

(19) **DANMARK**

(10) **DK/EP 3334190 T3**



Patent- og
Varemærkestyrelsen

(12) Oversættelse af
europæisk patentskrift

-
- (51) Int.Cl.: **H 04 R 25/00 (2006.01)**
- (45) Oversættelsen bekendtgjort den: **2021-11-15**
- (80) Dato for Den Europæiske Patentmyndigheds
bekendtgørelse om meddelelse af patentet: **2021-08-04**
- (86) Europæisk ansøgning nr.: **16202920.1**
- (86) Europæisk indleveringsdag: **2016-12-08**
- (87) Den europæiske ansøgnings publiceringsdag: **2018-06-13**
- (84) Designerede stater: **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**
- (73) Patenthaver: **GN HEARING A/S, Lautrupbjerg 7, 2750 Ballerup, Danmark**
- (72) Opfinder: **VENDELBO, Allan Munk, c/o GN Hearing A/S, Att.: Group IPR, Lautrupbjerg 7, 2750 Ballerup, Danmark**
- (74) Fuldmægtig i Danmark: **Aera A/S, Niels Hemmingsens Gade 10, 1153 København K, Danmark**
- (54) Benævnelse: **Høreindretninger, brugertilbehørsindretninger og fremgangsmåde til opdatering af en
høreindretningskonfiguration**
- (56) Fremdragne publikationer:
WO-A1-2016/078710
WO-A2-2012/109640
US-A1- 2002 054 689
US-A1- 2016 173 278

DESCRIPTION

[0001] The present disclosure relates to a hearing system comprising a server device, a hearing device, and a user accessory device. In particular, the present disclosure relates to methods for updating the hearing device configuration, related hearing devices, and related user accessory devices.

BACKGROUND

[0002] Wireless communication to and from different entities of a hearing system has been increasing in continuation of the developments within wireless communication technology. However, the new technologies entail new challenges for the hearing aid manufacturers in order to secure communication in a hearing system. Wireless communication interfaces of a hearing system desirably use an open standard-based interface. However, this poses many challenges in terms of security. Further, a hearing device is a very small device with strict constraints in terms of computational power, memory space etc. US 20160173278 A1 describes a hearing device which includes: a processing unit configured to compensate for hearing loss of a user of the hearing device; and an interface; wherein the processing unit is configured to: receive a session request for a session via the interface, obtain and store a session key, encrypt the session key based on a hearing device key, send a session response comprising the encrypted session key, and receive session data in the session via the interface. WO201607871 A1 describes a hearing aid (10, 11) which has a memory (123) for storing personal settings for alleviating a hearing loss for the hearing aid user. A user account is created from an Internet enabled computer device (17) on a remote server (25), and the user account includes the personal settings for alleviating a hearing loss for the hearing aid user and personal information. A wireless connection is set up a between the hearing aid (10, 11) and the personal communication device (13), and the personal communication device (13) is identified as a gateway to the Internet for said hearing aid. The user grants access rights to a third party to modify data in a sub-set of the user account stored on the server (25). US 2002/0054689 A1 describes improved approaches to update existing hearing devices by downloading software resources over a network from a remote server to a local client. The software resources are then stored in the existing hearing devices, thereby upgrading the functionality or operation of the existing hearing devices.

SUMMARY

[0003] There is a need for hearing devices, user accessory devices, and methods that provide an improved and effective security supporting an updating of the hearing device configuration, e.g. a remote fitting or a remote fine-tuning of the hearing device. Further, there is a need for devices and methods reducing the risk that the hearing device performs an update using

configuration data being compromised by a third (unauthorized) party.

[0004] It is an object of this disclosure to provide a method, performed at a hearing device, for updating a hearing device configuration at the hearing device of a hearing system, according to claim 1.

[0005] This disclosure relates to a method performed at a user accessory device, for remote configuration of a hearing device in a hearing system. The method may be performed at a user application installed on the user accessory device. The hearing system comprises the hearing device associated with the user accessory device, the user accessory device, a fitting device, and a server device. The user accessory device is associated, paired, or coupled with the hearing device, such as wirelessly coupled. The method comprises receiving one or more of a configuration verification package, a configuration authentication package, and a configuration package from the server device. The configuration package comprises a configuration payload block and a control block (such as metadata). The method comprises determining if a verification criterion is fulfilled. The verification criterion is based at least on verifying one of the configuration verification package, the configuration authentication package, and the configuration package. The method comprises transmitting the configuration authentication package and/or the configuration package to the hearing device if the verification criterion is fulfilled.

[0006] This disclosure relates to a hearing device comprising a processor configured to compensate for a hearing loss of a user based on a hearing device configuration; an interface; and a memory unit. The hearing device is configured to perform the method according to claim 1.

[0007] This disclosure relates to a user application configured to be installed on a user accessory device of a hearing system. The user accessory device comprises a processing unit; a memory unit; and an interface. The user application, when installed on the user accessory device is configured to perform the method disclosed herein.

[0008] This disclosure relates to a user accessory device of a hearing system. The user accessory device comprises a processing unit; a memory unit; and an interface. The user accessory device is configured to perform the method disclosed herein.

[0009] It is an advantage of the present disclosure that the disclosed hearing device and the disclosed user accessory device support a secure remote configuration or remote tuning that is compliant with the limited computational power of the hearing device.

[0010] Thus, the present disclosure advantageously provides methods, related hearing devices, related user applications, and related user accessory devices that enable an effective and secure remote configuration of the hearing device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The above and other features and advantages of the present disclosure 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 a hearing system,

Fig. 2

is a flow diagram of an exemplary method performed at a hearing device according to this disclosure,

Fig. 3

is a flow diagram of an exemplary method performed at a user accessory device, or a user application installed thereon, according to this disclosure,

Fig. 4

schematically illustrates an exemplary configuration package, and an exemplary configuration verification package according to this disclosure,

Fig. 5

schematically illustrates an exemplary configuration authentication package according to this disclosure,

Fig. 6

schematically illustrates an exemplary hearing device according to this disclosure, and

Fig. 7

schematically illustrates an exemplary user accessory device according to this disclosure.

DETAILED DESCRIPTION

[0012] Various exemplary embodiments and details are described hereinafter, with reference to the figures when relevant. It should be noted that the figures may or may not be drawn to scale and that elements of similar structures or functions are represented by like reference numerals throughout the figures. 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 invention or as a limitation on the scope of the 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.

[0013] The present disclosure relates to enabling and securing a remote updating or configuring of a hearing device in a hearing system. The hearing system comprises a server

device, a hearing device, a user accessory device and a fitting device. The fitting device is controlled by a dispenser and is configured to determine the configuration data, such as fitting parameters. The server device may be controlled by the hearing device manufacturer. The server device may be a distributed server device, i.e. a server device with distributed processors. Namely, the methods, hearing devices, user accessory devices, and user applications disclosed herein enable a remote configuration of the hearing device by the fitting device, where the remote configuration is robust against security threats, vulnerabilities and attacks by implementing appropriate safeguards and countermeasures, such as security mechanisms, to protect against threats and attacks. The present disclosure relates to a method for updating a hearing device configuration, which is robust against replay attacks, unauthorized access, battery exhaustion attacks, and man-in-the-middle attacks.

