



- (51) **International Patent Classification:**
G06F 8/61 (2018.01) G06F 9/4401 (2018.01)
- (21) **International Application Number:**
PCT/US2021/027673
- (22) **International Filing Date:**
16 April 2021 (16.04.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant: HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Dr., Spring, Texas 77389 (US).
- (72) **Inventors: RETNAMONI BRADUKE, Rosilet;** 10300 Energy DR, Spring, Texas 77389 (US). **LIU, Wei Ze;** 10300 Energy DR, Spring, Texas 77389 (US). **SHAH, Rajesh;** 10300 Energy DR, Spring, Texas 77389 (US).
- (74) **Agent: JENNEY, Michael et al.;** HP Inc., Mail Stop 35, 3390 E Harmony Rd, Fort Collins, Colorado 80528 (US).
- (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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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).

Declarations under Rule 4.17:

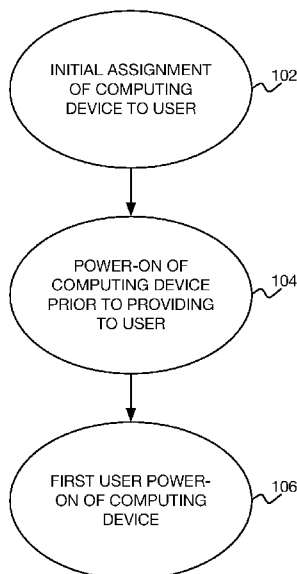
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) **Title:** OPERATING SYSTEM CONFIGURATION AND REGISTRATION WITHOUT MANUAL USER INPUT OR INTERACTION AT COMPUTING DEVICE

FIG 1



(57) **Abstract:** A computing device includes a storage device storing an operating system, and a secure storage device storing previously user-provided configuration information for the operating system, a username, and a security token. The computing device includes a processor, and a memory storing instructions executable by the processor. The instructions are executable to, at first user power-on of the computing device, automatically configure the operating system according to the previously user-provided configuration information so that the operating system is configured without manual user input at the computing device. The instructions are executable to automatically register the operating system with the username and with the security token as a single-use password without user interaction.

WO 2022/220840 A1

OPERATING SYSTEM CONFIGURATION AND REGISTRATION WITHOUT MANUAL USER INPUT OR INTERACTION AT COMPUTING DEVICE

BACKGROUND

[0001] Computing devices used by end users include desktop, laptop, and
5 notebook computers, as well as smartphones, tablet computing devices, and
other types of computing devices. A computing device generally includes an
operating system, which is the computer program that manages hardware and
software resources, and provides common services for other computer programs
running on the computing device. Before a user can use a computing device for
10 the first time, therefore, an operating system usually has to be installed and
configured on the computing device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. 1 is a diagram of examples stages in relation to which
automatic configuration and registration of a computing device's operating
15 system without manual user input or interaction at the computing device can
be provided.

[0003] FIG. 2 is a diagram of example automatic configuration and
registration of a computing device's operating system without manual user input
or registration at the computing device.

20 **[0004]** FIG. 3 is a diagram of an example non-transitory computer-
readable data storage medium storing program code to acquire configuration and
other information in accordance with which a computing device's operating

system can be subsequently automatically configured and registered without manual user input or interaction at the computing device.

[0005] FIG. 4 is a flowchart of an example method for storing, on a secure storage device of the computing device, previously user-provided configuration and other information for automatically configuring and registering the operating system of a computing device, prior to providing the computing device to a user.

[0006] FIG. 5 is a diagram of an example computing device that can have its operating system automatically configured and registered according to previously user-provided configuration and other information stored on a secure storage device of the computing device, without manual user input or interaction at the computing device.

DETAILED DESCRIPTION

[0007] Before a user can use a computing device for the first time, the operating system of the computing device has to be installed and configured.

15 For instance, when the user powers on the computing device for the first time, the user may have to input configuration information such as the geographic region in which the user is using the computing device, the language in which the computing device is to be used (English, Spanish, Mandarin, and so on), and the keyboard layout of the computing device (US, UK, and so on). The user may
20 also have to input the name of the wireless network with which the computing device is to connect, as well as the password for this network. The user may further provide a username, such as an email address, and a password for

registering the operating system and thus by which the user will subsequently log onto the operating system.

[0008] Such initial configuration and registration of the computing device's operating system can be laborious. Not all the information may be solicited from the user at the beginning of the configuration and registration process. Rather, the user may be prompted for the information over a period of extend that can exceed 10, 20, 30, or more minutes, as the operating system is installed, updated, and/or configured. For example, once the wireless network information has been received, the operating system may proceed to acquire and install operating system updates, and may reboot one or multiple times, before other information is requested from the user. The user, therefore, cannot simply turn on the computing device and walk away until operating system configuration and registration have been completed, but rather must attend to the computing device throughout this process until the device is ready for use.

[0009] Techniques described herein ameliorate these and other issues. A computing device includes a secure storage device storing previously user-provided configuration for the operating system, a username, and a security token. At first user power-on of the computing device, the operating system of the computing device is automatically configured according to the previously user-provided configuration information without manual user input of such information at the computing device. The operating system is automatically registered with the username and the security token without user interaction,

where the security token serves as a single-use password for logging into the operating system.

[0010] Therefore, the first time the user powers on the computing device, the user can simply walk away from the device instead of having to attend to the computing device while configuration and registration of the operating system occur. When the user returns after configuration and registration have been completed, the user may encounter the operating system presenting a login screen at which the user can enter the username and an operating system password. Responsive to the user entering the username and the security token (the latter serving as the operating system password), the operating system may prompt the user to change the operating system password to something else. After this user does this, the user can begin using the computing device. The initial operating system configuration and registration process thus occurs with reduced user inconvenience.

