(19) DANMARK

Patent- og
Varemærkestyrelsen

(10) **DK/EP 3334185 T3**

(12) Oversættelse af europæisk patentskrift

(51) Int.Cl.: ***H 04 R 25/00 (2006.01)***

(45) Oversættelsen bekendtgjort den: **2021-09-13**

(80) Dato for Den Europæiske Patentmyndigheds
bekendtgørelse om meddelelse af patentet: **2021-06-02**

(86) Europæisk ansøgning nr.: **16202912.8**

(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: **HEARING SYSTEM, DEVICES AND METHOD OF SECURING COMMUNICATION FOR A USER APPLICATION**

(56) Fremdragne publikationer:
US-A1- 2011 030 040
US-A1- 2014 211 973
US-A1- 2015 125 014
US-A1- 2015 281 863
US-B1- 8 467 770

DESCRIPTION

[0001] The present disclosure relates to a hearing system comprising a server device and a hearing device system, wherein the hearing device system comprises a hearing device and a user accessory device. In particular, the present disclosure relates to devices for securing communication for a user application on a user accessory device of a hearing system comprising a hearing device, and a method of securing communication for a user application on a user accessory device of a hearing system comprising a hearing device.

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 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.

[0003] US 2014/0211973 relates to location-based assistance using hearing instruments and a method wherein a hearing instrument may be used for user identification for a device, e.g. a computer, with a key or password being sent from the hearing instrument to the device.

SUMMARY

[0004] There is a need for apparatus, devices and methods for providing improved security for hearing system communication. Further, there is a need for devices and methods reducing the risk of a hearing aid and hearing aid function being compromised by a third (unauthorized) party.

[0005] Accordingly, a method of securing communication for a user application on a user accessory device of a hearing system comprising a hearing device is disclosed, wherein securing communication for the user application comprises obtaining challenge data in a server device; transmitting the challenge data from the server device to the user application; optionally transmitting a challenge request comprising the challenge data from the user application to the hearing device; optionally receiving a challenge response comprising response data from the hearing device; optionally forwarding the response data from the user application to the server device; optionally receiving a response message comprising response data from the user application; verifying the response data in the server device based on the challenge data; and optionally approving the user application in the server device if verifying the response data is successful.

[0006] Further, a hearing system comprising a server device and a hearing device system, the hearing device system comprising a user accessory device and a hearing device, the server device being configured for securing communication for a user application on the user accessory device, is disclosed. The server device is configured to approve the user application, wherein to approve the user application comprises to obtain challenge data; transmit the challenge data to the user application; receive a response message comprising response data from the user application, the response data comprising a hearing device identifier; verify the response data based on the challenge data; and approve the user application if the response data are verified, the user accessory device comprising a processing unit; a memory unit; and an interface, wherein the user application is configured to secure communication for the user application, and wherein to secure communication for the user application comprises to: obtain challenge data from a server device; transmit a challenge request comprising the challenge data to the hearing device of the hearing device system; receive a challenge response comprising response data from the hearing device; and forward the response data to the server device.

[0007] It is an important advantage of the present disclosure that the risk of user sensitive data, such as hearing device settings and/or user specific software updates, being sent to or shared with third party user applications or otherwise corrupted user applications is heavily reduced or eliminated.

[0008] Further, the present disclosure allows a hearing device manufacturer to securely keep and maintain updated and correct information on user applications. Even further, a server device/hearing device manufacturer can keep updated information on and link user applications with specific hearing devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The above and other features and advantages of the present invention 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
shows an exemplary signaling diagram,

Fig. 3
is a flow diagram of an exemplary method according to the invention, and

Fig. 4
schematically illustrates an exemplary server device.

DETAILED DESCRIPTION

[0010] 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 descri bed.

[0011] The present disclosure relates to improved security in hearing system communication. The hearing system comprises a server device, a user accessory device having a user application installed thereon and a hearing device. 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 processor. Namely, the method, user application and server device disclosed herein enables hearing system communication that 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 hearing system communication that is robust against replay attacks, unauthorized access, battery exhaustion attacks, and man-in-the-middle attacks.

[0012] 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 of e.g. 8 bits, 16 bits, 32 bits, 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.

[0013] The user accessory device comprises a memory unit and an interface respectively connected to a processing unit. The memory unit may include removable and non-removable data storage units including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), etc. The memory unit has a user application stored thereon. The interface comprises an antenna and a wireless transceiver, e.g. configured for wireless communication at frequencies in the range from 2.4 to 2.5 GHz. The interface may be configured for communication, such as wireless communication, with the hearing device comprising an antenna and a wireless transceiver.

