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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/015748 A1

(51) International Patent Classification:
H04W 12/10 (2009.01) *H04L 29/06* (2006.01)
G06F 21/64 (2013.01) *G06F 21/57* (2013.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2017/068197

(22) International Filing Date:
19 July 2017 (19.07.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for LC only)*: **SONY MOBILE COMMUNICATIONS AB** [SE/SE]; Mobilvägen, 221 88 Lund (SE).

(71) Applicant: **SONY MOBILE COMMUNICATIONS INC** [JP/JP]; 4-12-3 Higashi-Shinagawa, Shinagawa-ku, Tokyo, 140-0002 (JP).

(72) Inventor: **BERGSELL, Benny**; Svanevägen 23, 21223 Malmö (SE).

(74) Agent: **NEIJ & LINDBERG AB**; Pedellgatan 11, SE-224 60 Lund (SE).

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

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

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

WO 2019/015748 A1

(54) Title: A SERVER, A HEADLESS DEVICE, A CONTROLLER AND METHODS RELATING THERETO

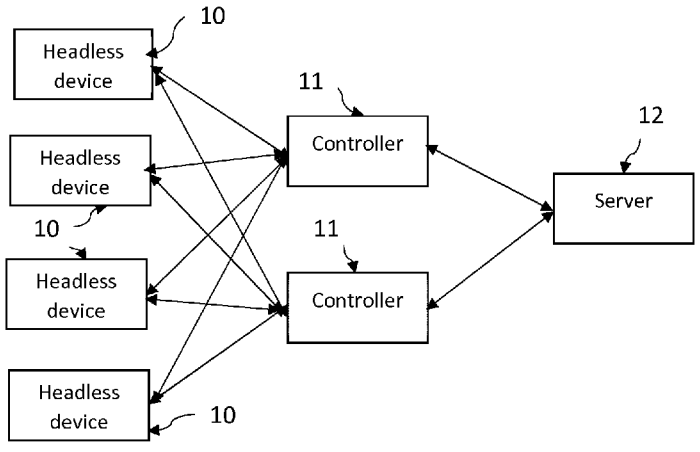

FIG. 1

(57) Abstract: A server (12) for managing headless devices (10) comprises a processor (41), which is configured to receive, from a controller (11), which is used to control a headless device (10), identifying information for the headless device (10) and at least one updated setting to be applied to the headless device (10). In response to the receipt thereof, the processor is further configured to retrieve secret information using the identifying information for the headless device (10),to digitally sign the updated setting with the secret information, and to initiate transmission of the digitally signed updated setting to the headless device (10) in order to enable the headless device (10) to validate that the updated setting originates from the server (12) before applying the updated setting. A controller, a headless device and related methods are also disclosed.

A SERVER, A HEADLESS DEVICE, A CONTROLLER AND METHODS RELATING THERETO

Technical Field

The present invention generally relates to security aspects relating to control of headless devices. More particularly, the invention relates to a server for managing headless devices, a headless device, a controller for controlling a headless device and methods relating thereto.

Background Art

A device without a user interface or only having a very limited user interface is commonly called a "headless device". Such a device typically lacks a monitor, a graphical user interface, a keyboard, a keypad, a mouse or the like, making it difficult to interact with the device.

The article "Simplifying IoT: Connecting, Commissioning and Controlling with Near Field Communication (NFC)", White Paper June 2016, Copyright 2016 NFC Forum, indicates that headless devices can be interacted with using an NFC-enabled smartphone, the screen of which operates as the graphical user interface.

However, there is always a risk that a user, involuntarily or on purpose, interacts with a headless device in a way that would make the device malfunction or inoperable. Thus, there is a need to improve the security aspects relating to the interaction with headless devices.

Summary

One aspect of the present invention is a server for managing headless devices, comprising a processor, which is configured to receive, from a controller, which is used to control a headless device, identifying information for the headless device and at least one updated setting to be applied to the headless device, and, in response to the receipt thereof, retrieve secret information using the identifying information for the headless device, digitally sign the updated setting with the secret information, and initiate transmission of the digitally signed updated setting to the headless device in order to enable the headless device to validate that the updated setting originates from the server before applying the updated setting.

A second aspect of the present invention is a method for managing headless devices, comprising the steps of receiving identifying information for a headless device and at least one updated setting to be applied to the headless device, and in response to the receipt thereof, retrieving secret information associated with the identifying

information for the headless device, and digitally signing the updated setting with the secret information, and initiating transmission of the digitally signed updated setting to the headless device in order to enable the headless device to validate the origin of the updated setting before applying the updated setting.

A third aspect of the present invention is a headless device, comprising a processor and a memory storing security information, wherein the processor is configured to receive a digitally signed, updated setting, which has been digitally signed by a server using secret information of the server, and to validate, using the security information, the origin of the updated setting, and to apply the updated setting only if it is validated that the updated setting originates from the server.

A fourth aspect of the present invention is a method in a headless device, comprising the steps of receiving a digitally signed, updated setting, which has been digitally signed by a server using secret information of the server; validating, using security information stored in the headless device, the origin of the updated setting; and applying the updated setting only if it is validated that the updated setting originates from the server.

A fifth aspect of the present invention is a controller for controlling a headless device, comprising a processor, which is configured to receive from a user, at least one updated setting to be applied in the headless device, transfer the updated setting, together with information identifying the headless device, to a server with a request for digital signing of the updated setting; to receive from the server the requested digitally signed, updated setting, and to transfer the digitally signed, updated setting to the headless device in order to enable the headless device to validate that the updated setting originates from the predetermined server before applying the updated setting.

