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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2016 (04.02.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/018390 A1

(51) International Patent Classification:
G06F 21/46 (2013.01) *G06F 15/16* (2006.01)

(21) International Application Number:
PCT/US2014/049232

(22) International Filing Date:
31 July 2014 (31.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **KAO, Liang-Chin**; 10F-1, No. 66, Jingmao 2nd Rd., NanGang District, Taipei, 11568 (TW). **HUNG, Shang-Ching**; 10F-1, No. 66, Jingmao 2nd Rd., NanGang District, Taipei, 11568 (TW). **CHIN, Hao Lun**; 10F-1, No. 66, Jingmao 2nd Rd., NanGang District, Taipei, 11568 (TW).

(74) Agents: **ADEKUNLE, Olaolu, O.** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, CO 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Continued on next page]

(54) Title: SECURE BIOS PASSWORD METHOD IN SERVER COMPUTER

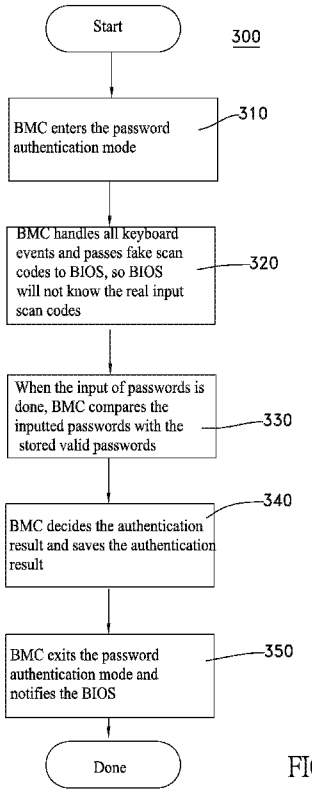

FIG. 3

(57) Abstract: A method for securing BIOS passwords in a server computer under a BIOS user privilege control operation is disclosed. Said method comprises: a BIOS (Basic Input/Output System) of the server computer requesting a BMC (Baseboard Management Controller) to enter a password authentication mode for user privilege authentication; the BMC receiving passwords inputted by a user and comparing the inputted passwords with valid passwords, wherein the valid passwords are stored in the BMC; the BMC deciding an authentication result after the comparing the inputted passwords with the stored valid passwords and saving the authentication result; and the BMC exiting the password authentication mode and notifying the BIOS of the authentication result; wherein the BMC passes fake scan codes of key strings of the inputted passwords to the BIOS, such that the BIOS does not have access to the actual passwords.

WO 2016/018390 A1

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 the identity of the inventor (Rule 4.17(i))*

— *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))*

SECURE BIOS PASSWORD METHOD IN SERVER COMPUTER

TECHNICAL FIELD

[0001] The present application relates to user privilege control operations. In particular, the present application relates to methods and systems for securing Basic Input/Output System (BIOS) passwords in a server computer under user privilege control operations, and the server computer thereof.

BACKGROUND

[0002] In a server computer, the traditional BIOS User Privilege Control operation runs on a system processor, which uses BIOS to perform user authentications. BIOS User Privilege Control comprises User Privilege and User Authentication. User privilege can be read from Non-volatile random-access memory (NVRAM) or written to NVRAM by BIOS. User Authentication depends on saved User Privilege.

[0003] In traditional methods, BIOS reads the valid passwords from an NVRAM and the user inputs the passwords from a keyboard. The passwords may be a single string of a password or a list of passwords. The BIOS compares the inputted passwords with the valid passwords. When the user changes the passwords, the BIOS saves the new passwords and sets the user privilege on the BIOS NVRAM.

[0004] Such traditional methods handle the user privilege in an unsecured way due to the lack of anti-spy mechanism or encryption over the network. Any spy software may crack the BIOS passwords and then get power on or administration privileges, such that the hacker may obtain the control privilege of a server computer. In a server group, which uses one global set of passwords for all server computers, if the hacker steals the passwords from a server computer in the server group, he/she can then obtain the control privilege of all of the server computers in the group and steal any data in the whole group.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Various features and advantages of the disclosed embodiments will be apparent from the detailed description which follows, taken in conjunction with the accompanying drawings, which together illustrate, by way of example, features of the disclosed embodiments.

[0006] Figures 1A and 1B illustrate a block diagram of the firmware components for user privilege authentication in a server computer.

[0007] Figures 2A to 2C illustrate a flow chart of user privilege authentication.

[0008] Figure 3 illustrates a flow chart of user privilege authentication handled by a Baseboard Management Controller (BMC).

[0009] Figure 4 illustrates a flow chart of three types of user privilege operation.

[0010] Figure 5 illustrates a flow chart for the BIOS keyboard driver under user privilege operation mode.

DETAILED DESCRIPTION

[0011] As described above, the traditional BIOS User Privilege Control operation applies an unsecured method to handle the user privilege for the password authentication, such that a hacker may easily obtain the control privilege of server computers. The present invention aims to solve the aforesaid issue and provides a different structure over the traditional methods in order to avoid that the BIOS passwords and the control privilege of the server computers being hacked.