[0014] The method comprises obtaining challenge data in a server device. Obtaining challenge data may comprise generating the challenge data, e.g. based on a default challenge value and/or a timestamp. Accordingly, the server device may be configured to generate the challenge data, e.g. based on a default challenge value and/or a timestamp. The server device may be configured to generate the challenge data at a certain interval, such as every 5 minutes, every 10 minutes, or every 30 minutes. While a short time between generation of (different) challenge data may increase security, a too short time between generation of (different) challenge data may set too high timing requirements for the user application/hearing device, which in turn leads to unnecessary faulty verifications and requires power-consuming challenge-response generation in the hearing device. The challenge data may be random or pseudo-random. The challenge data may comprise at least 8 bytes, such as at least 16 bytes. The challenge data may be a 16-bytes value. The server device may be configured to generate the challenge data based on a look-up table and/or a function, e.g. having a timestamp as input. Obtaining challenge data based on a timestamp value enables and/or provides challenge data with a built-in validity period. Obtaining challenge data with a given interval enables and/or provides challenge data with a built-in validity period.

[0015] The present disclosure relates to secure communication between entities of a hearing system. The hearing system comprises a server device and a hearing device system, the hearing device system comprising a user accessory device and a hearing device. The user accessory device forms an accessory device to the hearing device. The user accessory device is typically paired or otherwise 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.

[0016] Obtaining challenge data may comprise storing the challenge data in the server device. The server device may be configured to delete the challenge data after verifying the response data. The method may comprise deleting the challenge data after a certain period of time and/or replacing the challenge data with new challenge data.

[0017] The method comprises transmitting the challenge data from the server device to the user application.

[0018] The method comprises transmitting a challenge request comprising the challenge data from the user application to the hearing device.

[0019] The method comprises receiving a challenge response, e.g. in the user application, the challenge response comprising response data from the hearing device. The response data may comprise at least 8 bytes, such as at least 16 bytes or at least 32 bytes. The response data may have a length in the range from 16 to 72 bytes. The response data may comprise a hearing device identifier. The response data may comprise a key identifier for enabling the server device to use or apply the correct keying material when verifying the response data. The response data may comprise hearing device challenge data generated in the hearing device.

[0020] The response data comprises a response value, e.g. a challenge response value, and/or hearing device data. The response data may comprise a checksum value based on the response value and/or the hearing device data. The response value may be based on the challenge data and/or hearing device data, e.g. a hearing device identifier. The response value may be generated based on one or more of the challenge data from the server device, a hearing device key identified by the key identifier, the hearing device identifier, and hearing device challenge data. The response value may be based on a static string. The response value may be encrypted using one or more of challenge data from the server device, a key identified by the key identifier, the hearing device identifier, and hearing device challenge data as keying material.

[0021] The method comprises forwarding the response data from the user application to the server device, e.g. in a response message. The response data, e.g. the response value of the response data, are verified in the server device based on the challenge data. Verifying the response data in the server device based on the challenge data may comprise calculating the challenge data, e.g. based on a default challenge value and/or a timestamp. Verifying the response data in the server device based on the challenge data may comprise retrieving the challenge data from a memory of the server device. Verifying the response data in the server device may be based on hearing device challenge data of the response data. Verifying the response data in the server device may be based on hearing device identifier of the response data. Verifying the response data may comprise calculating a verification value based on the challenge data from the server device and/or one or more of a key identified by the key identifier, hearing device challenge data, and hearing device identifier of the response data. Verifying the response data may comprise comparing the verification value with the response value. The response data may be verified (verifying is successful) if the verification value corresponds to the response value.

[0022] The method optionally comprises approving the user application in the server device if verifying the response data is successful. Thus, the server device regards the user application as a trusted entity in the system if verifying the response data is successful. In other words, the user application can be said to be white-listed in the server device if verifying the response data is successful.

[0023] The method optionally comprises disapproving the user application in the server device if verifying the response data fails. Thus, the server device may regard the user application as an un-trusted entity in the system if verifying the response data is successful. The user application may be black-listed, e.g. for a certain period, in the server device if verifying the response data fails, e.g. if verifying the response data fails for a number of times, e.g. two, three or more. The method may comprise setting a user application status identifier to a value indicative of the user application not being approved if verifying the response data fails.

[0024] The method may comprise determining the response data, or at least a response value thereof, in the hearing device based on the challenge data and/or hearing device identifier of the hearing device. Thus, the hearing device may be configured to generate the response data based on the challenge data and/or a hearing device identifier. Response data, such as a response value, based on a hearing device identifier enables the server device to authenticate the hearing device. The response data optionally comprises or is indicative of a hearing device identifier. Thus, the server device can identify a specific hearing device.

[0025] In the method, receiving a challenge response comprising response data from the hearing device may be performed by the user application.

[0026] In the method, approving the user application comprises setting a user application status identifier to a value indicative of the user application being approved.

[0027] The method may comprise linking the user application to a hearing device, e.g. to the hearing device identifier of the hearing device, in a memory of the server device if verifying the response data is successful.

[0028] The method may comprise transmitting a request for challenge data from the user application. Thus, the user application and/or hearing device may be able to initiate the secure communication between the user application and the server device, e.g. if the user application is updated and/or if the user accessory device and/or the user application is restarted, in turn increasing the security level.