[0014] The present disclosure addresses a situation that is encountered by dispensers and hearing device users. This can be illustrated in the following example. A hearing device user calls a dispenser (e.g. from home) and complains about the configuration or fitting done earlier at the professional dispenser's office. To avoid having the user come back to the dispenser's office for a configuration again, the inventors propose to have dispenser adjust certain configuration values (e.g. +3db gain at 1 kHz) in the office and send the resulting configuration package - or fine tuning package - to the hearing device or a user accessory having an application installed thereon to handle the hearing device. The hearing device user is able to use the application to download the configuration package and apply it to the hearing device. However, such a retrieval of the configuration package shall be secured, the configuration package shall be integrity protected, and the entire chain of processing leading to the installation of the configuration package on the hearing device shall be confidential, authenticated and integrity protected.

[0015] The present disclosure relates to hearing system communication between entities of a hearing system. The user accessory device forms an accessory device to the hearing device. The user accessory device is typically paired or wirelessly coupled to the hearing device. The hearing device may be a hearing aid, e.g. of the behind-the-ear (BTE) type, in-the-ear (ITE) type, in-the-canal (ITC) type, receiver-in-canal (RIC) type or receiver-in-the-ear (RITE) type. Typically, the hearing device system is in possession of and controlled by the hearing device user. The user accessory device may be a hand-held device, such as smartphone, a smartwatch, or a tablet computer.

[0016] As used herein the term "identifier" refers to a piece of data that is used for identifying, such as for categorizing, and/or uniquely identifying. The identifier may be in a form of a word, a number, a letter, a symbol, a list, an array or any combination thereof. For example, the identifier as a number may be in the form of an integer, such as unsigned integer, uint, with a length, or more, such as an array of unsigned integers. An identifier may have a length of several bytes. For example, a hearing device identifier may have a length of 20 bytes.

[0017] The present disclosure relates to a method performed at a hearing device, for updating a hearing device configuration at the hearing device of a hearing system, according to claim 1.

[0018] The configuration package comprises configuration data, such as data related to the hearing device. The data related to the hearing device may comprise hearing device settings and/or fitting parameters.

[0019] In one or more exemplary methods performed at the hearing device, the hearing system comprises a user accessory device. Receiving the configuration package and the configuration authentication package may comprise receiving the configuration package and the configuration authentication from the user accessory device or from a user application installed on the user accessory device. The user accessory device may have received the configuration package and the configuration authentication package from the fitting device and/or from the server device.

[0020] In one or more exemplary methods performed at the hearing device, determining if the update criterion is fulfilled comprises verifying the dispenser certificate, and the update criterion is not fulfilled if verifying the dispenser certificate fails. In other words, the update criterion is based on verifying the dispenser certificate included in the configuration authentication package and the update criterion is fulfilled if verifying the dispenser certificate succeeds. Verifying the dispenser certificate comprises verifying that the dispenser certificate is valid, and when it is verified that the dispenser certificate is valid, the exemplary method may comprise proceeding to updating the hearing device configuration based on the configuration package.

[0021] In one or more exemplary methods performed at the hearing device, verifying the dispenser certificate comprises decrypting the dispenser certificate using a certificate key. In other words, the configuration authentication package may comprise the dispenser certificate in encrypted form, which requires the hearing device to be configured to decrypt the received dispenser certificate using the certificate key. In one or more exemplary methods performed at the hearing device, verifying the dispenser certificate comprises deriving the certificate key based on keying material from a memory unit of the hearing device and/or material from the configuration authentication package. Deriving the certificate key may comprise obtaining a common secret from e.g. a memory unit of the hearing device, and calculating the certificate key based on the common secret. For example, obtaining the common secret may comprise retrieving the common secret from memory unit of the hearing device using a common secret identifier provided in the configuration authentication package and computing the certificate key based on the common secret and possibly a base key. Alternatively or additionally, obtaining the common secret may comprise retrieving keying material using an identifier provided in the configuration authentication package and computing the common secret based on the retrieved keying material and random data.

[0022] In claim 1 the configuration authentication package further comprises authentication data. Verifying the dispenser certificate comprises comparing one or more elements of the authentication data with corresponding elements of the dispenser certificate, and verifying the dispenser certificate fails if at least one elements of the authentication data does not match the corresponding element of the dispenser certificate. Stated differently, the update criterion may

not be fulfilled if at least one element of the authentication data does not match the corresponding element of the dispenser certificate, which results in the update not being triggered. Comparing one or more elements of the authentication data with corresponding elements of the dispenser certificate may comprise comparing one or more elements of the authentication data received in plain text with corresponding elements of the decrypted dispenser certificate. For example, the authentication data comprises a fitting type identifier received in plain text, and a fitting key identifier received in plain text while the decrypted dispenser certificate comprises a fitting type identifier and, a fitting key identifier. In this example, the hearing device compares the fitting type identifier received in plain text with the fitting type identifier of the decrypted dispenser certificate, and a fitting key identifier received in plain text with the fitting key identifier of the dispenser certificate. In this example, if the hearing device identifies a mismatch between the fitting type identifier received in plain text with the fitting type identifier of the decrypted dispenser certificate, and/or between a fitting key identifier received in plain text with the fitting key identifier of the dispenser certificate, the update criterion is not fulfilled and the update is aborted.

[0023] In one or more exemplary methods performed at the hearing device, verifying the dispenser certificate comprises determining if the fitting device and/or the dispenser is blacklisted, and verifying the dispenser certificate fails if the fitting device and/or the dispenser is blacklisted. For example, determining if the fitting device and/or the dispenser is blacklisted is performed using a blacklist comprising an identifier of a fitting device and/or the dispenser that has been excluded from the hearing system. The blacklist serves as a mitigation tool, for preventing attacks using lost credentials. The one or more exemplary methods performed at the hearing device may comprise verifying a certificate type identifier of the dispenser certificate. Certain hearing device can only accept configuration package from certain types of fitting devices.

[0024] In one or more exemplary methods performed at the hearing device, updating the hearing device configuration based on the configuration package comprises decrypting the configuration package using a configuration session key. For example, updating the hearing device configuration based on the configuration package may comprise deriving the configuration session key based on a base key stored in the memory unit of the hearing device. The base key may be shared or common with the server device.

[0025] In one or more exemplary methods performed at the hearing device, the configuration package comprises a configuration data integrity indicator, and updating the hearing device configuration comprises verifying the configuration data integrity indicator based on the configuration package, and terminating or aborting the update of the hearing device configuration based on the configuration package if the verification of the configuration data integrity indicator fails. The configuration data integrity indicator may be computed over the configuration data, e.g. using SHA1 or SHA2. If the verification of the configuration data integrity indicator succeeds, the update proceeds to storing the configuration data comprised in the configuration package. This supports protecting the hearing device from accepted configuration data that has been tampered with.

[0026] In one or more exemplary methods performed at the hearing device, the hearing device is a hearing aid, configured to compensate for hearing loss of a user.

[0027] This disclosure relates to a hearing device comprising a processor configured to compensate for a hearing loss of a user based on a hearing device configuration; an interface; and a memory unit. The hearing device is configured to perform the method disclosed herein.