[0011] FIG. 1 shows the three example stages 102, 104, and 106 in relation to which the techniques described herein can provide automatic configuration and registration of a computing device's operating system without manual input or interaction at the computing device. The first stage 102 corresponds to initial assignment of the computing device to a user, prior to the user being provided the device. For example, in an enterprise environment the first stage 102 may occur when the user is being assigned a new computer, and has logged into a web site to provide configuration and other information for the new computer's operating system prior to receiving the new computer. As

another example, in a home environment the first stage 102 may occur when the user has purchased a new computer online via a web site, and as part of this process provides configuration and other information for the new computer's operating system. In both these examples, the first stage 102 can thus occur
5 incident to a procurement process initiated by the user in relation to the computing device.

[0012] The second stage 104 occurs after the first stage 102 has been completed, and corresponds to power-on of the computing device before the computing device is provided to the user. For example, in an enterprise
10 environment the second stage 104 may occur when the computing device assigned to the user has been turned on by an administrator or another user other than the user to which the computing device has been assigned, to store the previously user-provided configuration and other information on a secure storage device of the computing device. As another example, in a home
15 environment the second stage 104 may occur when the computing device is turned on at the factory at which the computing device is being manufactured or otherwise prepared for shipment or delivery to the user, to store the previously user-provided configuration and other information on a secure storage device of the computing device. The second stage 104 thus occurs prior to the user being
20 provided the computing device.

[0013] The third stage 106 occurs after the second stage 104 has been completed, and corresponds to the first time the user powers on the computing device upon the user having been provided the computing device. For example,

in both an enterprise environment and a home environment, the third stage 106 may occur once the user has received the computing device and has turned the device on for the first time. In the third stage 106, the operating system of the computing device is automatically configured and registered using the previously
5 user-provided information stored on the computing device's secure storage device, without user input of this information at the computing device and without user interaction. After the user initiates power-on for the first time, therefore, the user does not have to attend to the computing device to configure and register the operating system.

10 **[0014]** FIG. 2 illustratively shows example automatic configuration and registration of a computing device's operating system without manual user input or interaction at the computing device. A user 202 has an existing user device 204, which may be a computing device like a desktop, laptop, or notebook computer, a smartphone, a tablet computing device, or another type of
15 computing device. The user device 204 is communicatively connected to a procurement server 206 via a network 208. The procurement server 206 may be, for instance, an electronic commerce server by which the user 202 can purchase a new computing device 210, a corporate server by which the user 202 can obtain the new computing device 210 in the context of the user 202's
20 employment, and so on. The network 208 may be or include the Internet, an intranet, an extranet, a local-area network (LAN), a wide-area network (WAN), a wired network, a wireless network, and so on.

[0015] The computing device 210 can be assigned to the user incident to the procurement process initiated by the user 202 in relation to the computing device 210 via communicating with the procurement server 206 over the network 208 using the existing user device 204. The procurement server 206 prompts the user for configuration information 212 in accordance with which an operating system 234 of the computing device 210 is to be configured at first user power-on of the device 210 upon receipt of the computing device 210 by the user. The procurement server 206 also prompts the user for a username 214 in accordance with which the operating system 234 is to be registered and thus used to log onto the operating system 234.

[0016] As noted above, the configuration information 212 can include the geographic region in which the user is using the computing device 210, the language in which the computing device 210 is to be used (English, Spanish, Mandarin, and so on), and the keyboard layout of the computing device 210 (US, UK, and so on). The configuration information 212 can include the name of the wireless network with which the computing device 210 is to connect when received by the user, as well as the password for this network. The configuration information 212 can include other information as well. The username 214 may be in the form of an email address of the user 202 by which the user will subsequently log onto the operating system 234.

[0017] The user 202 enters the requested configuration information 212 and username 214 at the user device 204, which transmits the information 212 and the username 214 to the procurement server 206 over the network 208, per

arrows 216. The procurement server 206 generates a security token 218, which serves as a single-use or one-time password in accordance with which the operating system 234 of the computing device 210 is to be registered (along with the username 214) at first user power-on of the device 210 upon the user 202 receiving the computing device 210. The security token 218 may be a random string of characters, for instance.

[0018] The procurement server 206 transmits the security token 218 to the user 202 via the provided username 214, per arrows 220. For instance, the procurement server 206 may send an email to the username 214 of the user 202 that includes the security token 218. More generally, the procurement server 206 may transmit the security token 218 to the user 202's existing user device 204 over the network 208.

[0019] The procurement server 206 is communicatively connected to a configuration server 222, as indicated by dashed line 224. For instance, the procurement server 206 may be communicatively connected to the configuration server 222 by the network 208 or via a different network. The configuration server 222 may be a different server than the procurement server 206, as in the example of FIG. 2, or may be the same server as the procurement server 206.

[0020] The procurement server 206 stores the received configuration information 212 and username 214, and the generated security token 218, on the configuration server 222, per arrows 226. The entry of the configuration information 212 and the username 214 by the user 202, the generation of the security token 218 by the procurement server 206, and the storage of the

information 212, the username 214, and the security token 218 on the configuration server 222, occur during the first stage 102 of FIG. 1. That is, such entry and storage of the configuration information 212 and the username 214, and such generation and storage of the security token 218, occur during or as
5 part of initial assignment of the computing device 210 to the user 202.