[0029] The request for challenge data may be transmitted if a first approval criterion, e.g. in the user application, is fulfilled. The first approval criterion may comprise determining, e.g. in the user application, if the user application has been approved earlier, wherein the first approval criterion is fulfilled if the user application has not been approved earlier. The first approval criterion may be fulfilled if the user application is started for the first time, e.g. after installation of the user application and/or after repowering of the user accessory device. The first approval criterion may be fulfilled if the user application has been updated to a new version.

[0030] The method may comprise storing an approval timestamp indicative of time of last approval; determining if a second approval criterion based on the approval timestamp is fulfilled; and initiate securing communication for the user application if the second approval criterion is fulfilled. Thereby is ensured that the server device approves/disapproves a user application with a certain frequency, further increasing the security in the hearing system by keeping an updated user application database in the server device and to optimize hearing system communication.

[0031] In the method, approving the user application may comprise transmitting hearing device settings specific for the hearing device to the user application. Approving the user application may comprise transmitting hearing device operating parameters specific for the hearing device to the user application.

[0032] The method may comprise not approving or disapproving the user application if response data are not received within an approval period, e.g. from obtaining challenge data or transmitting the challenge data. In one or more exemplary server devices/methods, the length of an approval period may be determined by a frequency of determining new challenge data. In one or more exemplary devices/methods, challenge data are calculated or generated with a given interval, such as every 5 minutes or every 10 minutes.

[0033] The method may comprise establishing a secure session between the user application and the hearing device and optionally transmitting the challenge request in the secure session, such as an integrity-protected, encrypted, authenticated, and/or mutually authenticated session. The challenge response may be received in the secure session.

[0034] The method may comprise establishing a secure session, such as an integrity-protected, encrypted, authenticated, and/or mutually authenticated session, between the server device and the user application, and optionally transmitting the challenge data in the secure session. The response data may be forwarded from the user application to the server device in the secure session.

[0035] The server device may be configured to determine if an approval criterion is fulfilled, the server device being configured to initiate securing communication for the user application if the approval criterion is fulfilled, wherein the approval criterion comprises a first approval criterion and a second approval criterion, and wherein the approval criterion is fulfilled if the first approval criterion and/or the second approval criterion is fulfilled. The second approval criterion may be fulfilled if the time since last approval is longer than an approval time threshold, e.g. one or more days, such as 7 days, 14 days. Thus, approval of a user application with a minimum frequency may be employed to ensure updated user application data in the server device.

[0036] The present disclosure also relates to a user application for a user accessory device of a hearing system. The user accessory device may be a smartphone, a smartwatch or a tablet computer. The user application is, when installed on the user accessory device, configured to secure communication for the user application.

[0037] The user application may be configured to determine if a first approval criterion is fulfilled and to initiate securing communication for the user application if the first approval criterion is fulfilled, and wherein to obtain challenge data comprises to transmit a request for challenge data to the server device. The request for challenge data is a message requesting the server device to transmit challenge data to the user application. Thus, the user application and/or hearing device (via the user application) can actively initiate approval of the user application in the server device.

[0038] By enabling hearing system entities to initiate securing communication for the user application, the approval procedures can be optimized, e.g. by enabling the approval procedure to be initiated only when necessary or when justified due to changes in the different entities in the hearing system.

[0039] The figures are schematic and simplified for clarity, and they merely show details which are essential to the understanding of the invention, while other details have been left out. Throughout, the same reference numerals are used for identical or corresponding parts.

[0040] Fig. 1 shows an exemplary hearing system. The hearing system 2 comprises a server device 4 and a hearing device system 6 comprising a hearing device 8 and a user accessory device 10. The user accessory device 10 is a 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. In one or more exemplary user applications, the user application 12 is configured to transfer firmware and/or hearing device settings to the hearing device.

[0041] The server device 4 and/or the user application 12 may be configured to perform any acts of the method disclosed herein. The hearing device 2 may be configured to compensate for hearing loss of a user of the hearing device 2. The hearing device 8 is configured to configured to communicate with the user accessory device 10/user application 12, e.g. using a wireless and/or wired first communication link 20. The first communication link 20 may be a single hop communication link or a multi-hop communication link. The first communication link 20 may be carried over a short-range communication system, such as Bluetooth, Bluetooth low energy, IEEE 802.11 and/or Zigbee.

[0042] The user accessory device 10/user application 12 is configured to connect to the server device 4 over a network, such as the Internet and/or a mobile phone network, via a second communication link 22. The server device 4 may be controlled by the hearing device manufacturer. The hearing device 8 comprises an antenna 24 and a radio transceiver 26 coupled to the antenna 4 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, wherein hearing device settings are stored in the memory unit.

[0043] The hearing device 2 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.