[0028] This disclosure relates to a method performed at a user accessory device, for remote configuration of a hearing device in a hearing system. The method may be performed at a user application installed on the user accessory device. The user application is, when installed on the user accessory device, configured to perform the method disclosed herein as performed at the user accessory device. The hearing system comprises the hearing device associated with the user accessory device, the user accessory device, a fitting device, and a server device. The user accessory device is associated, paired, or coupled with the hearing device, such as wirelessly coupled. The method comprises receiving one or more of a configuration verification package, a configuration authentication package, and a configuration package from the server device, e.g. via communication link 21. The configuration package comprises a configuration payload block and a control block (such as metadata).

[0029] The method comprises determining if a verification criterion is fulfilled. The verification criterion is based at least on verifying one of the configuration verification package, the configuration authentication package, and the configuration package.

[0030] The method comprises transmitting the configuration authentication package and/or the configuration package to the hearing device, via e.g. a wireless communication link if the verification criterion is fulfilled. The method may comprise transmitting the configuration package to the hearing device only if or after the configuration authentication package is successfully verified. The method may comprise omitting to transmit any of the configuration authentication package and the configuration package to the hearing device if the verification criterion is not fulfilled.

[0031] In one or more exemplary methods performed at the user accessory device, the configuration authentication package comprises a second digital signature; and the verification criterion comprises a first verification criterion based on verifying the second digital signature. In one or more exemplary methods performed at the user accessory device, the verification criterion is not fulfilled if the first verification criterion is not fulfilled. In other words, the verification criterion may be fulfilled if the first verification criterion is fulfilled. Verifying the second digital signature may be performed using a configuration public key, which may be stored in the memory unit of the user accessory device.

[0032] In one or more exemplary methods performed at the user accessory device, the configuration verification package comprises an integrity indicator set and/or a first digital signature, and the verification criterion comprises a second verification criterion comprising a

second primary verification criterion and a second secondary verification criterion. The integrity indicator set may comprise a first integrity indicator, a second integrity indicator, and optionally a third integrity indicator. The second primary verification criterion may be based on verifying the first digital signature, such as using the configuration public key. The second secondary verification criterion may be based on verifying the integrity indicator set, e.g. based on the configuration payload block, and the control block, such as by calculating a first configuration data integrity indicator over the configuration payload block and comparing the calculated first configuration data integrity indicator with the received first integrity indicator of the integrity indicator set and/or by calculating a second configuration data integrity indicator over the control block and comparing the calculated second configuration data integrity indicator with the received second integrity indicator of the integrity indicator set. The verification criterion may not be fulfilled if the second primary verification criterion or the second secondary verification criterion is not fulfilled. In other words, the verification criterion may be fulfilled if the second primary verification criterion and the second secondary verification criterion are fulfilled.

[0033] In one or more exemplary methods performed at the user accessory device, the configuration verification package, and/or the configuration authentication package, comprise a hearing device identifier and/or an address identifier. The verification criterion may comprise a third verification criterion based on the received hearing device identifier corresponding to a hearing device identifier of the hearing device associated with the user accessory, such as based on verifying whether the received hearing device identifier corresponds to the hearing device identifier of the hearing device associated with the user accessory. Alternatively or additionally, the verification criterion may comprise a fourth verification criterion based on the received address identifier corresponding to an address identifier of the hearing device associated with the user accessory, e.g. based on verifying whether the received address identifier corresponds to an address identifier of the hearing device associated with the user accessory. The verification criterion may not be fulfilled if the third verification criterion or the fourth verification criterion is not fulfilled. In other words, the verification criterion may be fulfilled if the third verification criterion and the fourth verification criterion are fulfilled.

[0034] In one or more exemplary methods performed at the user accessory device, the verification criterion is not fulfilled if the first verification criterion, or the second primary verification criterion, or the second secondary verification criterion, or the third verification criterion or the fourth verification criterion is not fulfilled.

[0035] In one or more exemplary methods performed at the user accessory device, the verification criterion is fulfilled if the first verification criterion, and the second primary verification criterion, and the second secondary verification criterion, and the third verification criterion and the fourth verification criterion are fulfilled.

[0036] This disclosure relates to a user application configured to be installed on a user accessory device of a hearing system. The user accessory device comprises a processing unit; a memory unit; and an interface. The user application, when installed on the user accessory device, is configured to perform the method disclosed herein.

[0037] This disclosure relates to a user accessory device of a hearing system. The user accessory device comprises a processing unit; a memory unit; and an interface. The user accessory device is configured to perform the method disclosed herein.

[0038] Fig. 1 shows an exemplary hearing system 1. The hearing system 1 comprises a server device 4, a fitting device 2 and a hearing device 8 and an accessory device 10. It may be envisaged that the hearing device 8 and the accessory device 10 form part of a hearing device system 6. The user accessory device 10 is a handheld device such as smartphone configured to wirelessly communicate with the hearing device 8. A user application 12 is installed on the user accessory device 10. The user application may be for controlling the hearing device 8 and/or assisting a hearing device user wearing/using the hearing device 8. In one or more exemplary user applications, the user application 12 is configured to transfer configuration data (e.g. hearing device settings or fitting parameters), to the hearing device. The user accessory device 10 comprises a processing unit 36, a memory unit 38, and an interface 40. The user application 12 may be installed in the memory unit 38 of the user accessory device 10.

[0039] The hearing device 8 comprises an antenna 24 and a radio transceiver 26 coupled to the antenna 24 for receiving/transmitting wireless communication including first communication link 20. The hearing device 8 comprises a set of microphones comprising a first microphone 28 and optionally a second microphone 30 for provision of respective first and second microphone input signals. The hearing device 8 may be a single-microphone hearing device. The hearing device 8 comprises a memory unit (not shown) connected to the processor 32, wherein configuration data, e.g. configuration or hearing device settings are stored in the memory unit.

[0040] The hearing device 8 comprises a processor 32 connected to the transceiver 26 and microphones 28, 30 for receiving and processing input signals. The processor 32 is configured to compensate for a hearing loss of a user based on hearing device settings and to provide an electrical output signal based on the input signals. A receiver 34 converts the electrical output signal to an audio output signal to be directed towards an eardrum of the hearing device user.

[0041] The fitting device 2 is capable of communicating with the server device 4 through communication link 22, and with the hearing device system 6 through communication link 23. In an embodiment, the fitting device is configured to communicate with the accessory device 10 via communication link 23. The hearing device 8 is capable of communicating with the user accessory device 10 through communication link 20. The user accessory device 10 may be configured to communication with the server device 4 via communication link 21. A communication link may comprise a wireless communication link and/or a wired communication link.

[0042] Fig. 2 shows a flow diagram of an exemplary method 100 performed at a hearing device (such as hearing device 8 of Fig. 1) according to this disclosure. The method 100 aims at updating a hearing device configuration at the hearing device of a hearing system, e.g. based on receiving a configuration package that has been prepared by a dispenser remotely.

The method 100 comprises receiving S101 a configuration package and a configuration authentication package, the configuration authentication package comprising a dispenser certificate. The method 100 comprises determining S102 if an update criterion is fulfilled. The update criterion is based on verifying the configuration authentication package. The method 100 comprises updating S103 the hearing device configuration based on the configuration package if the update criterion is fulfilled.