A sixth aspect of the present invention is a method for managing a headless device, comprising the steps of receiving, from a user, at least one updated setting to be applied in the headless device, transferring the updated setting, together with information identifying the headless device, to a server with a request for digital signing of the updated setting; receiving from the server the requested digitally signed, updated setting; and transferring the digitally signed, updated setting to the headless device in order to enable the headless device to validate that the updated setting originates from the predetermined server before applying the updated setting.

Brief Description of Drawings

Embodiments of the invention will now be described in more detail with reference to the accompanying schematic drawings.

Fig. 1 is a schematic block diagram of a system providing for improved security relating to control of headless devices.

Fig. 2 is a schematic block diagram of a headless device that may be used in the system of Fig. 1

Fig. 3 is a schematic block diagram of a controller that may be used in the system of Fig. 1.

Fig. 4 is a schematic block diagram of server that may be used in the system of Fig. 1.

Fig. 5 is a schematic sequence diagram, illustrating one exemplary embodiment of an operation of a system according to Fig. 1.

Detailed Description of Example Embodiments

Fig. 1 shows a system including a plurality of headless devices 10, a plurality of controllers 11 and a server 12, which system allows for improved security with regard to the control of the headless devices. By routing information read from the headless devices 10 and/or written to the headless devices 10 through the server 12, the security aspects may be improved as will be described in further detail below.

In the simplest version of the system of Fig.1, the system may include only one headless device 10, one controller 11 and the server 12.

As mentioned above, headless devices 10 are devices that lack a user interface or have a very basic user interface making it difficult for a user to interact with the headless devices. The headless devices may be simple, low-end devices with a limited number of basic functions, like timers, humidity sensors, temperature controllers, headsets, smoke alarms and car keys. Headless devices may also include more sophisticated apparatuses that for one reason or another, e.g. size, design or location, do not have an ordinary user interface. Examples of such devices may include pacemakers, hearing aids, engines and household appliances.

A headless device 10 may be controlled or interacted with using a separate controller 11 having a more user-friendly user interface than the headless device it is used to interact with. The controller 11 may be a dedicated device created only for interaction with a specific headless device 10. It may however also be a generic device adapted for the purpose. Typically, the controller 11 would be a smartphone with a software application that controls the interaction with the headless device. The controller may be used for controlling or interacting with one or more headless devices 10 of the same kind or for controlling or interacting with two or more headless devices 10 of different types. Different controllers 11 may be used for controlling or interacting with the same headless device 10.

The headless devices 10 may be but are typically not connected to the Internet, i.e. the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide.

All controllers 11 are configured to communicate with a server 12, which, in operation, may have access to one or more data storages that store information about the headless devices. The information may in one exemplary embodiment include identifying information for the headless devices 10 managed by the server 12 and secret information which makes it possible to establish a trust between the server 12 and the respective headless devices 10.

When a user wants to change a setting of a headless device 10 in the system shown in Fig. 1, the user enters an updated setting on a user interface of the controller 11. Instead of sending it directly to the headless device 10, the controller 11 first sends the updated setting and information identifying the headless device 10 to the server12. The server 12 uses the identifying information to retrieve secret information, which is used to digitally sign the updated setting. The digitally signed setting is transmitted, via the controller 11, to the headless device 10, which uses security information stored in its memory to validate that the updated setting originates from the server 12. The setting is only applied in the headless device 10 if the headless device can confirm that it originates from its trusted server 12.

By the system of routing updated settings to a trusted server which signs the settings before they are sent to the headless device, the security relating to control of headless devices can be improved. The system also makes it possible to further improve the security. The server may for instance check updated settings, before they are signed, to make sure that they comply with predetermined requirements. As a further security measure, the system may require user authentication and user authorization before allowing a user to see current settings of a headless device and/or update them.

Fig. 2 shows a schematic block diagram of a headless device 10 according to one exemplary embodiment of the invention. The headless device comprises a processor 21 for operating the headless device. The operation may include reading sensor values, outputting signals, turning on and off switches, and similar functions. The headless device 10 further comprises a first memory 22a for storing executable instructions for the processor, a second memory 22b for storing security information, such as one or more keys of a cryptographic system, a third memory 22c for storing identifying information for the headless device, like a device ID that makes it possible to uniquely identify the headless device, at least within a group of similar devices managed by the server, and a fourth memory 22d for storing one or more settings to be used for the operation of the headless device and, in some cases, an associated token. The settings

include at least one that can be changed by a user to affect the operation of the headless device. The first to fourth memories can be implemented in one or more different data storage units.

The headless device 10 may further comprise a communication unit 23, which is configured to allow for communication with a controller 11 for the headless device. The communication may for example be short-range communication. The communication unit may be passive, like a tag with a memory area that can be read from and written to by the controller 11 and the processor 21 of the headless device, or active in the sense that it can initiate communication and read from and write to the controller 11 or processor 21. It may or may not require a power source. The short-range communication range is typically less than 1 m, preferably less than 20 cm and more preferably less than 10 cm, so that the distance makes it clear with which device the user intends to interact by means of the controller. Suitable communications technologies may include Near Field Communication (NFC) and Bluetooth Low Energy (BLE), but other technologies like Infrared (IR) communication, communication via sound waves, or even by a USB cable may be conceivable.

The processor 21 is operably connected to the communication unit 22 and may be configured to make information, such as one or more current settings, a token, a device-ID or data relating to the operation of the headless device 10, available to the controller 11 and to receive information, such as a token, one or more updated settings or other data, from the controller 11.