[0044] The user accessory device 10 comprises a processing unit 36, a memory unit 38, and interface 40. The user application 12 is installed in the memory unit 38 of the user accessory device 10 and is configured to secure communication for the user application, wherein to secure communication for the user application comprises to obtain challenge data from the server device 4; transmit a challenge request comprising the challenge data to the hearing device 8; receive a challenge response comprising response data from the hearing device 8; and transmit the response data to the server device 4.

[0045] Fig. 2 shows an exemplary signaling diagram 100 between the entities 4, 8, 12 of the hearing system 2 illustrating an exemplary method of securing communication for a user application on a user accessory device of a hearing system comprising a hearing device. Securing communication for the user application comprises obtaining challenge data in the server device 4. The method comprises transmitting the challenge data 102 in a challenge message 104 from the server device 4 to the user application 12. The user application 12 receives the challenge data and transmits a challenge request 106 comprising the challenge data 102 from the user application 12 to the hearing device 8. The hearing device 8 generates response data based on the challenge data and optionally a hearing device identifier of the hearing device, and transmits a challenge response 108 to the user application 12, the user application receiving the challenge response 108 comprising response data 110 from the hearing device 8. The user application forwards the response data 110 in a response message 112 to the server device 4, and the server device 4 verifies the response data 110 based on the challenge data and approves the user application 12 in the server device 4 if verifying the response data 110 is successful.

[0046] Optionally, the method comprises transmitting a request 114 for challenge data from the user application 12 to the server device, e.g. if a first approval criterion is fulfilled. In the illustrated hearing system, the first approval criterion is fulfilled if the user application has started for the first time or the user application has been updated. Receipt of the request for challenge data in the server device 4, i.e. a first approval criterion fulfilled in server device, triggers securing communication for the user application. The server device 4 is configured to determine if an approval criterion is fulfilled and the server device 4 is configured to initiate securing communication for the user application if the approval criterion is fulfilled. The approval criterion in the server device comprises a first approval criterion and optionally a second approval criterion. The second approval criterion is fulfilled if the user application has not been approved for a certain period of time, e.g. 14 days. Thus, the second approval criterion may be based on an approval timestamp indicative of time of last approval of the user application. The approval criterion is fulfilled if the first approval criterion or the second approval criterion is fulfilled.

[0047] Fig. 3 shows a flow diagram of an exemplary method of securing communication for a user application on a user accessory device of a hearing system comprising a hearing device. In the method 200, securing communication for the user application comprises obtaining 202 challenge data in a server device; transmitting 204 the challenge data from the server device to the user application; transmitting 206 a challenge request comprising the challenge data from the user application to the hearing device; receiving 208 a challenge response comprising response data from the hearing device; and forwarding 209 the response data from the user application to the server device. The method 200 comprises verifying 210 the response data in the server device based on the challenge data; and approving 212 the user application in the server device if verifying the response data is successful 214. Optionally, the method comprises determining 216 if an approval criterion is fulfilled in the server device and proceed with obtaining 202 challenge data if the approval criterion is met. If so, the method initiates or proceeds to securing communication for the user application.

[0048] Fig. 4 shows an exemplary server device for securing communication for a user application on a user accessory device of a hearing system comprising a hearing device. The server device 4 comprises a processing unit 250, a memory unit 252, e.g. comprising a database, and an interface 254. The server device 4 is configured to approve the user application, wherein to approve the user application comprises to obtain challenge data, e.g. with obtain module 202a. To obtain challenge data comprises to generate challenge data, e.g. based on a default challenge value and/or a timestamp. The challenge data has a length of 16 bytes. The server device is configured to transmit the challenge data via the interface 254 to a user application of a user accessory device in a challenge message, e.g. with transmit module 204a, and receive a response message comprising response data from the user application via the interface 254, e.g. by receive module 256. The server device is configured to verify the response data, e.g. a response value of the response data, based on the challenge data and/or a hearing device identifier, e.g. by verification module 210a. The server device may comprise a hardware security module, e.g. as part of verification module 210a, configured to verify the response data/response value. If the response data are verified, the server device is configured to approve the user application, e.g. with approval module 212a. To verify the response data optionally comprises calculating the challenge data and verify the response data based on the calculated challenge data. Calculating challenge data as part of the response data verification eliminates the need for memory in the server device and storing of challenge data. To verify the response data comprises to verify a response value of the response data e.g. based on the challenge data and/or a hearing device identifier of the response data. To verify the response data in the server device may comprise to verify a checksum value of the response data.

[0049] The server device 4 is optionally configured to receive a request for challenge data from the user application via the interface 254, and to initiate securing communication for the user application upon receipt of the request for challenge data from the user application. Further, the server device 4 is optionally configured to determine if a second approval criterion based on a last approval timestamp is fulfilled; and to initiate approval of the user application if the second approval criterion is fulfilled, e.g. if the user application has not been approved for a certain period of time, e.g. 14 days.