[0043] In one or more exemplary methods, the hearing system comprises a user accessory device. Receiving S101 the configuration package and the configuration authentication package may comprise receiving S101a the configuration package and the configuration authentication from the user accessory device or from a user application installed on the user accessory device, via communication link 20.

[0044] In one or more exemplary methods performed at the hearing device, determining S102 if the update criterion is fulfilled comprises verifying S102a the dispenser certificate, and the update criterion is not fulfilled if verifying the dispenser certificate fails.

[0045] In one or more exemplary methods performed at the hearing device, verifying S102a the dispenser certificate comprises decrypting S102aa the dispenser certificate using a certificate key. In one or more exemplary methods performed at the hearing device, verifying S102a the dispenser certificate comprises deriving S102ab the certificate key based on keying material from a memory unit of the hearing device and/or material from the configuration authentication package. Deriving S102ab the certificate key may comprise obtaining a common secret from e.g. a memory unit of the hearing device, and calculating the certificate key based on the common secret. For example, obtaining the common secret may comprise retrieving the common secret from memory unit of the hearing device using a common secret identifier provided in the configuration authentication package and computing the certificate key based on the common secret and possibly a base key. Alternatively or additionally, obtaining the common secret may comprise retrieving keying material using an identifier provided in the configuration authentication package and computing the common secret based on the retrieved keying material and random data.

[0046] In claim 1 the configuration authentication package further comprises authentication data. Verifying S102a the dispenser certificate comprises comparing S102ac one or more elements of the authentication data with corresponding elements of the dispenser certificate, and verifying the dispenser certificate fails if at least one elements of the authentication data does not match the corresponding element of the dispenser certificate. Comparing S102ac one or more elements of the authentication data with corresponding elements of the dispenser certificate may comprise comparing one or more elements of the authentication data received in plain text with corresponding elements of the decrypted dispenser certificate.

[0047] In one or more exemplary methods performed at the hearing device, verifying S102a the dispenser certificate comprises determining S102ad if the fitting device and/or the dispenser is blacklisted, and verifying the dispenser certificate fails if the fitting device and/or

the dispenser is blacklisted. For example, determining S102ad if the fitting device and/or the dispenser is blacklisted is performed using a blacklist comprising an identifier of a fitting device and/or the dispenser that has been excluded from the hearing system.

[0048] In one or more exemplary methods performed at the hearing device, updating S103 the hearing device configuration based on the configuration package comprises decrypting S103a the configuration package using a configuration session key. For example, updating S103 the hearing device configuration based on the configuration package may comprise deriving S103b the configuration session key based on a base key stored in the memory unit of the hearing device. The base key may be shared or common with the server device.

[0049] In one or more exemplary methods performed at the hearing device, the configuration package comprises a configuration data integrity indicator, and updating S103 the hearing device configuration comprises verifying S103c the configuration data integrity indicator based on the configuration package, and terminating or aborting the update of the hearing device configuration based on the configuration package if the verification of the configuration data integrity indicator fails.

[0050] In one or more exemplary methods performed at the hearing device, method 100 may comprise storing and/or applying the configuration data to the hearing device when the update criterion is fulfilled.

[0051] Fig. 3 shows a flow diagram of an exemplary method 200 performed at a user accessory device (such as device 10 of Fig. 1) or at a user application installed on the user accessory device according to this disclosure. Method 200 method aims at supporting a remote configuration of a hearing device in a hearing system. The method may be performed at a user application installed on the user accessory device. The user application is, when installed on the user accessory device, configured to perform the method 200. Method 200 comprises receiving S201 at the hearing device one or more of a configuration verification package, a configuration authentication package, and a configuration package from the server device 4, e.g. via the communication link 21. The configuration package comprises a configuration payload block and a control block (such as metadata). One or more of a configuration verification package, a configuration authentication package, and a configuration package may be received at the user accessory device via the server device 4 from the fitting device 2, e.g. using the communication links 21 and 22.

[0052] Method 200 comprises determining S202 if a verification criterion is fulfilled. The verification criterion is based at least on verifying S202a one of the configuration verification package, the configuration authentication package, and the configuration package.

[0053] Method 200 comprises transmitting S203 the configuration authentication package and/or the configuration package to the hearing device, e.g. via communication link 20, if the verification criterion is fulfilled. The method may comprise transmitting the configuration package to the hearing device only if or after the configuration authentication package is

successfully verified. The method may comprise omitting to transmit any of the configuration authentication package and the configuration package to the hearing device if the verification criterion is not fulfilled.

[0054] In one or more exemplary methods performed at the user accessory device, the configuration authentication package comprises a second digital signature; and the verification criterion comprises a first verification criterion based on verifying S202a the second digital signature. In one or more exemplary methods performed at the user accessory device, the verification criterion is not fulfilled if the first verification criterion is not fulfilled.

[0055] In one or more exemplary methods performed at the user accessory device, the configuration verification package comprises an integrity indicator set and/or a first digital signature, and the verification criterion comprises a second verification criterion comprising a second primary verification criterion and a second secondary verification criterion. The integrity indicator set may comprise a first integrity indicator, a second integrity indicator, and optionally a third integrity indicator. The second primary verification criterion may be based on verifying S202b the first digital signature, such as using the configuration public key. The second secondary verification criterion may be based on verifying S202c the integrity indicator set, e.g. based on the configuration payload block, and the control block, by e.g. calculating a first configuration data integrity indicator over the configuration payload block and comparing the calculated first configuration data integrity indicator with the received first integrity indicator of the integrity indicator set and/or by calculating a second configuration data integrity indicator over the control block and comparing the calculated second configuration data integrity indicator with the received second integrity indicator of the integrity indicator set. The verification criterion may not be fulfilled if the second primary verification criterion or the second secondary verification criterion is not fulfilled.

[0056] In one or more exemplary methods performed at the user accessory device, the configuration verification package, and/or the configuration authentication package comprise a hearing device identifier and/or an address identifier. The verification criterion may comprise a third verification criterion based on the received hearing device identifier corresponding to a hearing device identifier of the hearing device associated with the user accessory, such as based on verifying S202d whether the received hearing device identifier corresponds to the hearing device identifier of the hearing device associated with the user accessory. Alternatively or additionally, the verification criterion may comprise a fourth verification criterion based on the received address identifier corresponding to an address identifier of the hearing device associated with the user accessory, e.g. based on verifying S202e whether the received address identifier corresponds to an address identifier of the hearing device associated with the user accessory. The verification criterion may not be fulfilled if the third verification criterion or the fourth verification criterion is not fulfilled.

[0057] Fig. 4 schematically illustrates an exemplary configuration package 402, and an exemplary configuration verification package 412 according to this disclosure.