[0012] The present application proposes methods and systems for securing BIOS passwords in a server computer under user privilege control operations. According to the present invention, the BIOS, system processor and system memory cannot access the actual passwords, so the spy software has no chance to discover the BIOS passwords. According to the present invention, the hacker cannot steal the passwords with any cracking methods, such as applying unauthorized applications or unauthorized option ROM (Read-Only Memory), to read the passwords from the BIOS NVRAM storage.

[0013] The proposed invention handles the BIOS User Privilege Control operation by a BMC firmware running in a baseboard management controller (BMC) instead of a BIOS firmware running in a system processor of a server computer. From the hardware's aspect, the proposed invention comprises a server computer system with a BMC. From the firmware's aspect, the proposed invention comprises BIOS, BMC firmware and option ROM, which supports the Human Interface Infrastructure (HII) Configuration. The passwords are stored by the BMC, so the BIOS does not need to keep, save or compare them.

[0014] Figure 1 illustrates a block diagram (100) of software components of BIOS, BMC firmware (150) and option ROM under user privilege operation mode (password mode). The BIOS loads an HII configuration driver (120) embedded in the BIOS or the option ROM. The HII configuration driver (120) provides an interface between the BIOS and the input devices controlled by a user, and communicates activities initiated by the user. The HII configuration driver (120) initiates an HII setup browser (110), which provides the user with a visual browser including system setup options, and enables a keyboard driver (130) for the user to input instructions in order to check whether the user requests a BIOS user privilege control operation. When the system runs in a normal mode instead of a password mode, the BIOS firmware runs on a system processor (170). However, if the user enters instructions to request a BIOS user privilege control operation, the system will then enter the password mode for user privilege authentication. The BIOS first loads a password mode driver (140) and requests the BMC firmware (150) to enter a password

authentication mode for user privilege authentication. The BMC firmware (150) runs on a BMC (180) instead of the system processor (170). The BMC (180) is a specialized microcontroller embedded on a motherboard of a computer, generally a server, which supports the Intelligent Platform Management Interface (IPMI) architecture. The BMC (180) manages the interface between system management software and platform hardware. In the password mode, the keyboard driver (130) redirects keyboard events and scan codes to the BMC firmware (150), such that the BIOS and the system processor (170) do not acquire the actual scan codes and cannot access the actual passwords. The BMC firmware (150) may further comprise a keyboard controller firmware, which processes the keyboard events inputted locally or remotely from an integrated remote console (160).

[0015] Under the aforesaid structure, when the user requests the password check operation locally, authentication operation will be handled by the BMC firmware (150) instead of the BIOS firmware running in a system processor of the server computer. When the user requests the password check operation and inputs the passwords remotely from the integrated remote console (160), the inputted passwords sent from the remote console (160) will be encrypted over a network.

[0016] Figure 2 illustrates a detailed flow chart (200) for the BIOS requesting the BMC firmware to enter a password authentication mode for user privilege authentication. According to the present invention, a user opens the password input box in an HII setup browser (201). The BIOS gets the user's instructions, chooses the UI operation and notifies the BMC to enter a password authentication mode (202). The BMC enters the password authentication mode (203) and notifies the BIOS keyboard driver to also enter a password authentication mode (204). The BIOS keyboard driver enters the password authentication mode and redirects keyboard events to the BMC instead of the BIOS (205). The BMC receives and processes the keyboard events and the scan codes of the inputted strings (206). After the user completes the input of the passwords, the BMC exits the password input mode (207). The BMC checks the passwords inputted by the user, compares

the inputted passwords with valid passwords and sets the user privilege (208). The BMC then notifies the BIOS of the authentication result and notifies the BIOS keyboard driver to exit the password authentication mode (208). The BIOS keyboard driver exits the password authentication mode (209) and resumes the normal mode (210). The BMC exits the password authentication mode and runs in the normal mode (211). The BIOS processes the following UI operation in response to the user (212) and may inquire into the user's privilege with the BMC if required (213).

[0017] Figure 3 illustrates a flow chart (300) of user privilege authentication handled by a BMC. The method for user privilege authentication can be processed locally by a BMC or remotely from an integrated remote console. The integrated remote console module provided by the BMC can be operated over a network via the integrated remote console. If a user enters instructions for set up user privilege in the BIOS of a server computer, the BIOS requests a BMC to enter a password authentication mode (310). The BMC receives all of the keyboard events and passes fake scan codes to the BIOS, such that the BIOS cannot access the actual input scan codes (320). When the user completes the input of the passwords, the BMC encrypts the passwords and compares the inputted passwords with valid passwords stored in the BMC (330). The BMC decides an authentication result after the aforesaid comparison and saves the authentication result (340). Finally, the BMC exits the password authentication mode and notifies the BIOS of the authentication result (350).