[0050] The server device 4 may be arranged to execute at least parts of methods of securing communication for a user application on a user accessory device of a hearing system as disclosed herein. The server device or the processing unit 250 may further comprise a number of optional functional modules, such as any of an obtain module 202a configured to perform step 202, a transmit module 204a configured to perform step 204, a receive module 256 configured to receive a response message, a verification module 210a configured to perform step 210, and an approval module 212a configured to perform step 212. In general terms, each functional module may be implemented in hardware or in software.

[0051] Although 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. The specification and drawings are, accordingly to be regarded in an illustrative rather than restrictive sense.

LIST OF REFERENCES

[0052]

2	hearing system
4	server device
6	hearing device system
8	hearing device
10	user accessory device
12	user application
20	first communication link
22	second communication link
24	antenna
26	radio transceiver
28	first microphone
30	second microphone
32	processor
34	receiver
36	processing unit

38

memory unit

40

interface

100

signalling diagram

102

challenge data

104

challenge message

106

challenge request

108

challenge response

110

response data

112

response message

114

request for challenge data

200

method of securing communication for a user application

202

obtaining challenge data in a server device

202a

obtain module

204

transmitting the challenge data

204a

transmit module

206

transmitting a challenge request comprising the challenge data

208

receiving a challenge response comprising response data

209

forwarding the response data

210

verifying the response data based on the challenge data

210a

verification module

212

approving the user application

212a

approval module

214
verification of response data successful?

216
determining if an approval criterion is fulfilled

250
processing unit

252
memory unit

254
interface

256
receive module

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

- US20140211973A [0003]

PATENTKRAV

1. Fremgangsmåde (200) til sikring af kommunikation for en brugerapplikation, der er installeret på en brugertilbehørsindretning af et høresystem, som omfatter en høreindretning, en serverindretning og brugertilbehørsindretningen, hvor sikring af kommunikation for brugerapplikationen omfatter:

- opnåelse (202) af forespørgselsdata i serverindretningen,

- transmission (204) af forespørgselsdataene fra serverindretningen til den brugerapplikation, der er installeret på brugertilbehørsindretningen,

- transmission (206) af en forespørgselsanmodning, der omfatter forespørgselsdataene, fra brugerapplikationen til høreindretningen,

- modtagelse (208) af et forespørgselssvar, der omfatter svardata, fra høreindretningen,

- videresendelse (209) af svardataene fra brugerapplikationen til serverindretningen,

- verificering (210) af svardataene i serverindretningen, baseret på forespørgselsdataene, og

- godkendelse (212) af brugerapplikationen i serverindretningen, hvis verificering af svardataene lykkes.

2. Fremgangsmåde ifølge krav 1, hvor fremgangsmåden omfatter bestemmelse af svardataene i høreindretningen, baseret på forespørgselsdataene og en høreindretningsidentifikator af høreindretningen.

3. Fremgangsmåde ifølge et hvilket som helst af kravene 1-2, hvor svardataene omfatter eller angiver en høreindretningsidentifikator.

4. Fremgangsmåde ifølge et hvilket som helst af kravene 1-3, hvor modtagelse af et forespørgselssvar, der omfatter svardata fra høreindretningen, udføres af brugerapplikationen.

5. Fremgangsmåde ifølge et hvilket som helst af kravene 1-4, hvor godkendelse af brugerapplikationen omfatter indstilling af en brugerapplikationsstatusidentifikator til en værdi, der angiver, at brugerapplikationen er godkendt.

6. Fremgangsmåde ifølge et hvilket som helst af kravene 1-5, hvilken fremgangsmåde omfatter indstilling af en brugerapplikationsstatusidentifikator til en værdi, der angiver, at brugerapplikationen ikke er godkendt, hvis verificering af svardataene mislykkes.

7. Fremgangsmåde ifølge et hvilket som helst af kravene 1-6, hvilken fremgangsmåde omfatter tilknytning af brugerapplikationen til en høreindretning i en hukommelse af serverindretningen, hvis verificering af svardataene lykkes.

8. Fremgangsmåde ifølge et hvilket som helst af kravene 1-7, hvilken fremgangsmåde omfatter transmission af en anmodning om forespørgselsdata fra brugerapplikationen.

9. Fremgangsmåde ifølge krav 8, hvor anmodningen om forespørgselsdata transmitteres, hvis et første godkendelseskriterium er opfyldt.

10. Fremgangsmåde ifølge et hvilket som helst af kravene 1-9, hvilken fremgangsmåde omfatter lagring af et godkendelsestidsstempel, der angiver tidspunktet for seneste godkendelse, bestemmelse af, om et andet godkendelseskriterium baseret på godkendelsestidsstemplet er opfyldt, og indledning af sikring af kommunikation for brugerapplikationen, hvis det andet godkendelseskriterium er opfyldt.

11. Fremgangsmåde ifølge et hvilket som helst af kravene 1-10, hvor godkendelse af brugerapplikationen omfatter transmission af høreindretningsindstillinger, der er specifikke for høreindretningen, til brugerapplikationen.