When the processor 21 of the headless device 10 receives a digitally signed, updated setting, it validates the origin of the updated setting, by means of the security information stored in its memory. The updated setting is only applied if the origin from its trusted server 12 that has digitally signed the updated setting, can be validated. In this way, it can be made sure that the updated setting originates from a trusted source and has not been tampered with during the transmission from the server.

Fig. 3 is a schematic block diagram of a controller 11 according to one exemplary embodiment of the invention. The controller 11 comprises a processor 31, a memory 32 storing executable instructions for the processor and a user interface 33. The executable instructions may be in the form of a generic or dedicated software application. The user interface typically comprises a presentation unit in the form or a screen or a display. It may also include other interface elements like buttons, switches, a microphone and/or a keypad. In one embodiment a loudspeaker is used as a presentation unit. The controller further comprises a communication unit 34 for communication with a headless device 10. The communication unit 34 should use the same communication technology as the communication unit of the headless device and have the same communication range.

The communication unit 34 may be configured to receive or read information from the headless device 10 and to write information to or make information available to the headless devices 10.

The controller further comprises a second communication unit 35 for wireless communication with a server 12.

In one embodiment, the controller 11 is an NFC-enabled smartphone which has a generic or dedicated software application for controlling interaction with a headless device 10 and a server 12.

The controller 11 is used by a user to control or interact with a headless device 10 by reading information from and writing information to the headless device. The controller 11 is configured to forward information read from the headless device 10 and/or entered by the user to the server 12 and to transmit information received from the server 12 to the headless device 10.

Fig. 4 schematically shows a block diagram of a server 12 or backend system for managing headless devices. The server 12 comprises a processor 41 and a memory 42 storing executable instructions for operating the server as further described in connection with Fig. 5, and a communication unit 43 for communication with one or more controllers 11. The server comprises or have access to one or more data storages 44 storing information relevant for the management of the headless devices. The information may be stored in one or more databases or other data structures.

The information stored by the data storage(s) 44 may include one or more of identifying information for one or more headless devices 10, secret information, e.g. one or more private keys, for one or more headless devices 10, current settings of one or more headless devices 10, tokens indicative of the current settings of one or more headless devices 10, user interface specifications for one or more headless devices 10, and authentication and authorization information for one or more users of the headless devices 10. The information may be stored such that it can be retrieved by means of the identifying information for the headless devices 10. Since the secret information may be more sensitive than the remaining information, it may be stored in a separate data storage with enhanced security, like a Hardware Security Module (HSM), that may also be used for generation and management of the secret information.

The sequence diagram of Fig. 5 illustrates interactions between a user, a headless device 10, a controller 11 and a server 12. The headless device 10 has one or more settings that can be changed by a user. Even though the example below refers to settings in plural, it should be understood that the example is equally valid for a headless device having a single setting that can be changed. In the example below it is further assumed that the communication between the headless device 10 and the controller 11 occurs via

Near Field Communication (NFC) and that the information stored in a data storage accessible by the server 12 is stored in a database 44 in the server.

The first part 510 of the sequence diagram relates to steps carried out during a production phase in order to establish trust between the server 12 and the headless device 10.

In the illustrated embodiment, these steps include generation of at least one key pair and identifying information in the form of a unique device ID (device identification) for the headless. In this example, the keys are a private key and a public key of an asymmetric cryptographic system, which are generated by a key generation algorithm. As is well-known, an asymmetric cryptographic system, also known as a public key cryptographic system, is any cryptographic system that uses pairs of keys: public keys that can be disseminated to anyone and corresponding private keys that are kept secret and only known to the owner. The keys can be used for two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key.

In this example, the device ID and the private key, are stored in the database of the server 12 such that the private key can be found via the device ID. The device ID, the public key that corresponds to the private key and initial settings for the headless device 10 are transferred to the headless device and stored in the headless device. The settings are applied when the headless device 10 is in operation. The initial settings are also stored as current settings of the headless device 10 in the database of the server 12.

The production phase may include the generation of further key pairs of an asymmetric crypto system. A second key pair may include a private key stored in the headless device and a corresponding public key stored in the database of the server. The private key of the headless device may be used to digitally sign information transmitted from the headless device to the server so that the server may be able to confirm that data purported to originate from the headless device has not been tampered with. A third key pair, comprising a public key stored in the headless device and a corresponding private key stored in the server, may be generated to allow for encryption of data transferred from the headless device to the server, whereas a fourth key pair, comprising a public key stored in the server and a corresponding private key stored in the headless device, may be generated to allow for encryption of data from the server to the headless device. One or more of the second, third or fourth key pairs may be used together with the first key pair.

In other embodiments, a symmetric cryptographic system or a combination of an asymmetric and a symmetric crypto system are used. In a symmetric cryptographic

system two parties, here the server 12 and the headless device 10, share a secret, e.g. the same cryptographic key. The requirement of a symmetric cryptographic system that both parties have access to a secret key is usually considered as a drawback compared to asymmetric cryptographic systems.

In one embodiment, the server 12 also creates a token which is indicative of or represents the initial settings of the headless device 10. In its simplest form the token may be the device ID itself. In another embodiment, the token is or includes a value representing the present settings of the headless device. In yet another embodiment, the token comprises both the device ID and the value representing the settings. The token may also include other data, like checksums. The token may be used to minimize the amount of data which has to be read from the headless device 10. If the token includes a value representing the present settings of the headless device 10, the value may be used to verify that the current settings stored by the server 12 are the same as those in the headless device.

A second part 520 of the sequence diagram illustrates how settings may be read from the headless device 10 and presented to the user.