[0021] Then, during the power-on of the computing device 210 prior to providing the device 210 to the user – i.e., during the second stage 104 of FIG. 1 – the computing device 210 is communicatively connected to the configuration server 222, as indicated by the dashed line 228. At this time, the computing
10 device 210 is caused to retrieve the previously user-provided configuration information 212, the username 214, and the security token 218 from the configuration server 222, per arrows 230. The computing device 210 is further caused to store the retrieved configuration information 212, username 214, and security token 218 to a secure storage device 232 of the computing device 210.
15 Upon such storage, the computing device 210 can be powered down and provided to the user 202, as indicated by arrow 236. For example, the computing device 210 may be shipped to the user 202.

[0022] Thereafter, during the first user power-on of the computing device 210 – i.e., during the third stage 106 of FIG. 1 – the computing device 210
20 automatically configures its operating system 234 in accordance with the previously user-provided configuration information 212 stored on the secure storage device 232 without manual user input of this information 212 at the device 210 itself. The computing device 210 further automatically registers the

operating system with the username 214 and with the security token 218, where the latter serves as a single-use password, without user interaction at the device 210.

[0023] The user 202 therefore does not have to attend to the configuration and registration of the operating system 234 during this time, and can instead walk away. When the user 202 returns to the computing device 210 upon completion of such configuration and registration, the user 202 can immediately begin using the device 210 upon entry of the username 214 and the security token 218 as the operating system password, and after changing the password to something different than the token 218 when prompted by the operating system. Therefore, the initial user experience of the computing device 210 is improved, and the computing device 210 is technologically improved insofar as its operating system 234 configuration and registration process is improved.

[0024] FIG. 3 shows an example non-transitory computer-readable data storage medium 300 storing program code 302 executable by a processor to perform processing to acquire configuration and other information in accordance with which a computing device's operating system can be subsequently automatically configured and registered without user input or interaction at the computing device itself. The processing may be performed in stage 102 of FIG. 1. The processor executing the program code 302 may be part of the procurement server 206 of FIG. 2.

[0025] The processing includes, prior to providing a computing device to a user, prompting the user for configuration information in accordance with which

an operating system of the computing device is to be automatically configured at first user power-on of the computing device without manual user input at the computing device (304). The processing includes responsively receiving the configuration information from the user (306). The processing includes, also
5 prior to providing the computing device to the user, prompting the user for a username with which the operating system is to be automatically registered at the first user power-on of the computing device without user interaction (308). The processing includes responsively receiving the username from the user (310). The prompting of parts 304 and 308 may be performed incident to a
10 procurement process initiated by the user in relation to the computing device, as has been described above.

[0026] The processing includes generating a security token as a single-use password with which the operating system is to be automatically registered at the first user power-on of the computing device without user interaction (312).
15 The processing includes storing the configuration information, the username, and the security token on a server for retrieval by and subsequent storage on the computing device at power-on of the computing device prior to providing the computing device to the user (314). The server on which the configuration information, username, and security token are stored may be the configuration
20 server 222 of FIG. 2. The processing includes sending the security token to the username for entry by the user after configuration and registration of the operating system at the first user power-on of the computing device (316).

[0027] FIG. 4 shows an example method 400 for storing, on a secure storage device of a computing device, previously user-provided configuration and other information for automatically configuring and registering the operating system of the computing device, prior to providing the computing device to a user.

5 The method 400 may be performed in stage 104 of FIG. 1. The method 400 is thus performed after the processing of FIG. 3 has been performed. The method 400 may be implemented at least in part as program code stored on a non-transitory computer program data storage medium and executable by a processor.

10 **[0028]** The method 400 includes, upon initial assignment of a computing device to a user, performing power-on of the computing device prior to providing the computing device to the user (402). The initial assignment of the computing device may have been achieved incident to a procurement process initiated by the user in relation to the computing device, as has been described. The method

15 400 includes, upon such power-on of the computing device, causing the computing device to retrieve previously user-provided configuration information, a username, and a security token from a server (404). For example, the computing device may have stored thereon instructions, such that upon power-on of the device, the computing device automatically executes the instructions.

20 The server from which the configuration information, username, and security token are retrieved may be the configuration server 222 of FIG. 2.

[0029] The configuration information is that in accordance with which an operating system of the computing device is to be automatically configured at

first user power-on of the computing device without manual user input at the computing device. The username is that with which the operating system is to be automatically registered at the first user power-on without user interaction. The security token is that, as a single-use password, with which the operating system
5 is to be automatically registered at the first user power-on without the user interaction.

[0030] The method 400 includes responsively causing the computing device to store the previously user-provided configuration information, the username, and the security token that have been retrieved from the server on a
10 secure storage device of the computing device (406). For example, the computing device may have stored thereon instructions such that upon power-on of the device, the computing device automatically executes the instructions after the configuration information, the username, and the security token have been retrieved. The secure storage device may be an endpoint security controller
15 (EpSC) of the computing device. The secure storage device is more generally a storage device that stores the configuration information, the username, and the security token in a secure manner – i.e., in an encrypted or other manner.

[0031] The computing device may store the configuration information, the username, and the security token using a management instrumentation service
20 provided by the operating system of the computing device. Such a service may provide an environment-independent specification by which management information can be shared within the computing device. In the context of the

MICROSOFT WINDOWS operating system, for instance, the service may be the Windows Management Instrumentation (WMI) service.

[0032] The method 400 includes then performing power-down of the computing device and providing the computing device to the user (408). That is, once the configuration information, username, and security token have been stored on the computing device's secure storage device, the computing device can be made ready for providing to the user and then powered down. The computing device may be provided to the user by shipping the device to the user, for instance.