[0058] The configuration package 402 comprising configuration package data 403. The configuration package data 403 comprises a configuration payload block 404 and a control block 406. The configuration package 402 is generated, by the fitting device in collaboration with the server device, based on configuration data 408 for the hearing device. The configuration package data 403 comprises the configuration data 408, which is the actual fitting parameters or hearing device setting parameters, which are used to configure the hearing device. The configuration data 408 may be included in the configuration package data 403 in encrypted form using a configuration keying material comprising a configuration key. The configuration package data 403 comprises a configuration data integrity indicator 409 computed over the configuration data 408, and included in the configuration package data 403. The configuration payload block 404 comprises the configuration data 408 and the configuration data integrity indicator 409, which are optionally in encrypted form as indicated by the dashed box in Fig. 4. The control block 406 comprises headers, length of the configuration data and/or metadata. The fitting device may be configured to generate the configuration package by encrypting, e.g. using the session key, the configuration package data 403, i.e. the configuration payload block 404 and the control block 406. The configuration package is generated at the fitting device.

[0059] The configuration verification package 412 is generated at the server device. The configuration verification package 412 comprises a set of integrity indicators, such as a first integrity indicator 414, a second integrity indicator 416. The server receives a configuration package 402 from the fitting device. The configuration package 402 comprises a configuration payload block 404 and a control block 406. The server generates a configuration block 419 by computing a first integrity indicator 414 based on the configuration payload block 404 and a second integrity indicator 416 based on the control block 406, and by including the first integrity indicator 414 and the second integrity indicator 416 into the configuration block 419. The server device signs the configuration verification package 412 using a configuration private key. The configuration verification package 412 comprises a first digital signature 418. The configuration verification package 412 is used at the user accessory device to verify the configuration package 402 and/or the configuration authentication package 502 before passing the configuration package 402 and/or the configuration authentication package 502 to the hearing device.

[0060] Fig. 5 schematically illustrates an exemplary configuration authentication package 502 according to this disclosure. The configuration authentication package 502 is generated by the server device. The configuration authentication package 502 comprises a configuration authentication material 504. The configuration authentication material 504 comprises a dispenser certificate 506, which may be encrypted using a certificate key. The server obtains a second digital signature 508 over the configuration authentication material 504 using a configuration private key that is stored in the server device and used for configuration purposes. The configuration public key and the certificate key are known to the hearing device. The configuration authentication package 502 comprises the second digital signature 508.

[0061] The configuration package 402 and the configuration authentication package 502 are

received and processed by the hearing device. The configuration authentication package 502 is generated by the server device so that the hearing device can verify the integrity of the configuration data. The configuration authentication package 502 is used at the hearing device to authenticate the configuration package 402 that actually comprises the fitting parameters or configuration data to be installed on the hearing device.

[0062] The configuration verification package 412 is used at the user accessory device to verify the configuration package 402 and/or the configuration authentication package 502. In other words, the dispenser or the fitting device uses the server device to create a configuration authentication package 502 for a specific hearing device, i.e. that can be verified by the specific hearing device. The configuration authentication package 502 and the configuration package data in the configuration package 402 are generated so that the hearing device is able to verify that the configuration package 402 comes from a legitimate dispenser or legitimate fitting device and that the configuration data in the configuration package 402 has not been tampered with nor disclosed by any other party because configuration data is private data that can be used to perform denial of service attack or battery exhaustion attacks on the hearing device.

[0063] Fig. 6 schematically illustrates an exemplary hearing device 8 according to this disclosure. The hearing device 8 comprises a processor 32 configured to compensate for a hearing loss of a user based on a hearing device configuration; an interface 33; and a memory unit 35. The interface 33 may comprise an antenna (such as antenna 24 of Fig. 1) and a radio transceiver (such as radio transceiver 26 of Fig. 1) coupled to the antenna for receiving/transmitting wireless communication, to and from a user accessory device, and optionally from any of a fitting device and a server device. The hearing device 8 is configured to perform the method 100 disclosed herein in Fig. 2.

[0064] The hearing device 8 or the interface 33 is configured to receive, e.g. from a user accessory device or a user application installed thereon, a configuration package and a configuration authentication package, the configuration authentication package comprising a fitting device certificate. The hearing device 8 or the processor 32 is configured to determine if an update criterion is fulfilled, wherein the update criterion is based on verifying the configuration authentication package; and to update the hearing device configuration based on the configuration package if the update criterion is fulfilled.

[0065] The processor 32 may be configured to verify the dispenser certificate, and to determine that the update criterion is not fulfilled if verifying the dispenser certificate fails.

[0066] The processor 32 may be configured to decrypt the dispenser certificate using a certificate key. In one or more exemplary hearing devices, The processor 32 may be configured to verify the dispenser certificate by deriving the certificate key based on keying material from a memory unit of the hearing device and/or material from the configuration authentication package. The processor 32 may be configured to obtain a common secret from e.g. a memory unit of the hearing device and calculating the certificate key based on the

common secret.

[0067] The configuration authentication package further comprises authentication data. The processor 32 is configured to verify the dispenser certificate by comparing one or more elements of the authentication data with corresponding elements of the dispenser certificate, and to determine that verifying the dispenser certificate fails if at least one elements of the authentication data does not match the corresponding element of the dispenser certificate. The processor 32 may be configured to compare one or more elements of the authentication data with corresponding elements of the dispenser certificate by comparing one or more elements of the authentication data received in plain text with corresponding elements of the decrypted dispenser certificate.

[0068] The processor 32 may be configured to verify the dispenser certificate by determining if the fitting device and/or the dispenser is blacklisted, and to determine that verifying the dispenser certificate fails if the fitting device and/or the dispenser is blacklisted. For example, determining if the fitting device and/or the dispenser is blacklisted is performed using a blacklist comprising an identifier of a fitting device and/or the dispenser that has been excluded from the hearing system.

[0069] The processor 32 may be configured to update the hearing device configuration based on the configuration package by decrypting the configuration package using a configuration session key, such as by deriving the configuration session key based on a base key stored in the memory unit 35 of the hearing device. The base key may be shared or common with the server device.

[0070] In one or more exemplary hearing devices, the configuration package comprises a configuration data integrity indicator, and the processor 32 may be configured to update the hearing device configuration based on the configuration package by verifying the configuration data integrity indicator based on the configuration package, and by terminating or aborting the update of the hearing device configuration based on the configuration package if the verification of the configuration data integrity indicator fails.

[0071] The processor 32 may be configured to update the hearing device configuration based on the configuration package by storing the configuration data in the memory unit 35 in order to apply the stored configuration data to the hearing device for a configuration update.

[0072] The hearing device 8 or the processing unit 32 is arranged to execute methods for updating the hearing device configuration as disclosed herein. The hearing device 8 or the processing unit 32 may further comprise a number of optional functional modules, such as any of a determine module 32a configured to perform steps S102 and optionally S102a, S102aa-ad, and an update module 32b configured to perform step S103. The functionality of each functional module 32a-b is disclosed in the context of which the functional modules 32a-b may be used in Fig. 2 and accompanying text. In general terms, each functional module 32a-b may be implemented in hardware or in software. Preferably, one, more, or all functional modules

32a-b may be implemented by the processing module 32, possibly in cooperation with functional units 35 and 33. The processing module 32 may thus be arranged to fetch instructions from the memory module 35 as provided by a functional module 32a-c and to execute these instructions, thereby performing any steps as disclosed herein in Fig. 2.

[0073] Fig. 7 schematically illustrates an exemplary user accessory device 10 according to this disclosure. The user accessory device 10 comprises a processing unit 36, a memory unit 38, and an interface 40. The user application 12 may be installed in the memory unit 38 of the user accessory device 10.