The user may indicate a wish to read data from the headless device 10 in different ways, e.g. by a specific gesture, pressing a button, or activating the controller. When the controller 11 and the headless device 10 are communicating via NFC, the user indicates the wish by putting the controller 11 close to, i.e. within NFC detection distance of, the headless device 10. A request for identifying information is then transferred from the controller to the headless device. The processor of the headless device responds by retrieving the requested information from the memory and making it available to the controller, either by transmitting it to the controller 11 or by storing it so that it is exposed for the controller 11 to read.

The identifying information may comprise the device ID or any other information that could be used to identify the headless device 10 to the server 12.

In the example of Fig. 5, the identifying information is a token ("settings token"), which is made available to the controller 11 by the headless device 10.

In a next step the controller 11 transfers the token to the server 12. The server may then use the token to identify the specific headless device 10 with which the controller has interacted and retrieve the current settings stored for the headless device in the database.

The server 12 may then transfer the current settings for the headless device 10 to the controller 11 so that they can be presented, e.g. displayed, to the user by the controller.

The server 12 may also return a specification of a user interface for presentation on the presentation unit of the controller 11. The user interface specification may be specific to the headless device 10 or specific to a group of similar headless devices 10. The specification may be in the form of a webpage to be displayed in a browser run by the controller 11, or it may be specific instructions expressed in a language suitable for the purpose and based on which the controller 11 can render the user interface. In another embodiment, the specification includes instructions for an audio presentation. In this way a generic software application can be used for different types of headless devices requiring different user interfaces.

The server 12 may also transfer the device ID to the controller 11.

In this example, the database 44 of the server 12 stores the same settings as are used in the headless device 10 itself. This means that the settings need not be transferred from the headless device 10 to the controller 11, but can be retrieved from the server 12 when they should be presented to the user. In this case, the token is the only information that has to be transferred from the headless device 10 to the controller 11 in order to enable display of the settings of the headless device. This may be advantageous if the transfer speed is low and/or the amount of data to transfer is high.

If there is no concern about amount of data or transfer speed, the settings can be read in full from the headless device 10 together with identifying information for the headless device. In such case there is no need for the database of the server 12 to store the current settings of the headless device. The identifying information may nevertheless be used to retrieve a user interface specification.

The third part 530 of the sequence diagram illustrates a process for making changes to the settings of the headless device 10. The process starts by the user changing one or more of the settings presented on the user interface of the controller 11. When the controller 11 receives the updated settings, it sends a request to the server 12 for signing of the settings. The request may include the updated settings and the device ID of the headless device 10. The processor 41 of the server 12 retrieves the private key associated with the headless device 10 identified by the device ID from the database and digitally signs the settings using the private key before initiating transmission of the digitally signed updated settings to the headless device 10 by returning the updated settings to the controller 11 .

When the controller 11 is activated for communication with the headless device 10, in this example when the user places the controller within the communication range of the headless device, the digitally signed, updated settings are transferred to the headless device, which validates that the settings originates from the trusted server 12 and that they have not been tampered with. In this embodiment, the validation is carried

out by means of a signature verifying algorithm and the public key which is stored in the memory of the headless device and which corresponds to or is paired with the private key used in the server 12 for digitally signing the updated settings. If the headless device 10 confirms the signature of the trusted server 12, the settings are stored in the memory 22d of the headless device 10 and applied by the processor 21 when operating the headless device. The headless device 10 then sends a confirmation to the controller 11 that the updated settings have been successfully applied. If the headless device is unable to confirm that the settings originate from the trusted server 12, they are discarded and a message to that effect is returned to the controller 11.

In one embodiment, the device ID is included in the digitally signed message from the server 12 and the headless device 10 checks the device ID in the message against the device ID stored in its memory to verify that the updated settings are intended for this headless device.

In one embodiment the data storage 44 accessible by the server 12 stores one or more different requirements that the settings for the different headless devices 10 have to comply with. Such requirements may include permitted intervals for numerical values, allowable combinations of settings, and compatibility with a firmware version used in the headless device.

In such case, the processor 41 of the server 12 may be configured to check the received updated settings against the stored requirements in order to make sure that the updated settings can be validly applied to the headless device 10. If the settings pass the check, then the settings are digitally signed as described above. If not, the server 12 may send a message to that effect to the controller 11.

The check of the settings against predetermined requirements for acceptable settings values makes it possible to prevent users from updating settings to settings that would harm the function of the headless device or its environment.

If the data storage 44 mirrors the settings of the headless device 10, as has been described above, the processor 41 of the server 12 updates the data storage 44 with the updated settings, if appropriate after the settings have been successfully tested against the predetermined requirements.

In one embodiment, the processor 41 of the server 12 calculates a delta or a difference between the updated settings and the current settings and only the delta or difference is transferred to the controller 11 and further to the headless device 10.

In an alternative embodiment, the delta is calculated in the controller 11 and only the delta is sent to the server 12.

If a token is used as an indication of the settings currently used in the headless device 10, a new token may be created by the processor 41when the settings are

successfully updated on the server 12. The processor stores the token in the data storage in association with the updated settings and provides for the transmission of the updated token, together with the updated settings, to the headless device 10 via the controller 11.

In the embodiment described in connection with Fig. 5, at least one key pair is created for each headless device 10. Thus the server 12 uses a separate private key for each headless device 10. In another embodiment, a common key pair is created for all the headless devices 10 so that all the headless devices have the same public key and the server has a single private key. When the server 12 is about to digitally sign an updated setting, it uses the common private key and the device ID of the headless device 10 to create a private key that is unique for the headless device. When the headless device 10 is about to validate the digitally signed, updated setting, it uses the common public key and the device ID to generate a public key paired to the unique private key generated by the server 12.