10 **[0033]** FIG. 5 shows an example computing device 210 that can have its operating system 234 automatically configured and registered without manual user input or interaction at the device 210. The computing device 210 includes a storage device 502 storing the operating system 234, such as a hard disk drive, solid state drive, or another type of storage device. The computing device 210 includes a secure storage device 232, such as an EpSC, storing previously user-provided configuration information 212 for the operating system 234, a username 214, and a security token 218 that were previously stored on the secure storage device 232. The computing device 210 includes a processor 504 and a memory 506 storing instructions 508 executable by the processor 504. The computing device 210 can include other components, in addition to those shown in FIG. 4.

20 **[0034]** The instructions 508 are executable by the processor 504 at first user power-on of the computing device 210 (i.e., once the computing device 210 has been provided to the user). The instructions 508 are thus executable after

the method 400 of FIG. 4 has been performed, and the computing device 210 may have been configured as part of readying the device 210 for providing to the user within the method 400 to execute the instructions 508 the next time the device 210 is powered on (i.e., the first power-on by the user). The instructions
5 508 are therefore executed in stage 106 of FIG. 1.

[0035] The instructions 508 are specifically executed by the processor 504 to, at first user power-on of the computing device 210, initially install and/or first-time execute the operating system 234 (510). For example, when the computing device 210 is readied for providing to the user within the method 400, the
10 operating system 234 may be placed in a partially or completely uninstalled state. Therefore, when the computing device 210 is powered on by the user for the first time, the operating system 234 is installed and subsequently executed. In another implementation, the operating system 234 may not be in a partially or completely uninstalled state, in which case when the computing device 210 is
15 powered on by the user for the first time, the operating system 234 is (just) executed for the first time by the user.

[0036] The instructions 508 are executed by the processor 504 to retrieve the previously user-provided configuration information 212, the username 214, and the security token 218 from the secure storage device 232 (512). For
20 example, a management instrumentation service, such as the WMI service in the case of the MICROSOFT WINDOWS operating system, may be used to retrieve the configuration information 212, username 214, and security token 218 from the storage device 232. The instructions 508 may be executed to retrieve the

configuration information 212, the username 214, and the security token 218 as part of or during initial installation and/or first-time execution of the operating system 234.

[0037] The instructions 508 are executed by the processor 504 to then
5 automatically configure the operating system 234 according to the retrieved configuration information 212 (514), such that the operating system 234 is configured without manual user input of the configuration information 212 at the computing device 210. That is, whereas if the configuration information 212 were not present the operating system 234 would have to prompt the user to enter the
10 information 212, because the configuration information 212 has been retrieved from the secure storage device 232, the operating system 234 does not have to prompt the user in this respect. The instructions 508 may be executed to automatically configure the operating system 234 according to the configuration information 212 as part of or during initial installation and/or first-time execution
15 of the operating system 234.

[0038] The instructions 508 are executable by the processor 504 to further automatically register the operating system 234 with the retrieved username 214 and with the retrieved security token 218 (the latter as a single-use password) without user interaction (516). Registration of the operating system 234 in this
20 respect can include creating a user account for usage of the operating system 234, where the user account is associated with the username 214 and with the security token 218 (the latter as a single-use password). Therefore, whereas if the username 214 and the security token 218 were not present the operating

system 234 would have to prompt the user for the username 214 and an operating system password to create a user account for usage of the operating system 234, because the username 214 and the security token 218 have been retrieved from the secure storage device 232, user interaction in this respect is avoided. The instructions 508 may be executed to automatically register the operating system 234 using the username 214 and the security token 218 as part of or during initial installation and/or first-time execution of the operating system 234.

[0039] The instructions 508 are executable by the processor 504 to, at completion of configuration and registration of the operating system 234, cause the operating system 234 to present a login screen at which a user can enter the username 214 and an operating system password, and responsive to user entry of the username 214 and the security token 218 as the password, prompt the user to change the operating system password (518). That is, once the operating system 234 has been configured and registered, the operating system 234 may be rebooted or otherwise executed in such a way that it can now be used by the user. Therefore, the operating system 234 presents the login screen so that the user can for the first time log into the user account created during operating system 234 registration. Because the security token 218 has been specified as a single-use password during such registration, the user has to enter a new password before he or she can actually use the operating system 234.

[0040] Techniques have been described for configuration and registration of an operating system of a computing device without manual user input or

interaction at the device. Configuration information and a username instead are received from the user at time of initial assignment of the computing device to the user, before the device has been provided to the user. The configuration information and the username, along with a generated security token that serves
5 as a single-use password for the operating system, are stored in a secure storage device of the computing device prior to providing the computing device to the user. At first user power-on, therefore, the operating system is automatically configured using the stored configuration information and is automatically registered using the stored username and token.

10

We claim:

1. A computing device comprising:
 - a storage device storing an operating system;
 - a secure storage device storing previously user-provided configuration
- 5 information for the operating system, a username, and a security token;
 - a processor; and
 - a memory storing instructions executable by the processor to:
 - at first user power-on of the computing device, automatically
 - configure the operating system according to the previously user-provided
 - 10 configuration information so that the operating system is configured without
 - manual user input at the computing device; and
 - automatically register the operating system with the username and
 - with the security token as a single-use password without user interaction.
2. The computing device of claim 1, wherein the instructions are executable
- 15 by the processor to further:
 - at the first user power-on of the computing device, first-time execute the
 - operating system on the computing device,
 - wherein automatic configuration and registration of the operating system
 - occur during first-time execution of the operating system.
- 20 3. The computing device of claim 2, wherein the instructions are executable
- by the processor to further:

at the first user power-on of the computing device, initially install the operating system on the computing device prior to the first-time execution the operating system,

wherein the automatic configuration of the operating system according to
5 the previously user-provided configuration information further occurs during installation of the operating system.

4. The computing device of claim 1, wherein the instructions are executed as part of first-time execution and/or initial installation of the operating system on the computing device.