[0018] Figure 4 illustrates three types of the authentication results under a BIOS user privilege control operation. When the BIOS requests the BMC for user privilege authentication, the BIOS needs to indicate the type of the user privilege to be processed by a unique number, usually a GUID used by the UEFI BIOS. The specified user privilege mechanism provides the option ROM with the ability to process the user privilege authentication. The user privilege can be categorized as one of the followings (for example and not limited to): BIOS power on user privilege; BIOS administrator user privilege; BMC access user privilege; and specified option ROM user privilege. Different privileges

provide different authorities for the control of the computer. The BIOS power on user privilege enables an authority for setting a specific time by a user, such that the computer can be automatically powered on at the aforesaid specific time. The BIOS administrator user privilege enables an authority for a user to change the system setup options in the BIOS. The BMC access user privilege enables an authority for a user to access the setting stored in the BMC. The specified option ROM user privilege enables an authority for a user to change the setup options stored in the option ROM. The authentication results (401) under a BIOS user privilege control operation may be "no password", "password denied", or "password granted". If the user privilege is "no password" (402), the BIOS and BMC will process to set up the passwords (405). If the user privilege is "password denied" (403), the BIOS and BMC will process to verify the passwords (406). If the user privilege is "password granted" (404), the BIOS and BMC will process to change or clear the passwords (407).

[0019] Figure 5 illustrates a flow chart (500) for the process of the BIOS keyboard driver under user privilege operation mode. According to the present invention, when the BMC enters the password authentication mode, the BMC notifies a BIOS keyboard driver to enter the password authentication mode (510). The BIOS keyboard driver enters the password authentication mode (520) and redirects keyboard events to the BMC instead of the BIOS, such that the BIOS does not receive the key strings of the keyboard events (530). Upon the BMC exiting the password authentication mode, the BMC notifies the BIOS keyboard driver to exit the password authentication mode (540). The BIOS keyboard driver then resumes the normal mode (550).

[0020] According to the illustrated operations for BIOS user privilege authentication, any server computers and systems including the disclosed functionality of the BIOS and BMC may also secure the BIOS passwords and are also claimed by the present application. According to the present invention, BIOS, system processor and system memory cannot access the actual passwords, so the spy software has no chance to discover the BIOS passwords. According to the present invention, the hacker cannot steal the

passwords with any codecrack methods, such as applying unauthorized applications or unauthorized option ROM, to read the passwords from the BIOS NVRAM storage. Accordingly, the present invention secures the user privilege for server computers and systems.

[0021] The aforesaid detailed descriptions illustrate the preferred embodiments of the present application. However, the scope of the claimed invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

Claims

What is claimed is:

1. A method for securing Basic Input/Output System (BIOS) passwords in a server computer under a BIOS user privilege control operation, comprising:

requesting a Baseboard Management Controller (BMC) to enter a password authentication mode for user privilege authentication;

receiving passwords inputted by a user and comparing the inputted passwords with valid passwords by the BMC, wherein the valid passwords are stored in the BMC;

deciding an authentication result by the BMC after the comparing the inputted passwords with the stored valid passwords, and saving the authentication result into the BMC; and

exiting the password authentication mode for the BMC and notifying the BIOS of the authentication result by the BMC;

wherein the BMC passes fake scan codes of key strings of the inputted passwords to the BIOS , such that the BIOS cannot access the actual passwords.

2. The method of claim 1, wherein the BMC processes the user privilege authentication locally when the user uses a local keyboard or remotely when the user performs a password check operation over a network from a remote console.

3. The method of claim 2, wherein the inputted passwords sent from the remote console over a network are encrypted.

4. The method of claim 1, wherein the authentication result comprises: no password; password denied; or password granted.

5. The method of claim 1, further comprising:

notifying a BIOS keyboard driver to enter the password authentication mode from a normal mode;

entering the password authentication mode for the BIOS keyboard driver and redirecting keyboard events to the BMC instead of the BIOS, such that the BIOS does not receive the key strings of the keyboard events;

upon exiting the password authentication mode for the BMC, notifying the BIOS keyboard driver to exit the password authentication mode by the BMC; and

resuming the normal mode for the BIOS keyboard driver.

6. A system for securing Basic Input/Output System (BIOS) passwords in a server computer under a BIOS user privilege control operation, comprising:

a BIOS including a Human Interface Infrastructure (HII) configuration driver, wherein the BIOS loads the HII configuration driver to check whether a user requests the BIOS user privilege control operation; and

a Baseboard Management Controller (BMC) embedded in the server computer, the BMC receiving a request from the BIOS to enter a password authentication mode when the user requests the BIOS user privilege control operation;

wherein the BMC receives passwords inputted by a user and compares the inputted passwords with valid passwords after entering the password authentication mode, the valid passwords are stored in the BMC, and the BMC passes fake scan codes of key strings of the inputted passwords to the BIOS , such that the BIOS cannot access the actual passwords,

the BMC decides an authentication result after the comparing the inputted passwords with the stored valid passwords and saves the authentication result, and

the BMC exits the password authentication mode and notifies the BIOS of the authentication result.

7. The system of claim 6, wherein the BMC processes the user privilege authentication locally when the user uses a local keyboard or remotely when the user performs a password check operation over a network from a remote console.

8. The system of claim 7, wherein the inputted passwords sent from the remote console over a network are encrypted.

9. The system of claim 6, wherein the authentication result comprises: no password; password denied; or password granted.