In one embodiment, which provides for increased security, authentication of the user is required before the user is allowed to change the settings of the headless device. The authentication is made in conventional and well-known manner by the user providing proof that he really is who he claims to be.

In another embodiment user authentication is required already for viewing the current settings of the headless device.

The authentication step may also include an implicit or explicit check that the user is authorized to change the settings of the specific headless device.

In user authentication the user has to prove its identity to the server 12. This may be done by the user providing a user name and a password to the server, which checks the name and the password against previously registered information. The name and password may be provided through a user interface of the controller. Other ways to authenticate can be by means of biometrics, such as fingerprints or voice recognition, or by means of one-time codes generated by the controller or a different device.

Authorization is in this case used to establish which headless device(s) 10 a user has the right to interact with. When the user has been authenticated, the server 12 may check the user's authorization against previously registered information associated with the user's identity. Authentication information and authorization information may be stored in a data storage in the server 12 or elsewhere where it is accessible for the server.

As is evident from above, the system described above includes at least three layers of security. A first one is the digital signing by the server 12 of updated settings, which means that the headless device 10 may validate the settings. A second one is the check, by the server 12, of the validity of the updated settings suggested by the user, which

means that unreasonable and harmful settings may be prevented from being applied to the headless device 10. A third one is the requirement for user authentication and/or authorization, which means that only pre-approved and registered users can update settings of a headless device 10.

All information transferred by the different components of the system can be made available unencrypted, encrypted and/or digitally signed depending on how the system has been set up during production.

In the above example, it is suggested that only a token or identifying information is read from the headless device 10 when the user wants to see the current settings and that updated settings are then signed by the server 12 before being transferred to the headless device. However, the idea of mirroring the current settings in the server 12 and only reading a token or identifying information from the headless device 10 may be used independently of the digital signing. The idea may instead be combined by one of the other security layers mentioned above.

The idea may be embodied by a server 12 for managing headless devices 10, comprising a processor 41 which is configured to receive, from a controller 11, which is used to control a headless device 10, identifying information for the headless device 10 and, in response to the receipt thereof, retrieve, using the identifying information, at least one current setting of the headless device 10 and transmit the retrieved at least one current setting to a presentation unit 33 for presentation to a user. The idea may also be embodied by a controller 11 for a headless device 10, comprising a processor 31 which is configured to read identifying information from the headless device 10 and transmit it to a server 12, and to receive , from the server 12, at least one current setting of the headless device 10 identified by the identifying information, and to present the current setting on a presentation unit 33. Also, the idea may be embodied by a method for interacting with a headless device 10, comprising the steps of receiving, from the headless device 10, information identifying the headless device 10; transmitting the identifying information to a server 12; receiving from the server 12, at least one current setting of the headless 10 device identified by the identifying information; and presenting the current setting on a presentation unit 33.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiments, it is to be understood that the invention is not to be limited to the disclosed embodiments, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and the scope of the appended claims.

CLAIMS

1. A server (12) for managing headless devices (10), comprising a processor (41), which is configured to receive, from a controller (11), which is used to control a headless device (10), identifying information for the headless device (10) and at least one updated setting to be applied to the headless device (10), and, in response to the receipt thereof, retrieve secret information using the identifying information for the headless device (10), digitally sign the updated setting with the secret information, and initiate transmission of the digitally signed updated setting to the headless device (10) in order to enable the headless device (10) to validate that the updated setting originates from the server (12) before applying the updated setting.

2. The server of claim 1, wherein the processor (41) is configured to check the validity of the received updated setting against at least one predetermined requirement for a setting of the headless device (10), and to digitally sign the updated setting only if it complies with the predetermined requirement.

3. The server of claim 1 or 2, wherein the secret information is a private key in an asymmetric cryptographic system, the corresponding public key being stored by the headless device (10) and being used for the validation of the updated setting.

4. The server of any one of the preceding claims, wherein the processor (41) is configured to authenticate a user of the controller (11).

5. The server of any one of the preceding claims, wherein the processor (41) is configured to have access to a data storage (44) which stores a current setting of the headless device (10).

6. The server of claim 5, wherein the processor (41) is configured to update the current setting of the headless device (10) in response to the receipt of the updated setting to be applied to the headless device (10).

7. The server of claim 6, wherein the processor (41) is configured to update a token, which is associated with the current setting of the headless device (10) , when the current setting is updated, the processor (41) being configured to provide for the transmission of the updated token to the headless device (10) together with the updated

setting.

8. The server of any one of claims 5-8, wherein the processor (41) is configured to retrieve, in response to the receipt from the controller (11) of identifying information for the headless device (10), the current setting of the headless device (10) and to transmit the current setting to a presentation unit (33) for presentation.

9. The server of any one of the preceding claims, wherein the processor (41) is configured to retrieve, in response to the receipt from the controller (11) of identifying information for the headless device (10), a specification of a user interface for the headless device (10) and to transmit the specification to a presentation unit (33) for presentation of the user interface.

10. A method for managing headless devices (10) , comprising the steps of receiving identifying information for a headless device (10) and at least one updated setting to be applied to the headless device (10), and in response to the receipt thereof, retrieving secret information associated with the identifying information for the headless device (10), and digitally signing the updated setting with the secret information, and initiating transmission of the digitally signed updated setting to the headless device (10) in order to enable the headless device (10) to validate the origin of the updated setting before applying the updated setting.

11. The method of claim 10, further comprising the steps of checking the validity of the received updated setting against at least one predetermined requirement for a setting of the headless device (10), and digitally signing the updated setting only if it complies with the predetermined requirement.