10 5. The computing device of claim 1, wherein at completion of automatic configuration and registration of the operating system, the operating system is to:
present a login screen at which a user is to enter the username and an operating system password; and
responsive to user entry of the username and of the security token as the
15 operating system password, prompt the user to change the operating system password.

6. The computing device of claim 1, wherein the instructions are executable to further:
retrieve the previously user-provided configuration information for the
20 operating system, the username, and the security token from the secure storage device.

7. The computing device of claim 6, wherein the previously user-provided configuration information for the operating system, the username, and the security token are retrieved from the secure storage device via a management instrumentation service provided by the operating system.

5 8. The computing device of claim 1, wherein the secure storage device comprises an endpoint storage controller.

9. A method comprising:

upon initial assignment of a computing device to a user, performing power-on of the computing device prior to providing the computing device to the
10 user;

upon the power-on of the computing device, causing the computing device to retrieve, from a server:

previously user-provided configuration information in accordance with which an operating system of the computing device is to be automatically
15 configured at first user power-on of the computing device without manual user input at the computing device;

a username with which the operating system is to be automatically registered at the first user power-on without user interaction; and

a security token as a single-use password with which the operating
20 system is to be automatically registered at the first user power-on without the user interaction;

responsively causing the computing device to store the previously user-

provided configuration information, the username, and the security token that have been retrieved from the server on a secure storage device of the computing device; and

performing power-down of the computing device and providing the
5 computing device to the user.

10. The method of claim 9, wherein the computing device is caused to retrieve, from the server, the previously user-provided configuration information, the username, and the security token via the computing device automatically executing instructions upon the power-on of the computing device.

10 11. The method of claim 9, wherein the computing device is responsively caused to store the previously user-provided configuration information, the username, and the security token that have been retrieved from the server on the secure storage device via the computing device automatically executing instructions upon the power-on of the computing device.

15 12. The method of claim 11, wherein the computing device stores the previously user-provided configuration information, the username, and the security token that have been retrieved from the server on the secure storage device via a management instrumentation service provided by the operating system.

13. The method of claim 9, wherein the computing device is initially assigned to the user incident to a procurement process initiated by the user in relation to the computing device.

14. A non-transitory computer-readable data storage medium storing program
5 instructions executable by a processor to perform processing comprising:

prior to providing a computing device to a user, prompting the user for,
and responsively receiving from the user, configuration information in accordance
with which an operating system of the computing device is to be automatically
configured at first user power-on of the computing device without manual user
10 input at the computing device;

prior to providing the computing device to the user, prompting the user for,
and responsively receiving from the user, a username with which the operating
system is to be automatically registered at the first user power-on of the
computing device without user interaction;

15 generating a security token as a single-use password with which the
operating system is to be automatically registered at the first user power-on of
the computing device without user interaction;

storing the configuration information, the username, and the security token
on a server for retrieval by and subsequent storage on the computing device at
20 power-on of the computing device prior to providing the computing device to the
user;

sending the security token to the username for entry by the user after

configuration and registration of the operating system at the first user power-on of the computing device.

15. The non-transitory computer-readable data storage medium of claim 14,
wherein the user is prompted for the configuration information incident to a
5 procurement process initiated by the user in relation to the computing device.