12. Fremgangsmåde ifølge et hvilket som helst af kravene 1-11, hvor opnåelse af forespørgselsdata omfatter lagring af forespørgselsdataene i serverindretningen, eller

hvor verificering af svardataene i serverindretningen baseret på forespørgselsdataene omfatter beregning af forespørgselsdataene.

13. Høresystem (2), der omfatter en serverindretning (4), og et høreindretningssystem, som omfatter en brugertilbehørsindretning (10) og en høreindretning (8), idet serverindretningen (4) sikrer kommunikation for en brugerapplikation (12), der er installeret på brugertilbehørsindretningen (10), hvor serverindretningen (4) er konfigureret til at godkende brugerapplikationen (12), hvor godkendelse af brugerapplikationen (12) omfatter at:

- opnå forespørgselsdata,

- transmittere forespørgselsdataene til brugerapplikationen (12),

- modtage en svarmeddelelse, der omfatter svardata fra brugerapplikationen (12), hvilke svardata omfatter en høreindretningsidentifikator,

- verificere svardataene baseret på forespørgselsdataene, og

- godkende brugerapplikationen (12), hvis svardataene verificeres, og

idet brugertilbehørsindretningen (10) omfatter:

- en behandlingsenhed,

- en hukommelsesenhed, og

- en grænseflade,

hvor brugerapplikationen (12) er konfigureret til at sikre kommunikation for brugerapplikationen, og hvor sikring af kommunikation for brugerapplikationen omfatter at:

- opnå forespørgselsdata fra serverindretningen (4),

- transmittere en forespørgselsanmodning, der omfatter forespørgselsdataene, til høreindretningssystemets (2) høreindretning (8),

- modtage et forespørgselssvar, der omfatter svardata, fra høreindretningen (8), og

- transmittere svardataene til serverindretningen (4).

14. Høresystem (2) ifølge krav 13, hvor serverindretningen (4) er konfigureret til at bestemme, om et godkendelseskriterium er opfyldt, idet serverindretningen (4) er

konfigureret til at indlede sikring af kommunikation for brugerapplikationen (12), hvis godkendelseskriteriet er opfyldt, hvor godkendelseskriteriet omfatter et første godkendelseskriterium og et andet godkendelseskriterium, og hvor godkendelses-kriteriet er opfyldt, hvis det første godkendelseskriterium eller det andet godkendelseskriterium er opfyldt.

15. Høresystem (2) ifølge et hvilket som helst af kravene 13-14, hvor brugerapplikationen (12) er konfigureret til bestemme, om et første godkendelseskriterium er opfyldt, og til at indlede sikring af kommunikation for brugerapplikationen, hvis det første godkendelseskriterium er opfyldt, og hvor opnåelse af forespørgselsdata omfatter at transmittere en anmodning om forespørgselsdata til serverindretningen.

