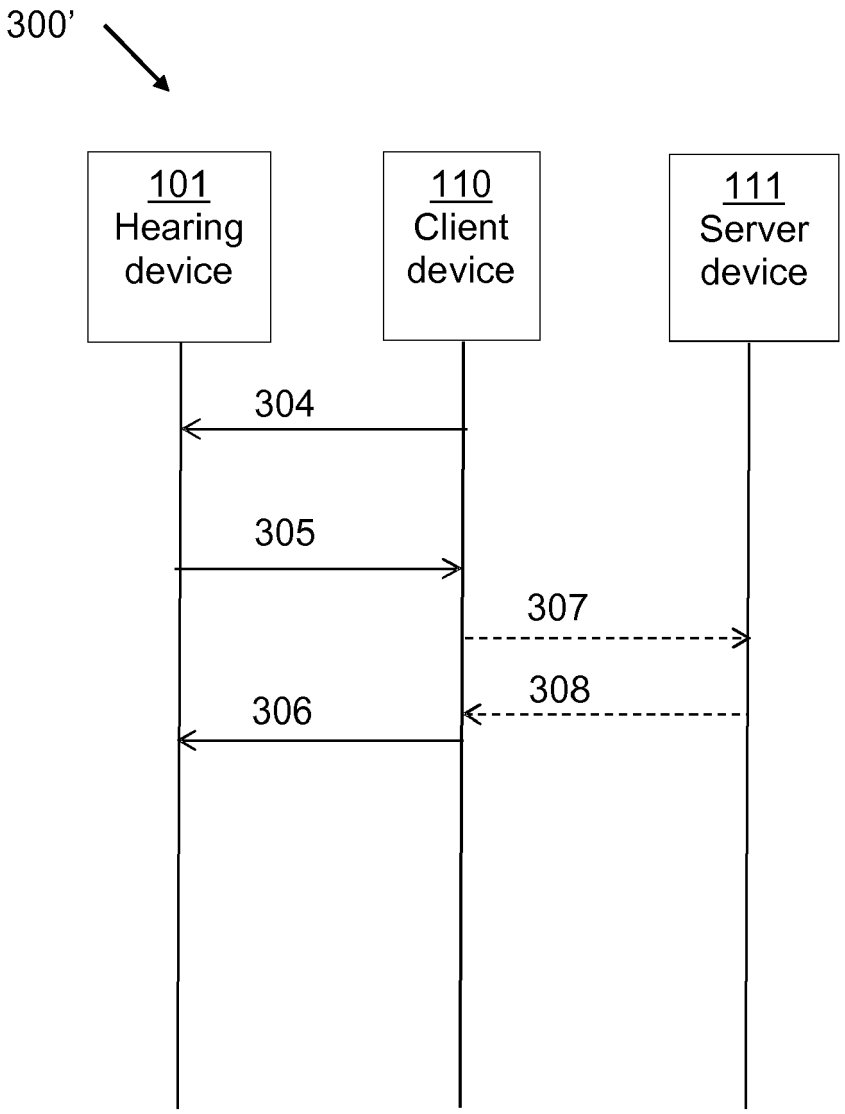
300'
101
Hearing device
110
Client device
111
Server device
304
305
307
308
306