FIG 1

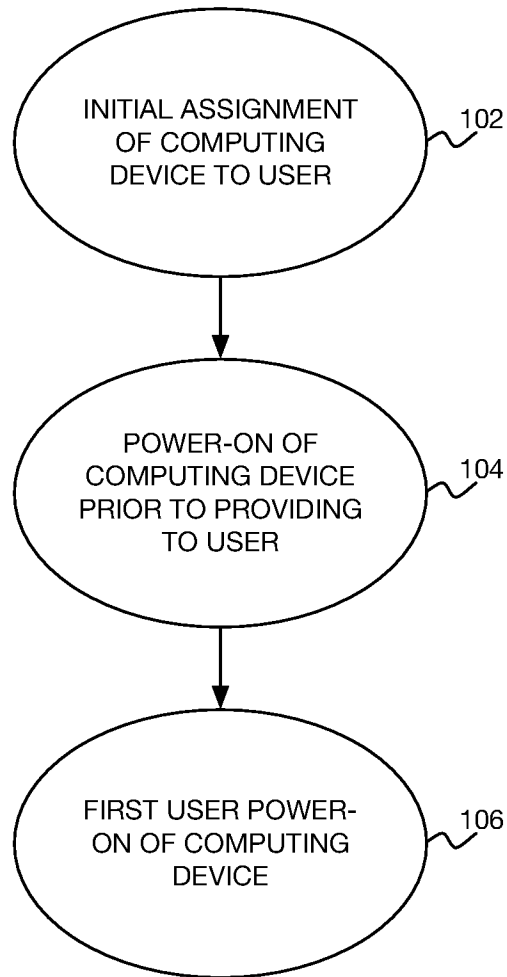


FIG 2

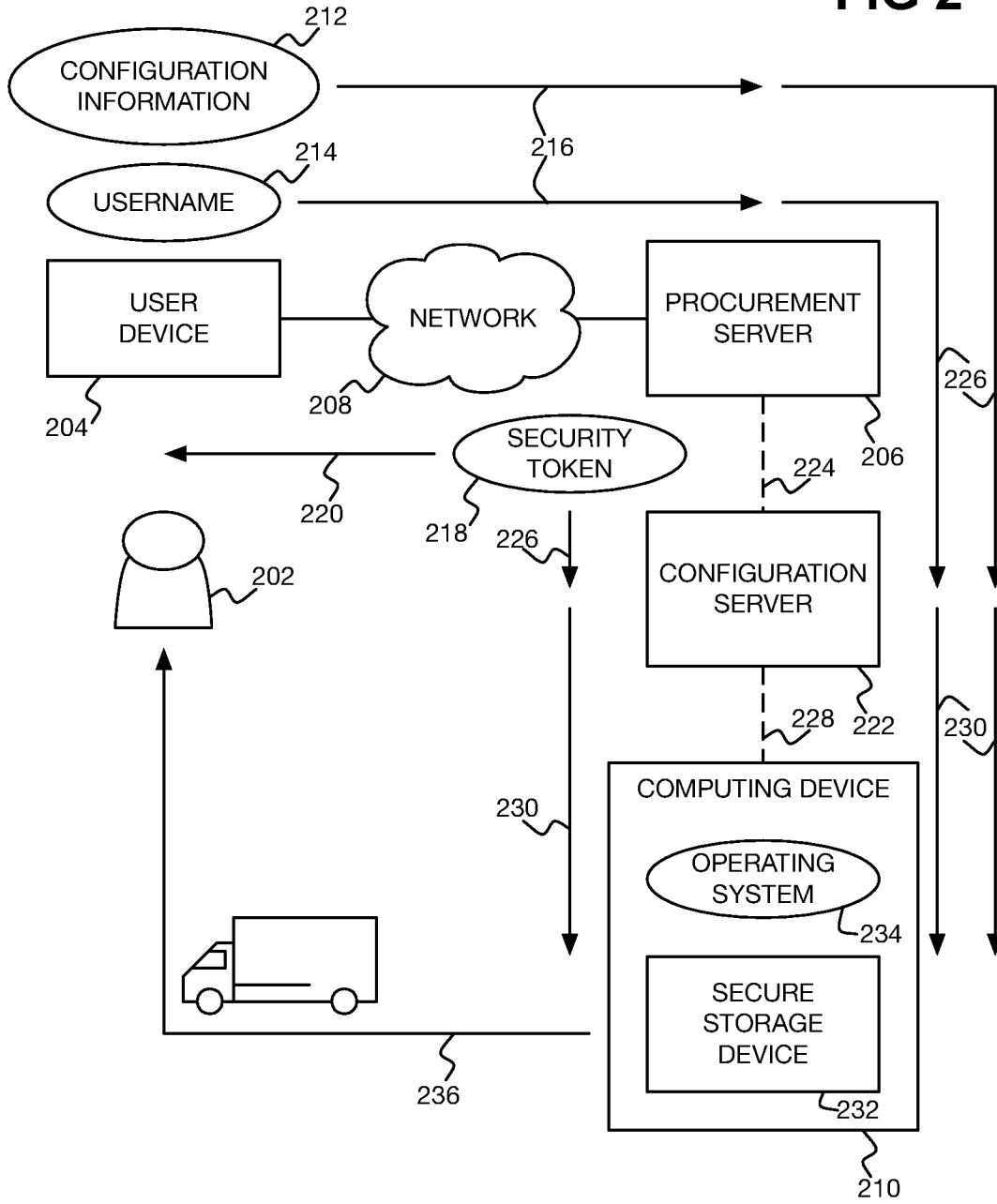


FIG 3