DRAWINGS

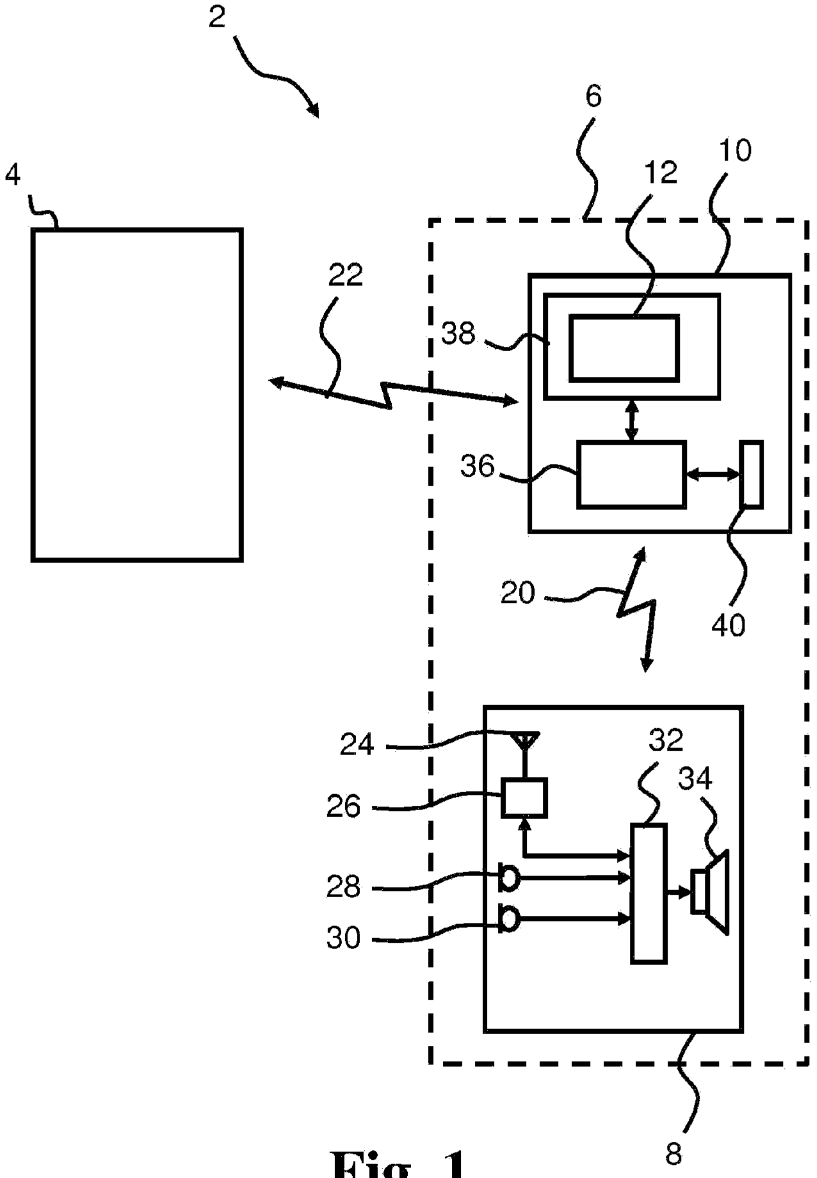

Fig. 1

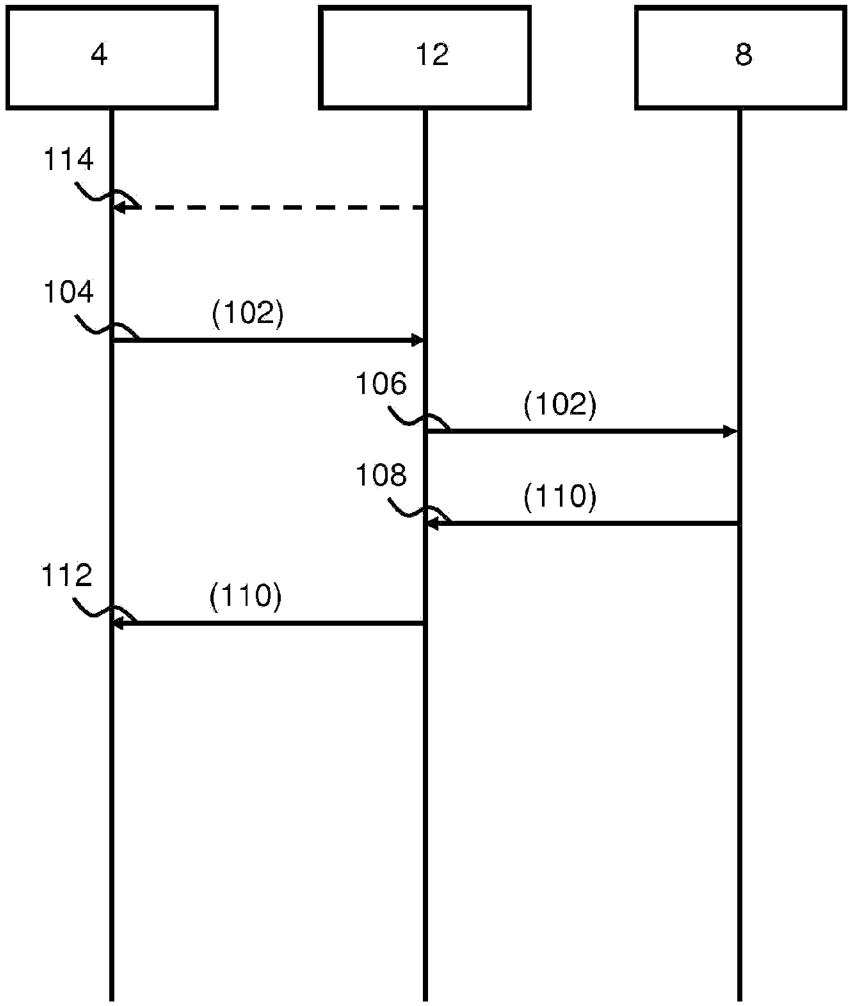

Fig. 2

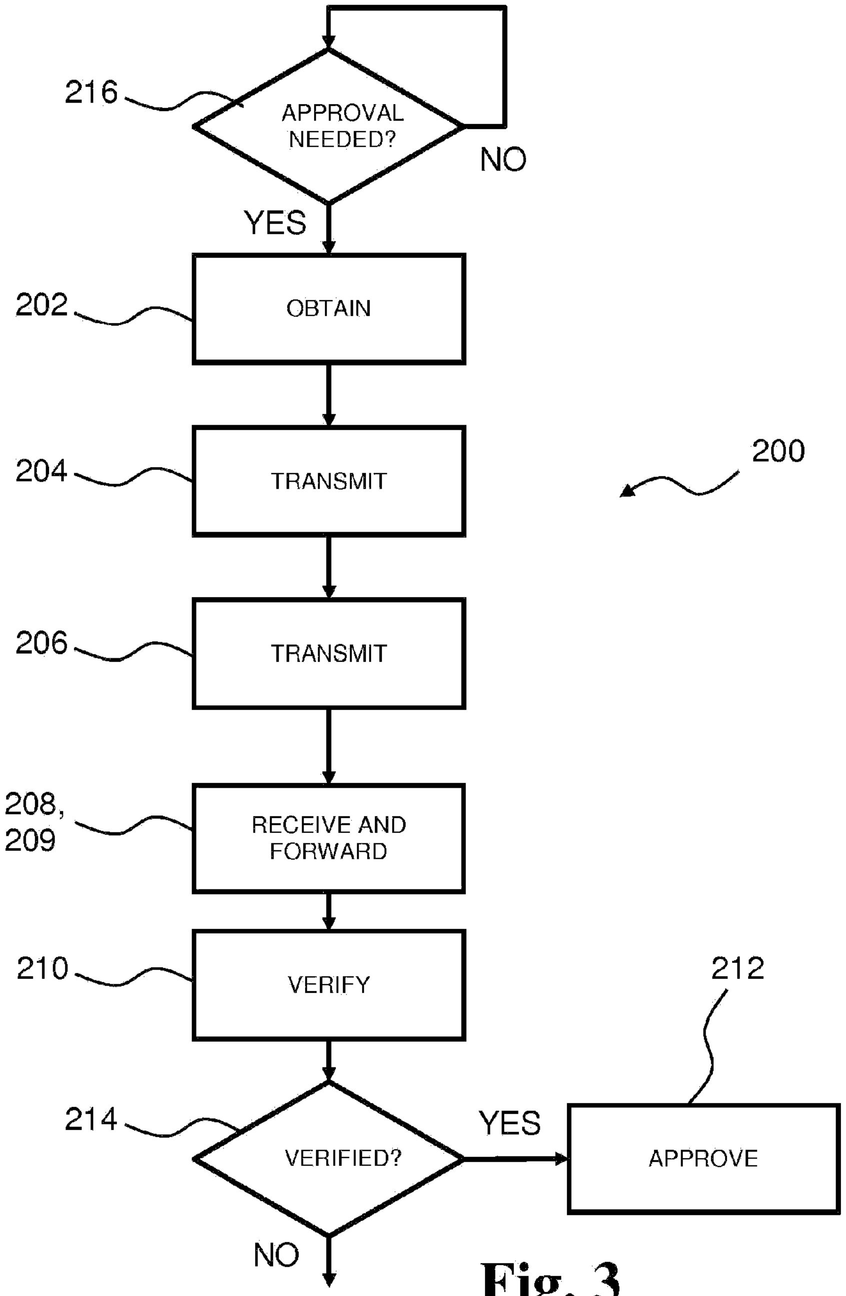
216
APPROVAL NEEDED?
NO