12. The method of claim 10 or 11, wherein the secret information is a private key in an asymmetric cryptographic system, the corresponding public key being stored by the headless device and being used for the validation of the updated setting

13. The method of claim 10 or 11, further comprising the step of authenticating a user of the headless device (10).

14. A headless device (10), comprising a processor (21) and a memory (22b) storing security information, wherein the processor is configured to receive a digitally signed, updated setting, which has been digitally signed by a server (12) using secret information of the server, and to validate, using the security information, the origin of the updated

setting, and to apply the updated setting only if it is validated that the updated setting originates from the server (12).

15. The headless device of claim 14, wherein the security information comprises a public key of an asymmetric cryptographic system, the corresponding private key being stored by the server (12) and being used to digitally sign the updated setting.

16. The headless device of claim 14 or 15, wherein the processor (21) is configured to receive, together with the digitally signed, updated setting, information identifying the headless device (10) and to use the received identifying information to check that the updated setting relates to the headless device (10).

17. The headless device according to any one of claims 14-16, comprising a communication unit (23) for short-range communication with a controller of the headless device.

18. The headless device according to claim 17, wherein the communication unit (23) is a near-field communication (NFC) unit.

19. A method in a headless device (10), comprising the steps of receiving a digitally signed, updated setting, which has been digitally signed by a server (12) using secret information of the server; validating, using security information stored in the headless device (10), the origin of the updated setting; and applying the updated setting only if it is validated that the updated setting originates from the server (12).

20. The method of claim 19, further comprising the step of receiving, together with the digitally signed, updated setting, information identifying the headless device (10) and using the received identifying information to check that the updated setting relates to the headless device (10).

21. A controller (11) for controlling a headless device (10), comprising a processor (31), which is configured to receive from a user, at least one updated setting to be applied in the headless device (10), transfer the updated setting, together with information identifying the headless device, to a server (12) with a request for digital signing of the updated setting; to receive from the server (12) the requested digitally signed, updated setting, and to transfer the digitally signed, updated setting to the headless device (10) in order to enable the headless device (10) to validate that the updated setting originates from the predetermined server (12) before applying the updated setting.

22. The controller of claim 21, wherein the processor (31) is configured to receive the identifying information from the headless device (10); to transfer the identifying information to the predetermined server(12); to receive in response thereto, a current setting of the headless device (10) and to present the current setting on a presentation unit (33)of the controller.

23. A method for managing a headless device (10), comprising the steps of receiving, from a user, at least one updated setting to be applied in the headless device (10), transferring the updated setting, together with information identifying the headless device (10), to a server (12) with a request for digital signing of the updated setting; receiving from the server (12) the requested digitally signed, updated setting; and transferring the digitally signed, updated setting to the headless device (10) in order to enable the headless device (10) to validate that the updated setting originates from the predetermined server (12) before applying the updated setting.

24. The method of claim 23, further comprising the steps of receiving the identifying information from the headless device (10); transferring the identifying information to the predetermined server (12); receiving in response thereto, a current setting of the headless device (10) and presenting the current setting on a presentation unit.

25. The method of claim 23 or 24, further comprising the step of receiving, from the server (12), a user interface specification for the headless device (10) and rendering a user interface according to the specification.

26. The method of any one of claims 23 – 25, further comprising the step of authenticating the user.

27. A computer-readable medium storing instructions which, when executed by a computer, cause the computer to perform a method according to any one of claims 23-36.

28. A smartphone, comprising a computer-readable medium according to claim 27.

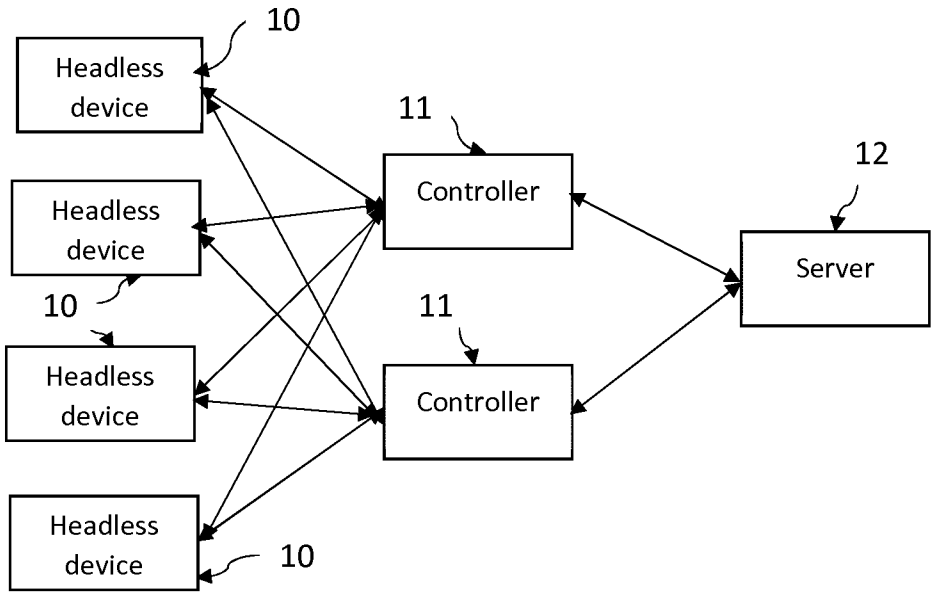
10
Headless device
11
Controller
12
Server
Headless device
10
11
Headless device
Controller
Headless device
10