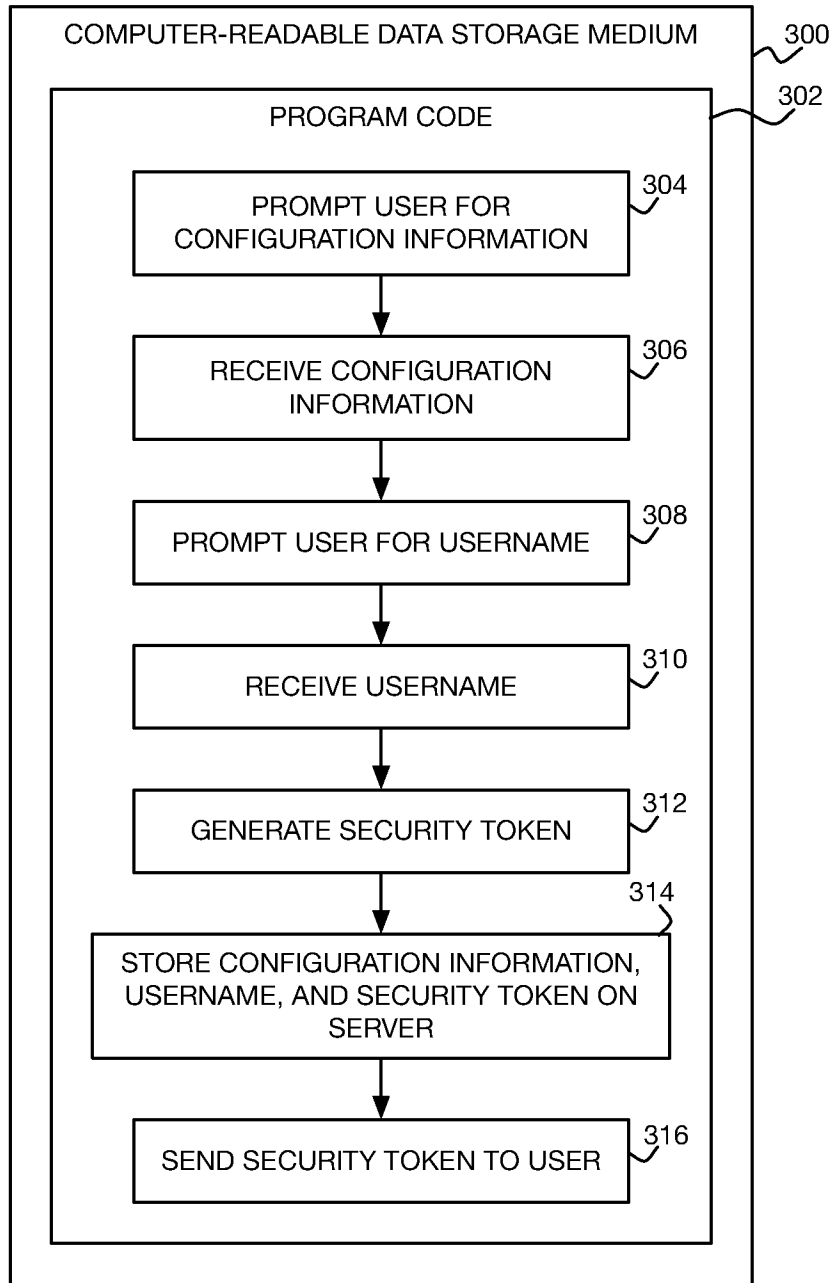


FIG 4

400
↙

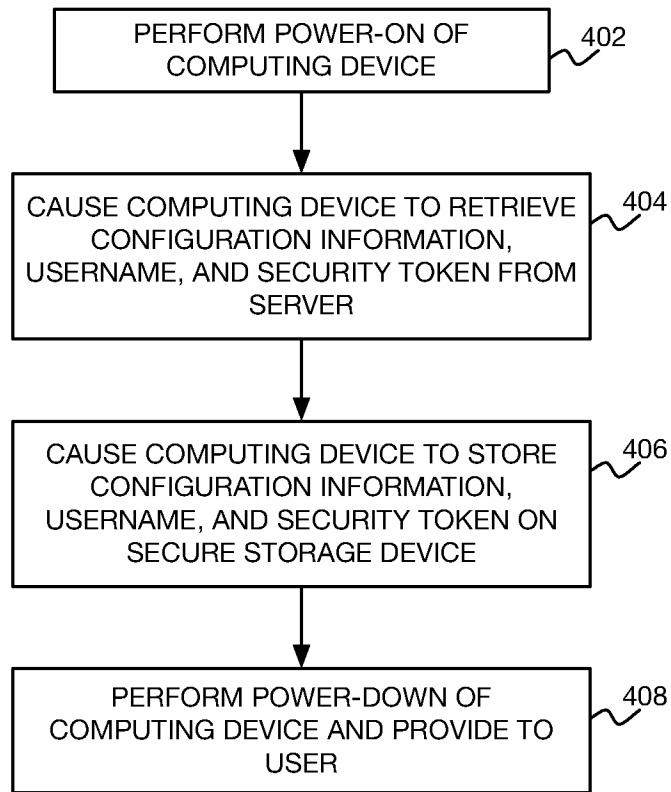
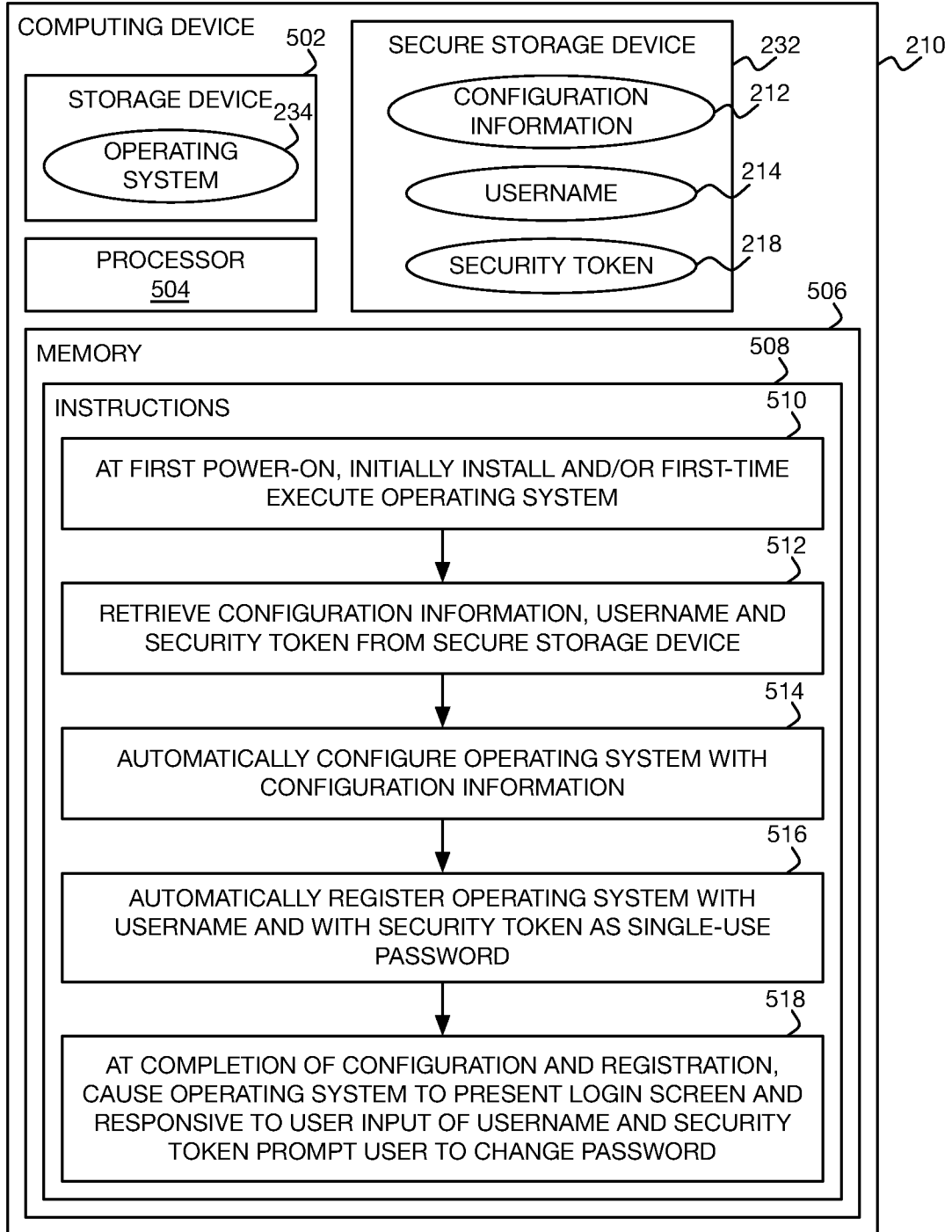