[0074] The user accessory device 10 or the interface 40 is configured to receive one or more of a configuration verification package, a configuration authentication package, and a configuration package from the server device. The configuration verification package may comprise an integrity indicator set and a first digital signature. The configuration authentication package may comprise a second digital signature. The configuration package comprises a configuration payload block and a control block.

[0075] The user accessory device 10 or the processing unit 36 is configured to determine if a verification criterion is fulfilled, wherein the verification criterion is based at least on one of the configuration verification package, the configuration authentication package, and the configuration package.

[0076] The user accessory device 10 or the interface 40 is configured to transmit the configuration authentication package and/or the configuration package to the hearing device, e.g. via communication link 20, if the verification criterion is fulfilled.

[0077] In one or more exemplary user accessory devices, the configuration authentication package comprises a second digital signature; and the verification criterion comprises a first verification criterion based on verifying the second digital signature using the processing unit 36. In one or more exemplary user accessory devices, the verification criterion is not fulfilled if the first verification criterion is not fulfilled.

[0078] In one or more exemplary user accessory devices, the configuration verification package comprises an integrity indicator set and/or a first digital signature, and the verification criterion comprises a second verification criterion comprising a second primary verification criterion and a second secondary verification criterion. The integrity indicator set may comprise a first integrity indicator, a second integrity indicator and optionally a third integrity indicator. The second primary verification criterion may be based on verifying the first digital signature using the processing unit 36, such as using the configuration public key. The second secondary verification criterion may be based on verifying the integrity indicator set using the processing unit 36, e.g. based on the configuration payload block and the control block, by e.g. calculating a first configuration data integrity indicator over the configuration payload block and comparing the calculated first configuration data integrity indicator with the received first integrity indicator of the integrity indicator set and/or by calculating a second configuration data

integrity indicator over the control block and comparing the calculated second configuration data integrity indicator with the received second integrity indicator of the integrity indicator set. The verification criterion may not be fulfilled if the second primary verification criterion or the second secondary verification criterion is not fulfilled.

[0079] In one or more exemplary user accessory devices, the configuration verification package and/or the configuration authentication package comprise a hearing device identifier and/or an address identifier. The verification criterion may comprise a third verification criterion based on the received hearing device identifier corresponding to a hearing device identifier of the hearing device associated with the user accessory, such as based on verifying using the processing unit 36 whether the received hearing device identifier corresponds to the hearing device identifier of the hearing device associated with the user accessory. Alternatively or additionally, the verification criterion may comprise a fourth verification criterion based on the received address identifier corresponding to an address identifier of the hearing device associated with the user accessory, e.g. based on verifying using the processing unit 36 whether the received address identifier corresponds to an address identifier of the hearing device associated with the user accessory. The verification criterion may not be fulfilled if the third verification criterion or the fourth verification criterion is not fulfilled.

[0080] The user accessory device 10 or the processing unit 36 is arranged to execute methods for remote configuration of the hearing device 8 as disclosed herein (e.g. in Fig. 3). The user accessory device 10 or the processing unit 36 may further comprise a number of optional functional modules, such as any of a determine module 36a configured to perform steps S202 and optionally steps S202a-e. The functionality of module 36a is disclosed in the context of which the functional modules 36a may be used in Fig. 3 and accompanying text. In general terms, functional module 36a may be implemented in hardware or in software. Preferably, functional module 36a may be implemented by the processing module 36, possibly in cooperation with functional units 38 and 40. The processing module 36 may thus be arranged to fetch instructions from the memory module 38 as provided by a functional module 32a and to execute these instructions, thereby performing any steps as disclosed herein in Fig. 3.

[0081] 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.

[0082] 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 scope of the claimed invention.

LIST OF REFERENCES

[0083]

- 1 hearing system
- 2 fitting device
- 4 server device
- 6 hearing device system
- 8 hearing device
- 10 user accessory device
- 12 user application
- 20 communication link between user accessory device and hearing device
- 21 communication link between server device and user accessory device
- 22 communication link between fitting device and server device
- 23 communication link between fitting device and hearing device system
- 24 antenna
- 26 radio transceiver
- 28 first microphone
- 30 second microphone
- 32 processor
- 32a determine module
- 32b update module
- 33 interface

34	receiver
35	memory unit
36	processing unit
36a	determine module
38	memory unit
40	interface
100	method performed in the hearing device
200	method performed in the user accessory device or the user application
402	configuration package
403	configuration package data
404	configuration payload block
406	configuration control block
408	configuration data
409	configuration data integrity indicator
412	configuration verification package
414	first integrity indicator
416	second integrity indicator
418	first digital signature
419	configuration block
502	configuration authentication package
504	configuration authentication material
506	dispenser certificate

508

second digital signature

REFERENCES CITED IN THE DESCRIPTION

Cited references

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

- US20160173278A1 [0002]
- WO201607871A1 [0002]
- US20020054689A1 [0002]

Høreindretninger, brugertilbehørsindretninger og fremgangsmåde til opdatering af en høreindretningskonfiguration

PATENTKRAV

5

1. Fremgangsmåde, udført ved en høreindretning (8), til opdatering af en høreindretningskonfiguration ved høreindretningen (8) af et høresystem (1), hvilket høresystem (1) omfatter høreindretningen (8), en tilpasningsindretning (2), der er konfigureret til at blive styret af en dispenser, og en serverindretning (4), **kendetegnet ved, at** fremgangsmåden omfatter:

10

- modtagelse (S101) af en konfigurationspakke (402) og en konfigurationsgodkendelsespakke (502), hvilken konfigurationsgodkendelsespakke (502) omfatter et dispensercertifikat (506) og godkendelsesdata,

15

- bestemmelse (S102) af, hvorvidt et opdateringskriterium er opfyldt, hvor opdateringskriteriet er baseret på verificering af det dispensercertifikat, der er omfattet af konfigurationsgodkendelsespakken (502), hvor verificering (S102a) af dispensercertifikatet (506) omfatter:

- dekryptering (S102aa) af dispensercertifikatet (506) under anvendelse af en certifikatnøgle, og

20

- sammenligning (S102ac) af et eller flere elementer af godkendelsesdataene med tilsvarende elementer af det dekrypterede dispensercertifikat, og hvor verificering af dispensercertifikatet (506) mislykkes, hvis mindst ét eller flere elementer af godkendelsesdataene ikke matcher det tilsvarende element af det dekrypterede dispensercertifikat,

25

- opdatering (S103) af høreindretningskonfigurationen baseret på konfigurationspakken (402), hvis opdateringskriteriet er opfyldt.

2. Fremgangsmåde ifølge krav 1, hvor høresystemet (1) omfatter en brugertilbehørsindretning (10), og hvor modtagelse (S101) af konfigurationspakken (402) og konfigurationsgodkendelsespakken (502) omfatter modtagelse (S101a) af

konfigurationspakken (402) og konfigurationsgodkendelsespakken (502) fra bruger-tilbehørsindretningen (10) eller fra en brugerapplikation (12), der er installeret på brugertilbehørsindretningen (10).