10. The system of claim 6, wherein the BIOS further comprises a BIOS keyboard driver, and the BMC notifies the BIOS keyboard driver to enter the password authentication mode from a normal mode;

the BIOS keyboard driver enters the password authentication mode and redirects keyboard events to the BMC instead of the BIOS, such that the BIOS does not receive the key strings of the keyboard events;

upon the BMC exiting the password authentication mode, the BMC notifies the BIOS keyboard driver to exit the password authentication mode; and

the BIOS keyboard driver resumes the normal mode.

11. The system of claim 6, wherein the server computer is included in the system and comprises a storage device storing the BIOS.

12. A non-transitory computer-readable storage medium storing instructions for executing a method for securing Basic Input/Output System (BIOS) passwords in a server computer under a BIOS user privilege control operation, when the instructions are executed by the server computer, cause the server computer to:

requesting a Baseboard Management Controller (BMC) to enter a password authentication mode for user privilege authentication;

receiving passwords inputted by a user and comparing the inputted passwords with valid passwords by the BMC, wherein the valid passwords are stored in the BMC;

deciding an authentication result by the BMC after the comparing the inputted passwords with the stored valid passwords, and saving the authentication result into the BMC; and

exiting the password authentication mode for the BMC and notifying the BIOS of the authentication result by the BMC;

wherein the BMC passes fake scan codes of key strings of the inputted passwords to the BIOS , such that the BIOS cannot access the actual passwords.

13. The non-transitory computer-readable storage medium of claim 12, wherein the BMC processes the user privilege authentication locally when the user uses a local keyboard or remotely when the user performs a password check operation over a network from a remote console.

14. The non-transitory computer-readable storage medium of claim 13, wherein the inputted passwords sent from the remote console over a network are encrypted.

15. The non-transitory computer-readable storage medium of claim 12, wherein the authentication result comprises: no password; password denied; or password granted.

16. The non-transitory computer-readable storage medium of claim 12, further cause the server computer to:

notifying a BIOS keyboard driver to enter the password authentication mode from a normal mode;

entering the password authentication mode for the BIOS keyboard driver and redirecting keyboard events to the BMC instead of the BIOS, such that the BIOS does not receive the key strings of the keyboard events;

upon exiting the password authentication mode for the BMC, notifying the BIOS keyboard driver to exit the password authentication mode by the BMC; and

resuming the normal mode for the BIOS keyboard driver.

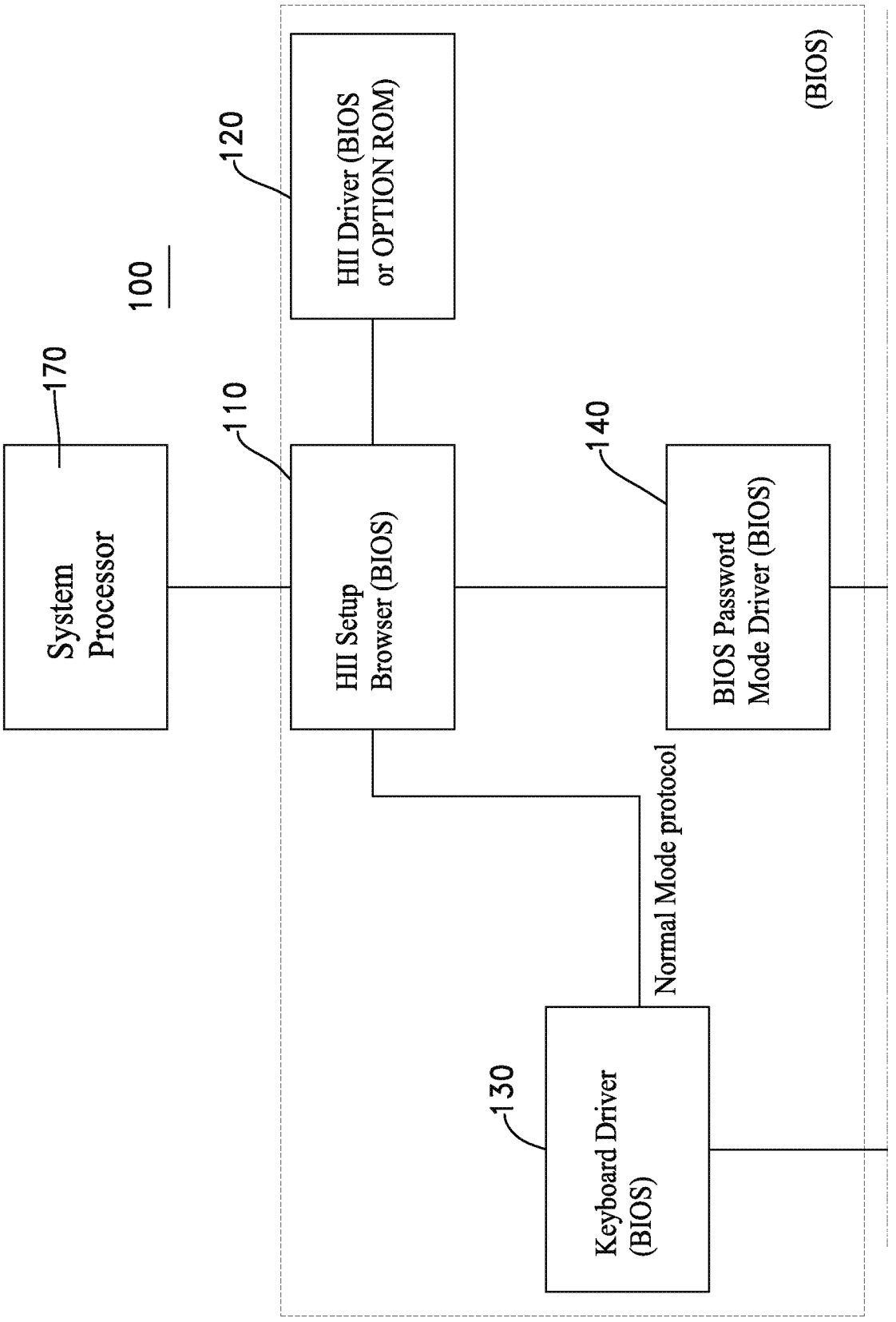
100
170
System Processor
110
HII Setup Browser (BIOS)
120
HII Driver (BIOS or OPTION ROM)
140
BIOS Password Mode Driver (BIOS)
(BIOS)
Normal Mode protocol
130
Keyboard Driver (BIOS)
B1
B2