FIG. 1

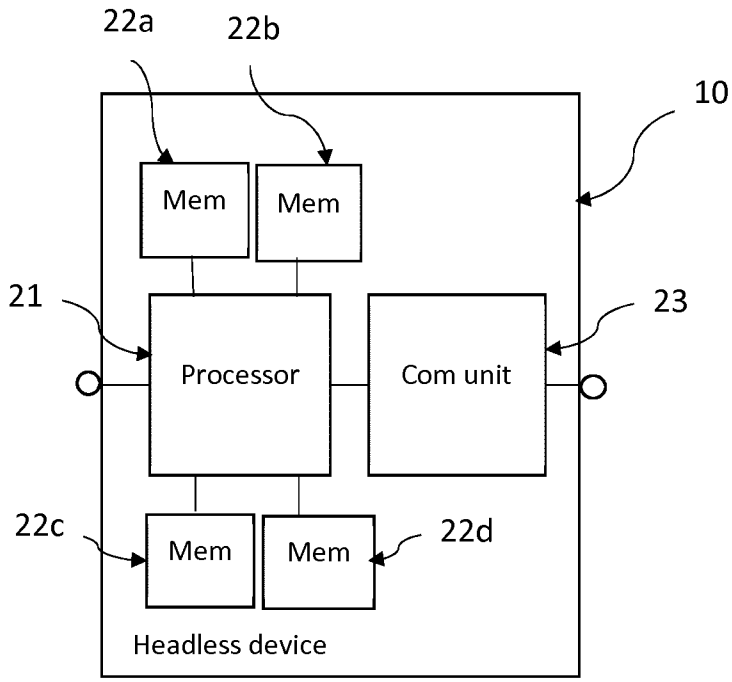
22a
22b
10
Mem
Mem
21
23
Processor
Com unit
22c
Mem
Mem
22d
Headless device

FIG. 2

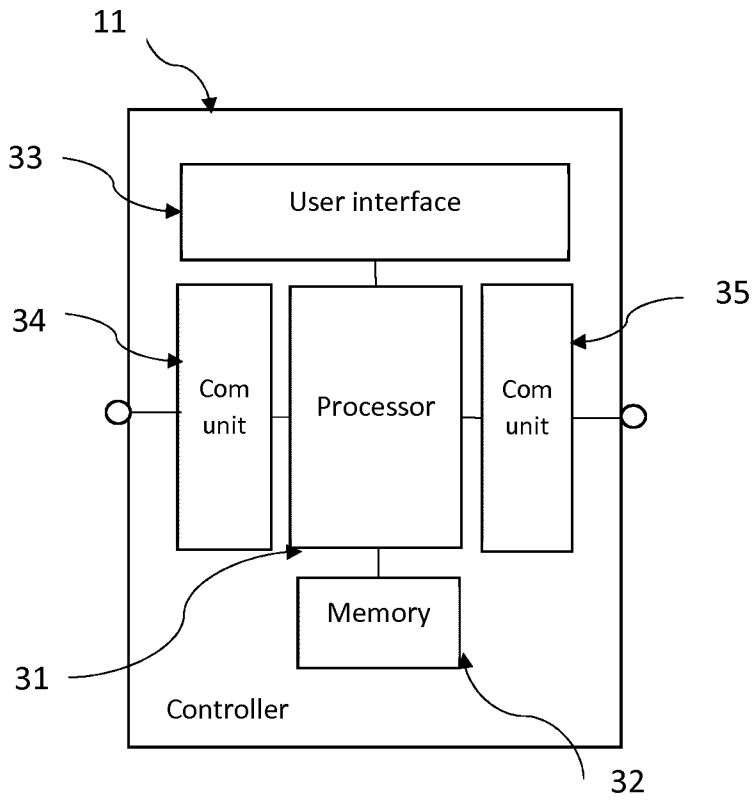
11
33
User interface
34
35
Com unit
Processor
Com unit
Memory
31
Controller
32

FIG. 3

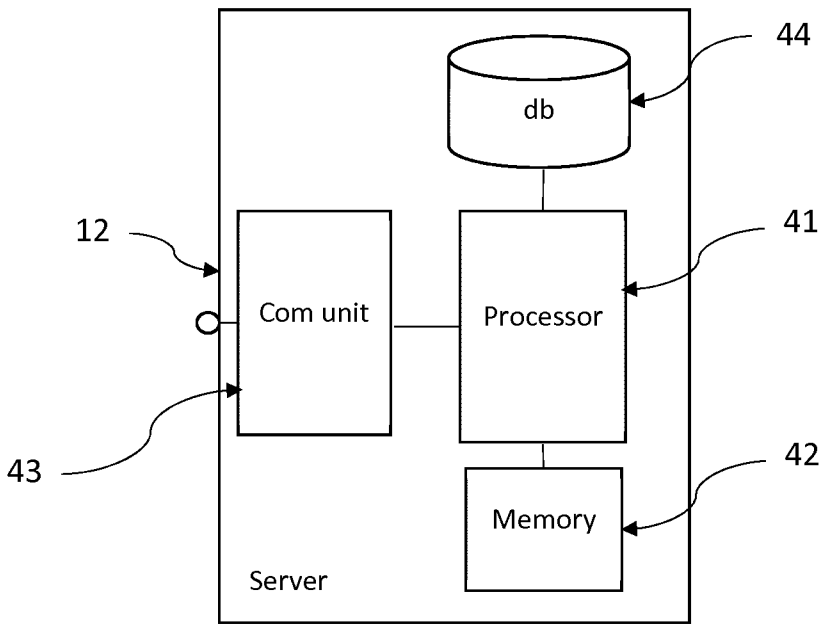
44
db
12
41
Com unit
Processor
43
42
Memory
Server