FIG 5



INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2021/027673

<p>A. CLASSIFICATION OF SUBJECT MATTER</p> <p style="text-align: center;">G06F 8/61 (2018.01) G06F 9/4401 (2018.01)</p> <p>According to International Patent Classification (IPC) or to both national classification and IPC</p>																																					
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols)</p> <p style="text-align: center;">G06F 8/00, 8/60, 8/61, 9/00, 9/06, 9/44, 9/4401, 9/445, 15/00, 15/16, 15/177, 21/00, 21/50, 21/57, H04L 29/02, 29/06</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)</p> <p style="text-align: center;">PatSearch (RUPTO Internal), USPTO, PAJ, Espacenet, Information Retrieval System of FIPS</p>																																					
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>US 2009/0222813 A1 (DELL PRODUCTS L.P.) 03.09.2009, paragraphs [0031]-[0033], [0035]-[0037], [0041]-[0045], [0050], [0052]-[0055], [0065], [0067], [0072]-[0073], [0078], [0100], figures 1A-1B, 6G</td> <td>1-4, 6-15</td> </tr> <tr> <td>Y</td> <td></td> <td>5</td> </tr> <tr> <td>Y</td> <td>US 2011/0225648 A1 (INTUIT INC.) 15.09.2011, paragraphs [0052], [0056]</td> <td>5</td> </tr> <tr> <td>A</td> <td>US 2003/0046682 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 06.03.2003</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>US 2011/0246981 A1 (VERIZON PATENT AND LICENSING, INC.) 06.10.2011</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>US 2020/0387385 A1 (VMWARE, INC.) 10.12.2020</td> <td>1-15</td> </tr> </tbody> </table> <p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.</p> <table border="1"> <tr> <td>* Special categories of cited documents:</td> <td>“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</td> </tr> <tr> <td>“A” document defining the general state of the art which is not considered to be of particular relevance</td> <td>“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</td> </tr> <tr> <td>“D” document cited by the applicant in the international application</td> <td>“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</td> </tr> <tr> <td>“E” earlier document but published on or after the international filing date</td> <td>“&” document member of the same patent family</td> </tr> <tr> <td>“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)</td> <td></td> </tr> <tr> <td>“O” document referring to an oral disclosure, use, exhibition or other means</td> <td></td> </tr> <tr> <td>“P” document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	US 2009/0222813 A1 (DELL PRODUCTS L.P.) 03.09.2009, paragraphs [0031]-[0033], [0035]-[0037], [0041]-[0045], [0050], [0052]-[0055], [0065], [0067], [0072]-[0073], [0078], [0100], figures 1A-1B, 6G	1-4, 6-15	Y		5	Y	US 2011/0225648 A1 (INTUIT INC.) 15.09.2011, paragraphs [0052], [0056]	5	A	US 2003/0046682 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 06.03.2003	1-15	A	US 2011/0246981 A1 (VERIZON PATENT AND LICENSING, INC.) 06.10.2011	1-15	A	US 2020/0387385 A1 (VMWARE, INC.) 10.12.2020	1-15	* Special categories of cited documents:	“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	“A” document defining the general state of the art which is not considered to be of particular relevance	“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	“D” document cited by the applicant in the international application	“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	“E” earlier document but published on or after the international filing date	“&” document member of the same patent family	“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	
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																																			
X	US 2009/0222813 A1 (DELL PRODUCTS L.P.) 03.09.2009, paragraphs [0031]-[0033], [0035]-[0037], [0041]-[0045], [0050], [0052]-[0055], [0065], [0067], [0072]-[0073], [0078], [0100], figures 1A-1B, 6G	1-4, 6-15																																			
Y		5																																			
Y	US 2011/0225648 A1 (INTUIT INC.) 15.09.2011, paragraphs [0052], [0056]	5																																			
A	US 2003/0046682 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 06.03.2003	1-15																																			
A	US 2011/0246981 A1 (VERIZON PATENT AND LICENSING, INC.) 06.10.2011	1-15																																			
A	US 2020/0387385 A1 (VMWARE, INC.) 10.12.2020	1-15																																			
* Special categories of cited documents:	“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																																				
“A” document defining the general state of the art which is not considered to be of particular relevance	“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																																				
“D” document cited by the applicant in the international application	“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																																				
“E” earlier document but published on or after the international filing date	“&” document member of the same patent family																																				
“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																																					
<p>Date of the actual completion of the international search</p> <p style="text-align: center;">13 December 2021 (13.12.2021)</p>		<p>Date of mailing of the international search report</p> <p style="text-align: center;">23 December 2021 (23.12.2021)</p>																																			
<p>Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37</p>		<p>Authorized officer</p> <p style="text-align: center;">N. Skokova</p> <p>Telephone No. 8(495)531-65-15</p>																																			