FIG. 1A

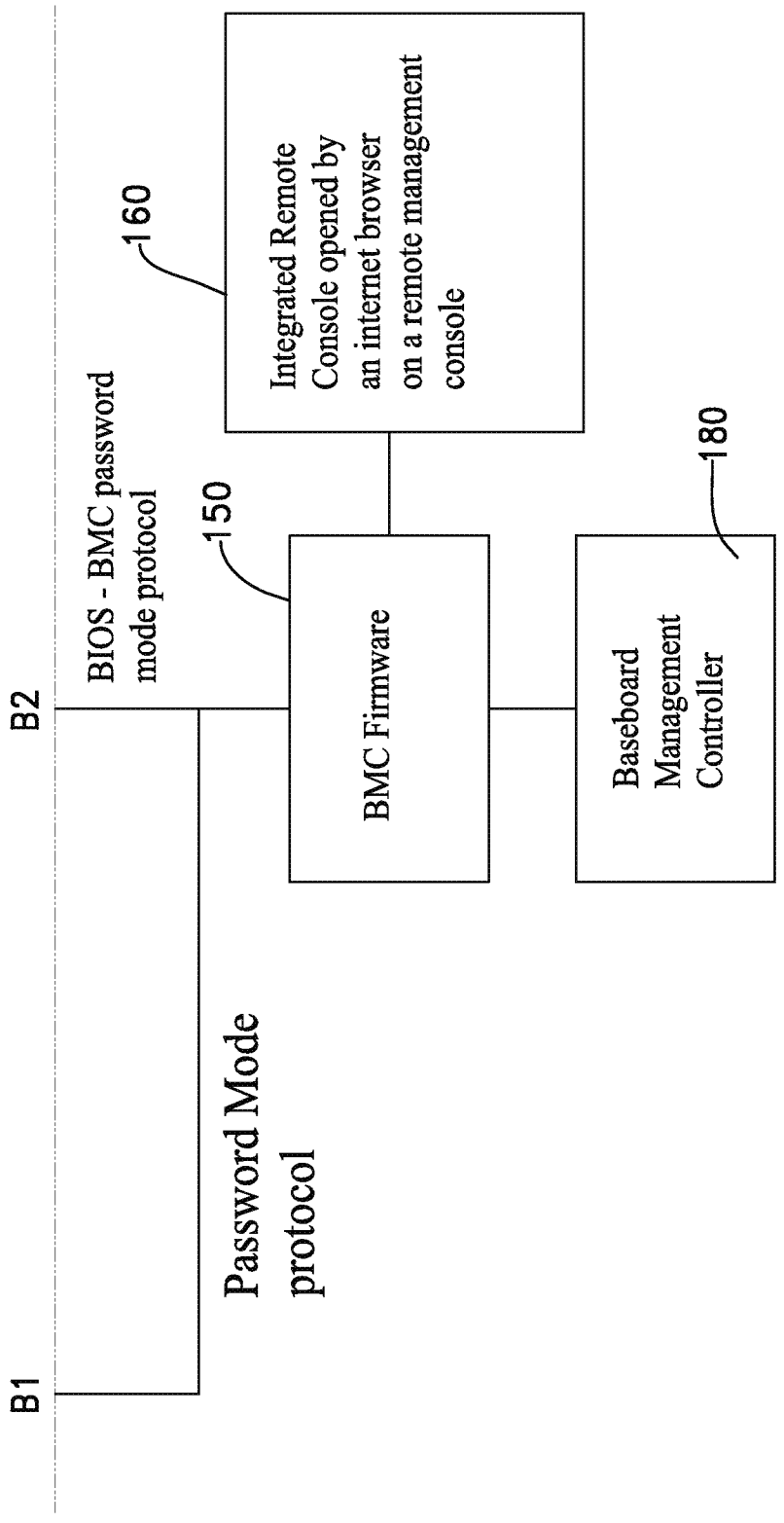
B1
B2
Password Mode protocol
BIOS - BMC password mode protocol
150
BMC Firmware
160
Integrated Remote Console opened by an internet browser on a remote management console
180
Baseboard Management Controller