FIG. 4

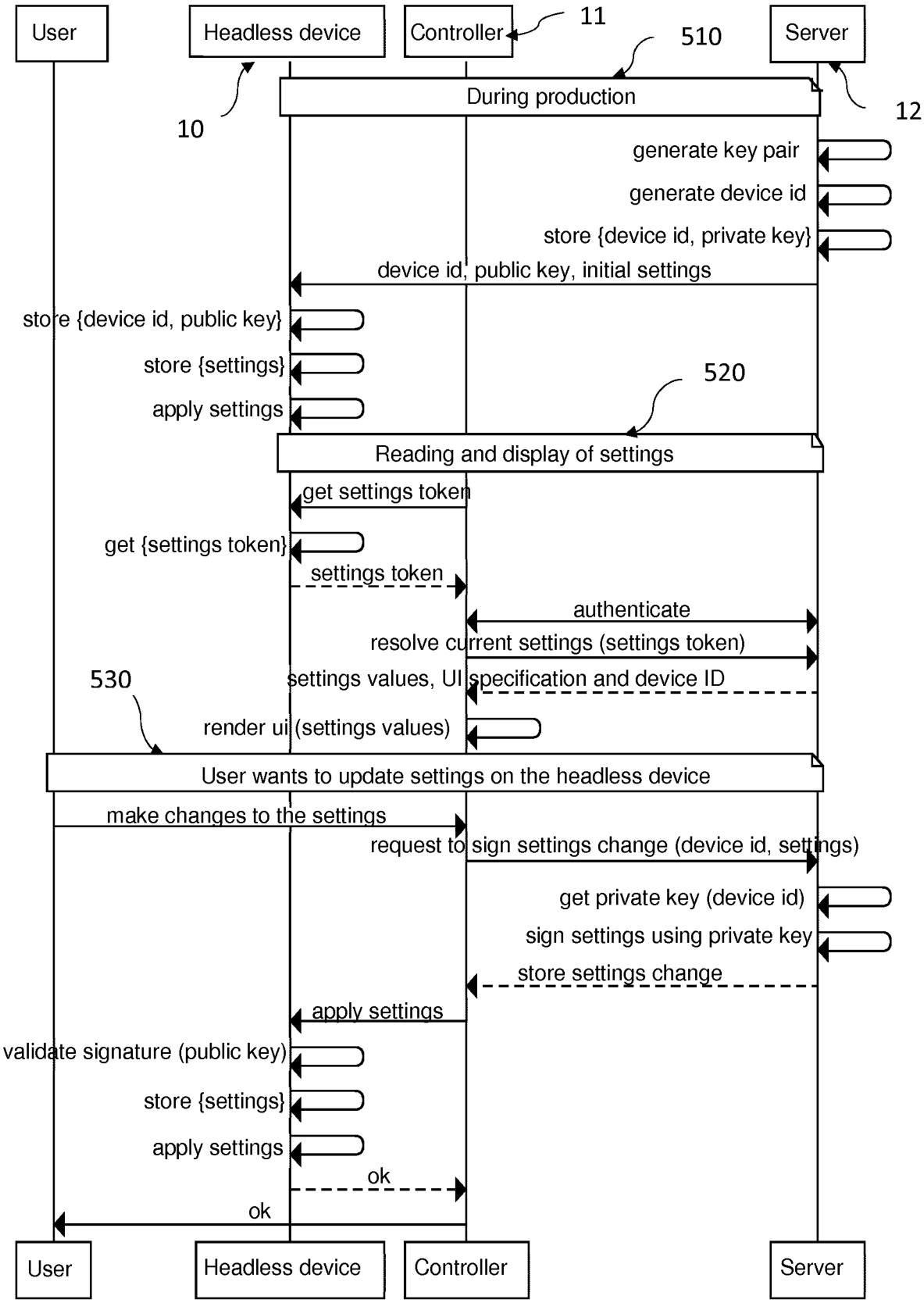
User
Headless device
Controller
11
510
Server
10
During production
12
generate key pair
generate device id
store {device id, private key}
device id, public key, initial settings
store {device id, public key}
store {settings}
apply settings
520
Reading and display of settings
get settings token
get {settings token}
settings token
authenticate
resolve current settings (settings token)
530
settings values, UI specification and device ID
render ui (settings values)
User wants to update settings on the headless device
make changes to the settings
request to sign settings change (device id, settings)
get private key (device id)
sign settings using private key
store settings change
apply settings
validate signature (public key)
store {settings}
apply settings
ok
ok
User
Headless device
Controller
Server

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/068197

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/10 G06F21/64 H04L9/32 H04L29/06 G06F21/57
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W G06F H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/271208 A1 (GALLANT ROBERT PHILIP [CA] ET AL) 24 September 2015 (2015-09-24) abstract paragraph [0051] - paragraph [0064] claim 1 figures 1, 2, 4-6	1-28
A	US 2017/180391 A1 (HINCHLIFFE ALEXANDER J [US] ET AL) 22 June 2017 (2017-06-22) the whole document	1-28
A	US 2010/275026 A1 (MCLEAN IVAN H [US]) 28 October 2010 (2010-10-28) the whole document	1-28

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 March 2018	14/03/2018

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/068197

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015271208 A1	24-09-2015	US 2015271208 A1	24-09-2015
		WO 2015143554 A1	01-10-2015
US 2017180391 A1	22-06-2017	US 2017180391 A1	22-06-2017
		WO 2017112152 A1	29-06-2017
US 2010275026 A1	28-10-2010	CN 102414689 A	11-04-2012
		EP 2425367 A1	07-03-2012
		JP 5743227 B2	01-07-2015
		JP 2012524954 A	18-10-2012
		KR 20120004536 A	12-01-2012
		US 2010275026 A1	28-10-2010
		WO 2010126837 A1	04-11-2010