YES
202
OBTAIN
204
TRANSMIT
200
206
TRANSMIT
208, 209
RECEIVE AND FORWARD
210
VERIFY
212
214
VERIFIED?
YES
APPROVE
NO

Fig. 3

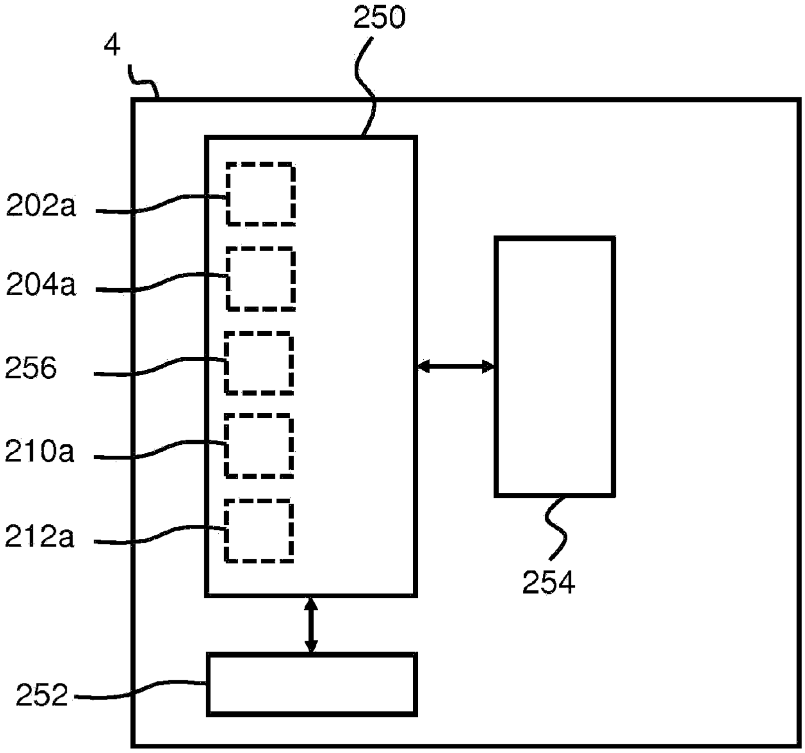

Fig. 4