FIG. 1B

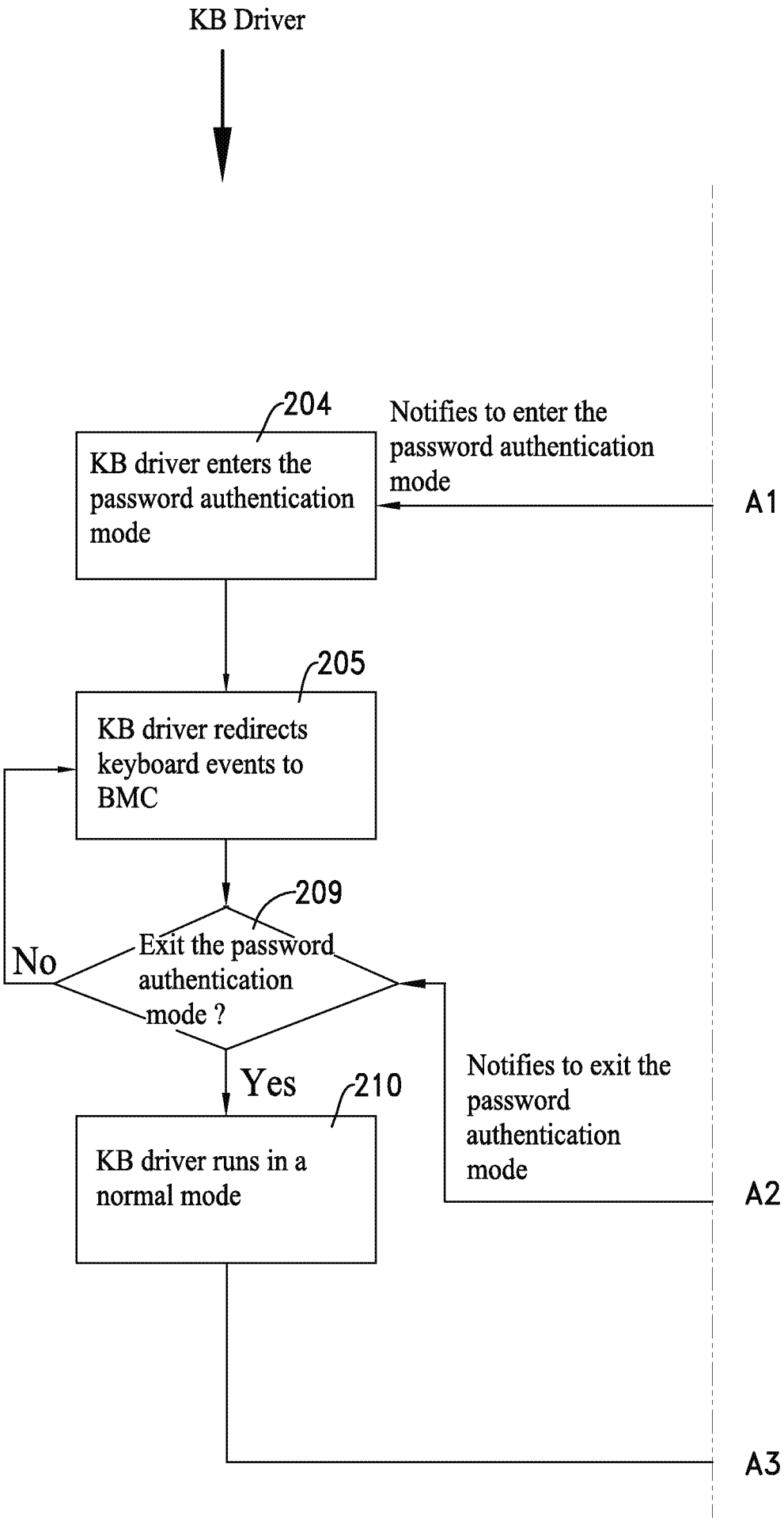
KB Driver
204
KB driver enters the password authentication mode
Notifies to enter the password authentication mode
A1
205
KB driver redirects keyboard events to BMC
209
Exit the password authentication mode ?
No
Yes
Notifies to exit the password authentication mode
A2
210
KB driver runs in a normal mode
A3