5 3. Fremgangsmåde ifølge et hvilket som helst af kravene 1-2, hvor bestemmelse (S102) af, hvorvidt opdateringskriteriet er opfyldt, omfatter verificering (S102a) af dispenser-
certifikatet (506), hvor opdateringskriteriet ikke er opfyldt, hvis verificering af
dispensercertifikatet (506) mislykkes.

10 4. Fremgangsmåde ifølge et hvilket som helst af kravene 1-3, hvor
sammenligning (S102ac) af et eller flere elementer af godkendelsesdataene med
tilsvarende elementer af dispensercertifikatet (506) omfatter sammenligning af et eller
flere elementer af godkendelsesdataene, der er modtaget i ren tekst, med tilsvarende
elementer af det dekrypterede dispensercertifikat.

15 5. Fremgangsmåde ifølge et hvilket som helst af kravene 1-4, hvor verificering (S102a)
af dispensercertifikatet (506) omfatter bestemmelse (S102ad) af, hvorvidt tilpasnings-
indretningen (2) og/eller dispenserens sortlistet, og hvor verificering af dispenser-
certifikatet (506) mislykkes, hvis tilpasningsindretningen og/eller dispenserens
sortlistet.

20 6. Fremgangsmåde ifølge et hvilket som helst af kravene 1-5, hvor opdatering (S103)
af høreindretningskonfigurationen baseret på konfigurationspakken (402) omfatter
dekryptering (S103a) af konfigurationspakken (402) under anvendelse af en
konfigurationssessionsnøgle.

25 7. Fremgangsmåde ifølge et hvilket som helst af kravene 1-6, hvor konfigurations-
pakken (402) omfatter en konfigurationsdataintegritetsindikator, og hvor
opdatering (S103) af høreindretningskonfigurationen omfatter verificering (S103c) af
konfigurationsdataintegritetsindikatoren baseret på konfigurationspakken (402), og
afslutning af opdateringen af høreindretningskonfigurationen baseret på konfigurations-
pakken (402), hvis verifikation af konfigurationsdataintegritetsindikatoren mislykkes.

8. Fremgangsmåde ifølge et hvilket som helst af kravene 1-7, hvor høreindretningen (8)
er et høreapparat.

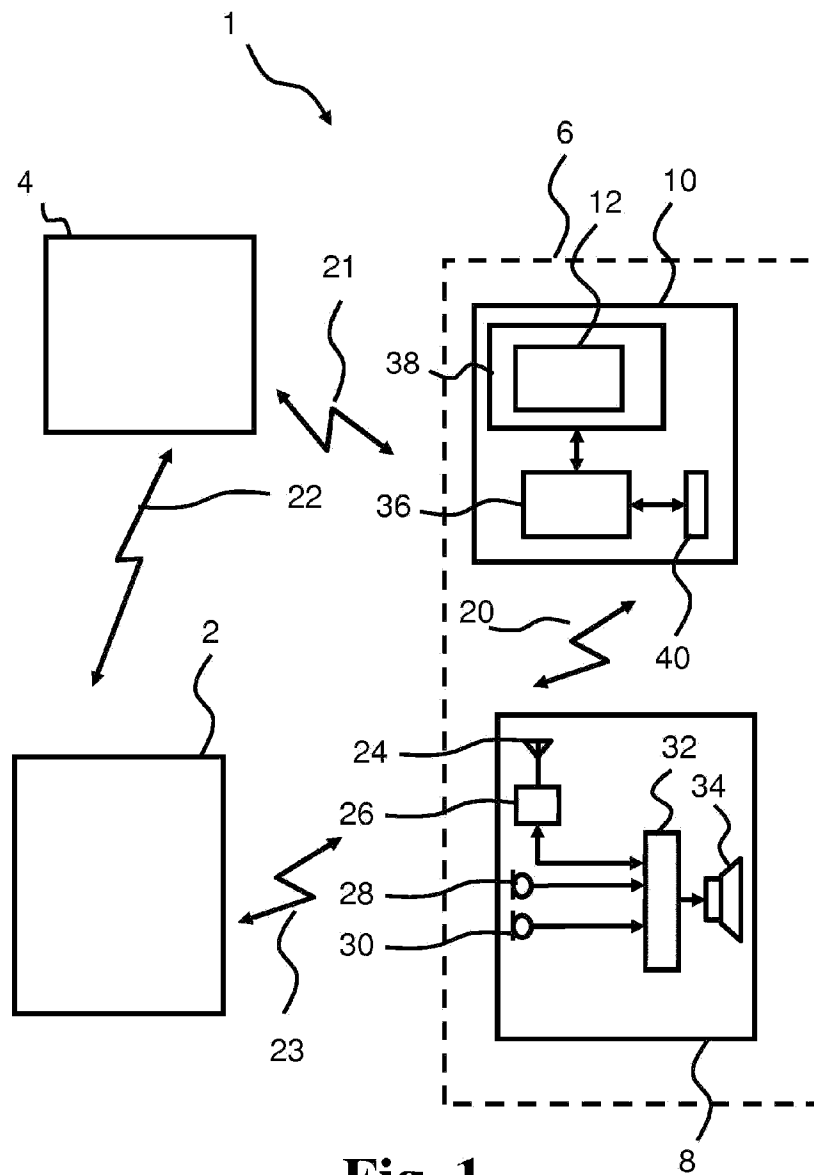
30 9. Høreindretning (8), der omfatter:

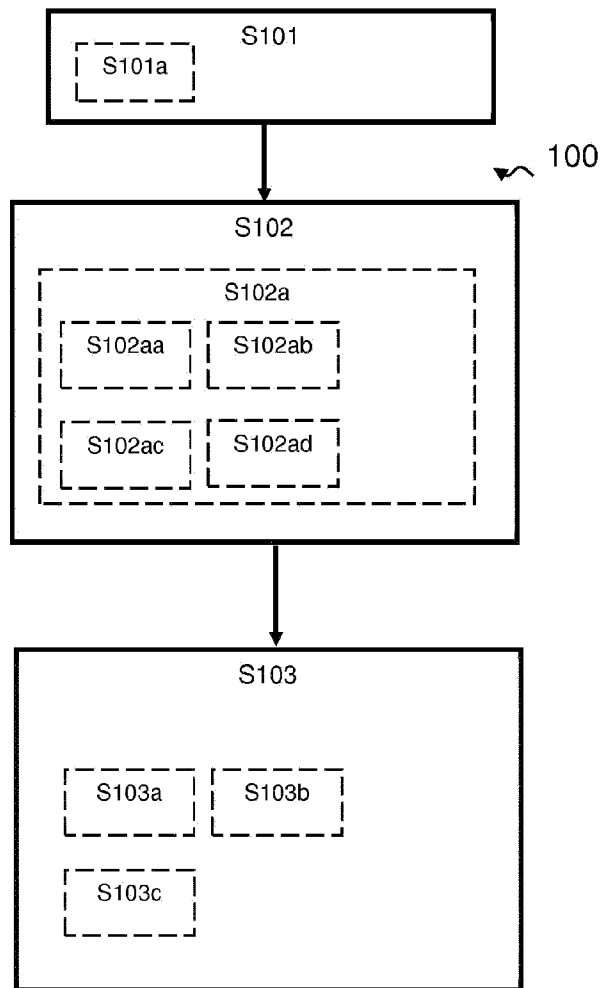
- en processor (32), som er konfigureret til at kompensere for et høretab hos en
bruger, baseret på en høreindretningskonfiguration,