Fig. 4

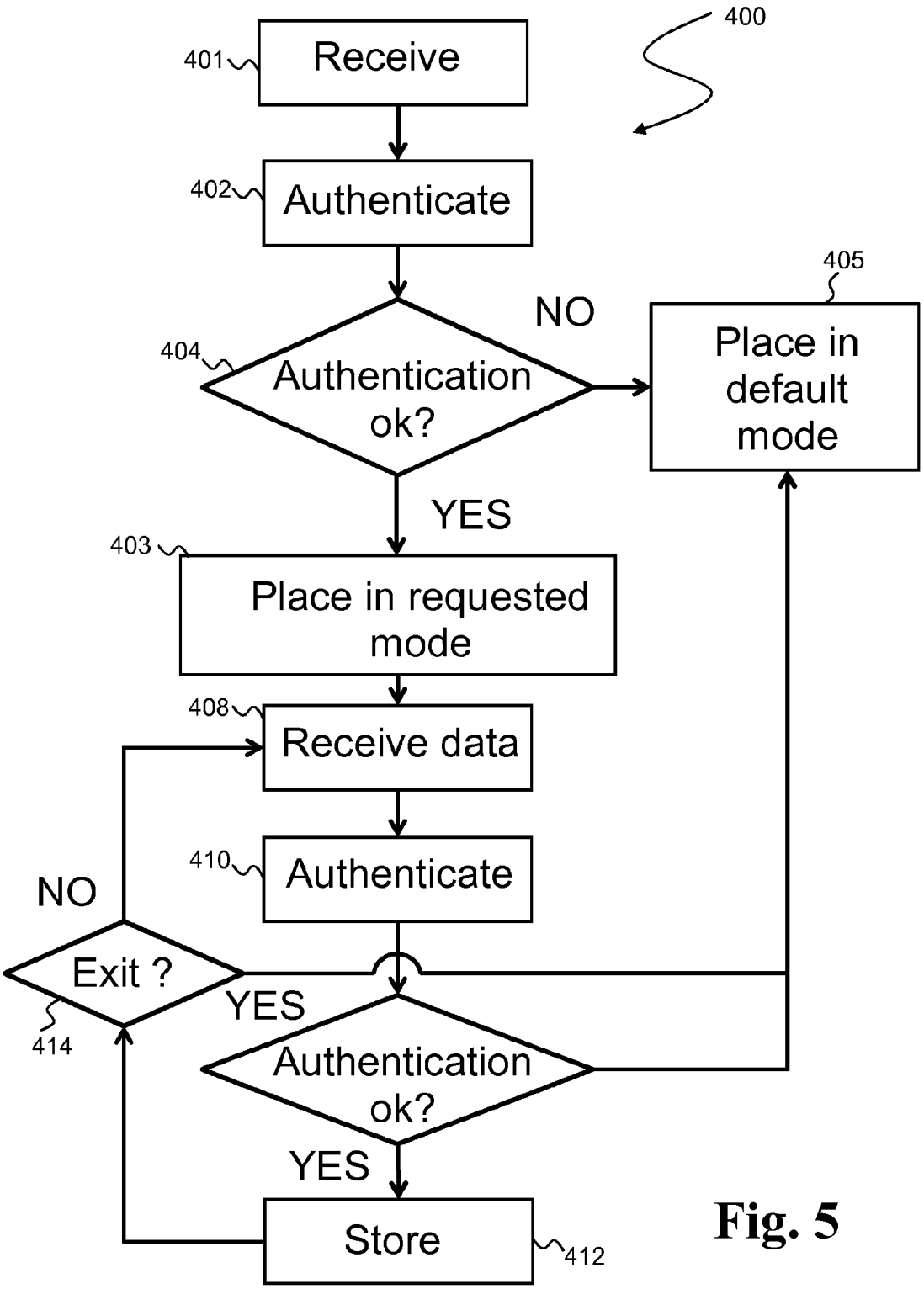
400
401
Receive
402
Authenticate
404
Authentication ok?
NO
405
Place in default mode
YES
403
Place in requested mode
408
Receive data
410
Authenticate
NO
Exit ?
414
YES
Authentication ok?
YES
Store
412

Fig. 5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 14 19 7819

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2005/069161 A1 (KALTENBACH MATT ANDREW [US] ET AL) 31 March 2005 (2005-03-31) * paragraphs [0026] - [0038]; figures 2, 8 *	1-18	INV. H04R25/00
X	US 2008/165994 A1 (CAREN BARRY [US] ET AL) 10 July 2008 (2008-07-10) * paragraphs [0016] - [0018]; figure 2 *	1-15	
X	US 2014/211972 A1 (KIM YU-NA [KR] ET AL) 31 July 2014 (2014-07-31) * paragraphs [0113] - [0142]; figures 1, 6A-6C *	1-18	

TECHNICAL FIELDS SEARCHED (IPC)

H04R

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	19 May 2015	Kunze, Holger

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 14 19 7819

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-05-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005069161 A1	31-03-2005	EP 1668958 A1	14-06-2006
		JP 5147238 B2	20-02-2013
		JP 5442828 B2	12-03-2014
		JP 2007510318 A	19-04-2007
		JP 2013042532 A	28-02-2013
		US 2005069161 A1	31-03-2005
		US 2007225050 A1	27-09-2007
		WO 2005034577 A1	14-04-2005
US 2008165994 A1	10-07-2008	NONE	
US 2014211972 A1	31-07-2014	KR 20140098615 A	08-08-2014
		US 2014211972 A1	31-07-2014
		WO 2014119845 A1	07-08-2014

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82