FIG. 2A

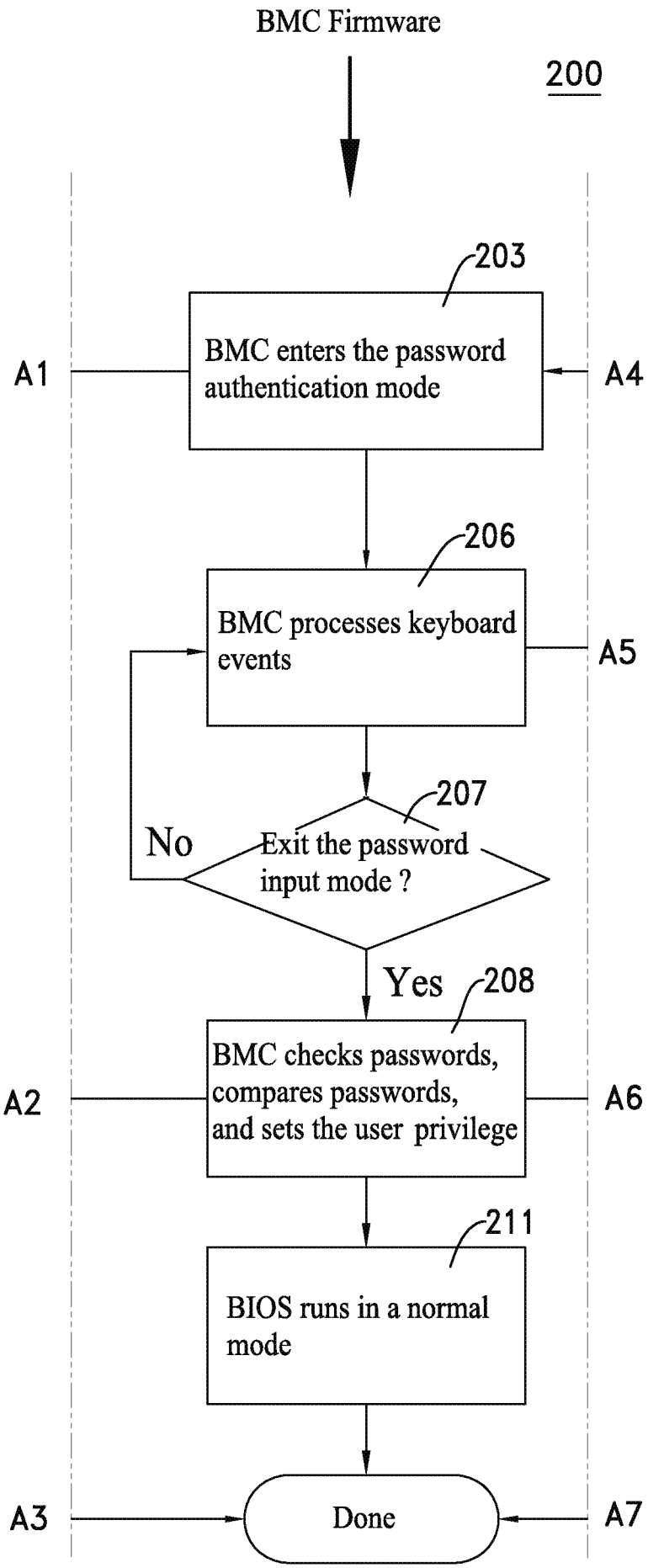
BMC Firmware
200
203
BMC enters the password authentication mode
A1
A4
206
BMC processes keyboard events
A5
207
No
Exit the password input mode ?
Yes
208
BMC checks passwords, compares passwords, and sets the user privilege
A2
A6
211
BIOS runs in a normal mode
A3
Done
A7

FIG. 2B

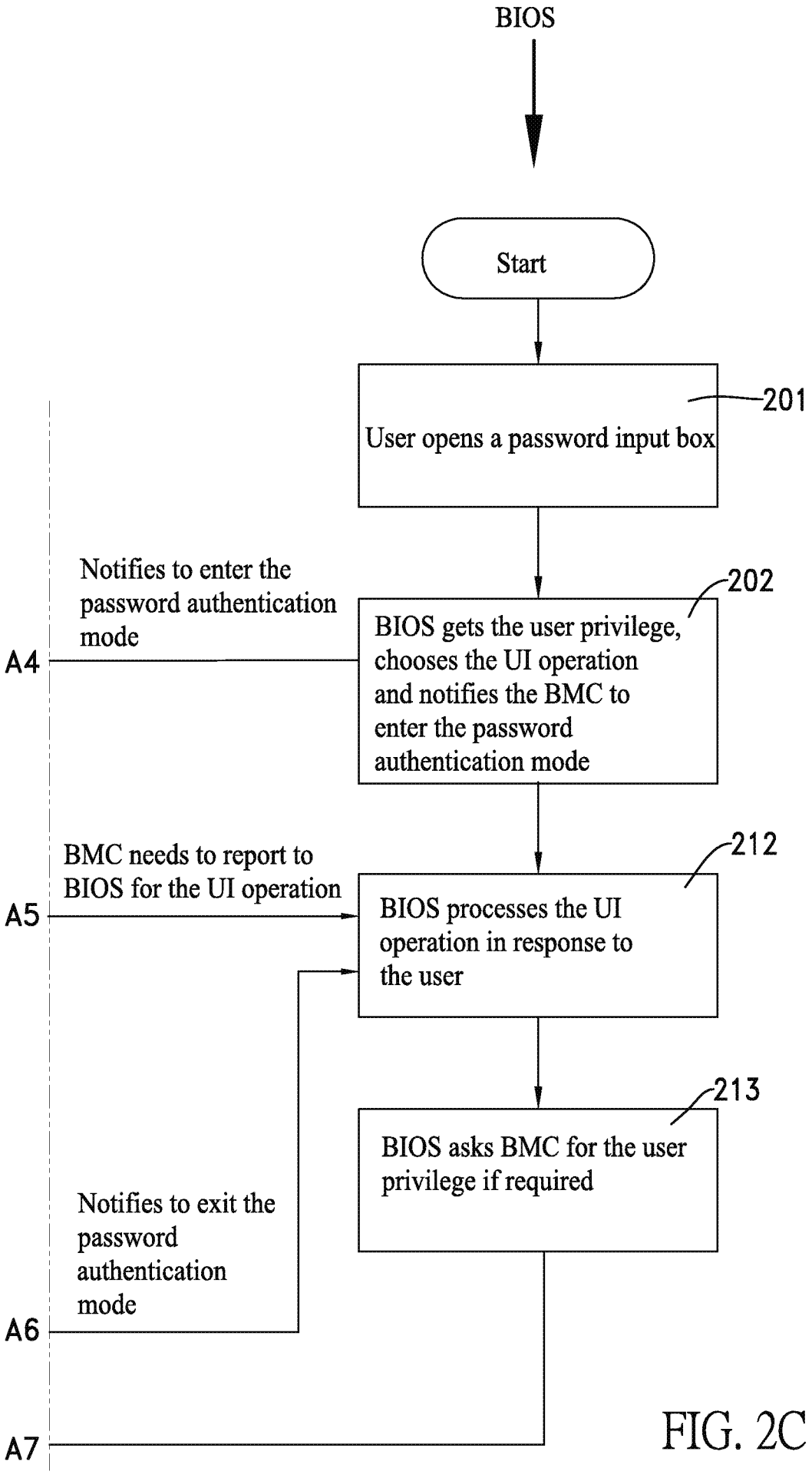
BIOS
Start
User opens a password input box
201
Notifies to enter the password authentication mode
A4
BIOS gets the user privilege, chooses the UI operation and notifies the BMC to enter the password authentication mode
202
BMC needs to report to BIOS for the UI operation
A5
BIOS processes the UI operation in response to the user
212
BIOS asks BMC for the user privilege if required
213
Notifies to exit the password authentication mode
A6
A7