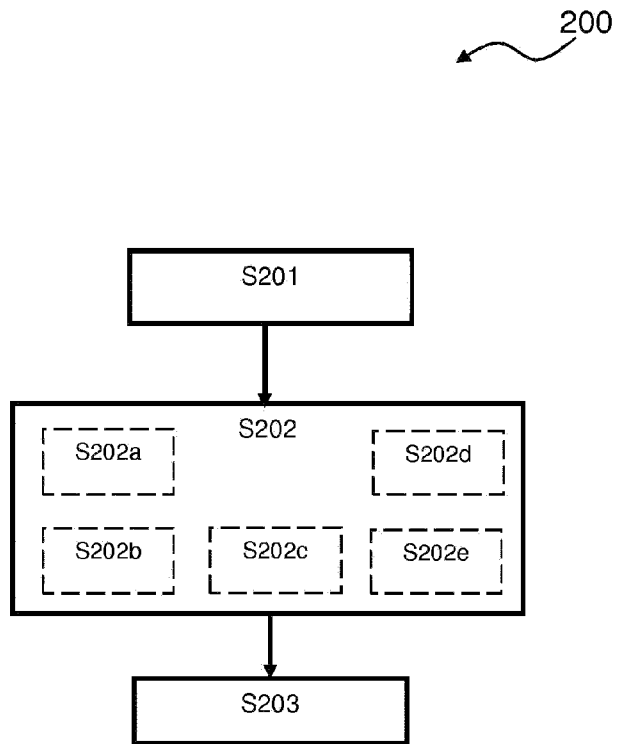
- en grænseflade (33), og
- en hukommelsesenhed (35),

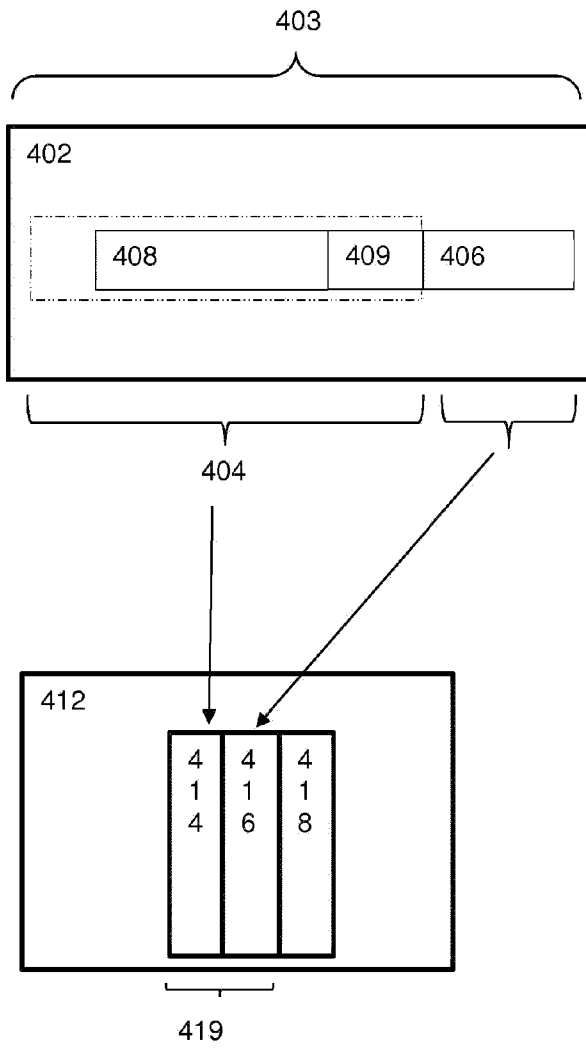
hvor høreindretningen (8) er konfigureret til at udføre fremgangsmåden ifølge et hvilket som helst af kravene 1 til 8.

DRAWINGS

**Fig. 1**

**Fig. 2**

**Fig. 3**

**Fig. 4**

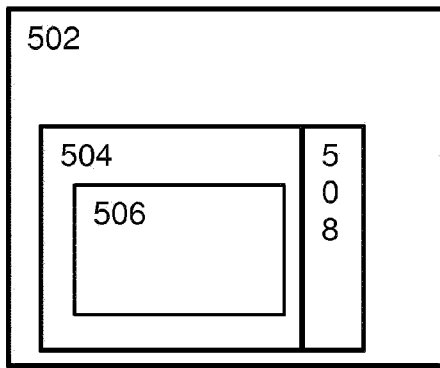
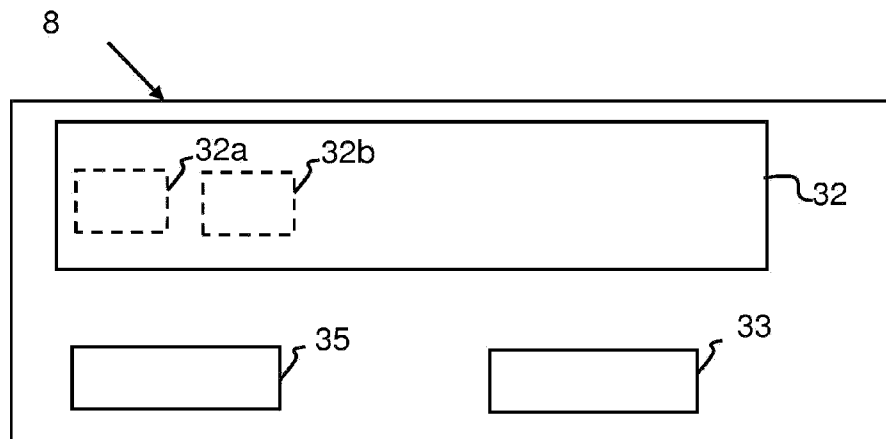
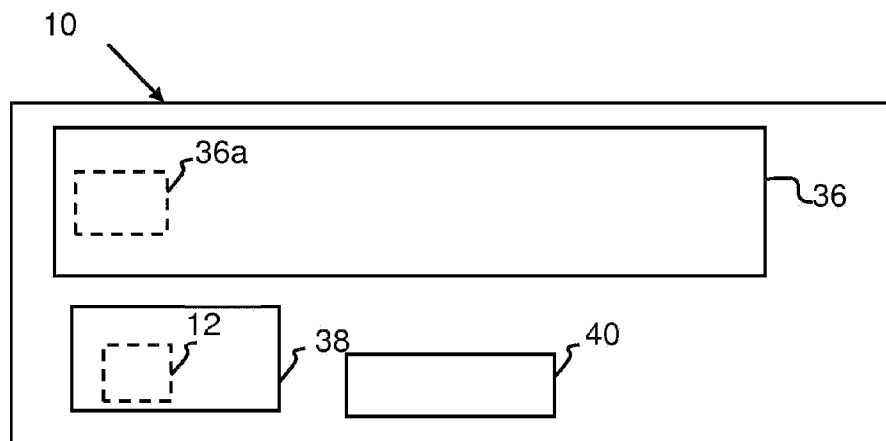


Fig. 5

**Fig. 6**

**Fig. 7**