FIG. 2C

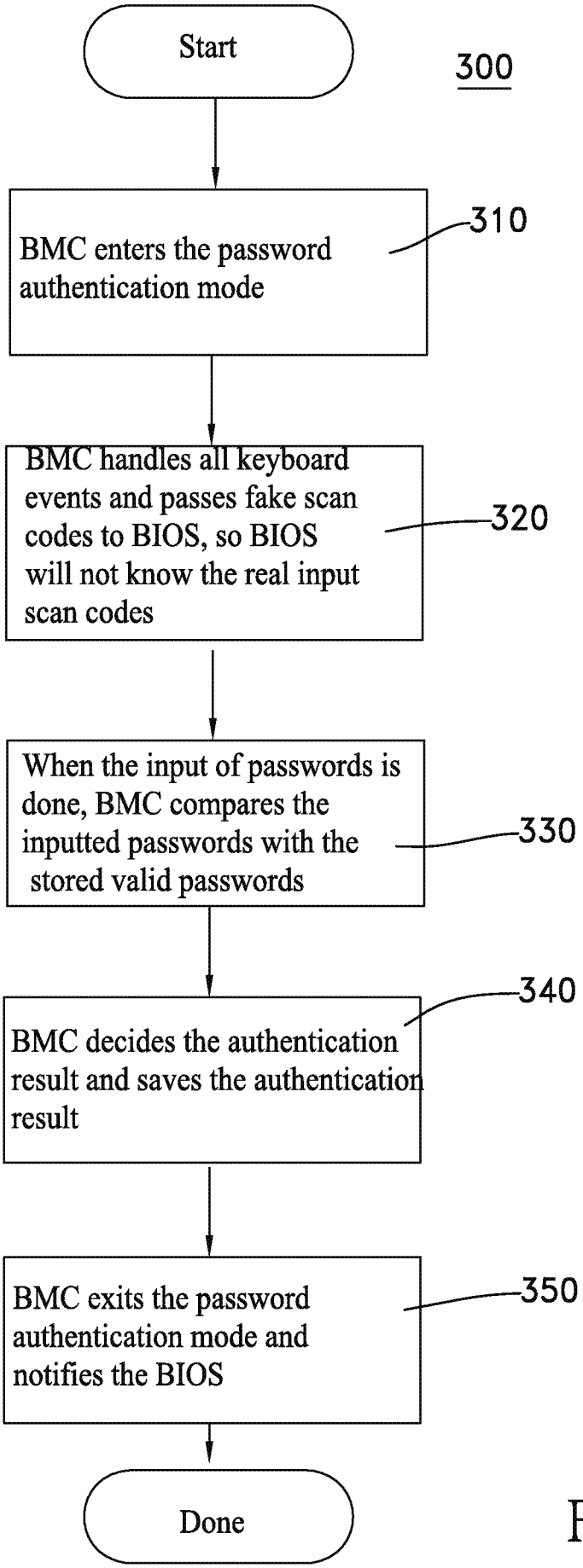
Start
300
BMC enters the password authentication mode
310
BMC handles all keyboard events and passes fake scan codes to BIOS, so BIOS will not know the real input scan codes
320
When the input of passwords is done, BMC compares the inputted passwords with the stored valid passwords
330
BMC decides the authentication result and saves the authentication result
340
BMC exits the password authentication mode and notifies the BIOS
350
Done

FIG. 3

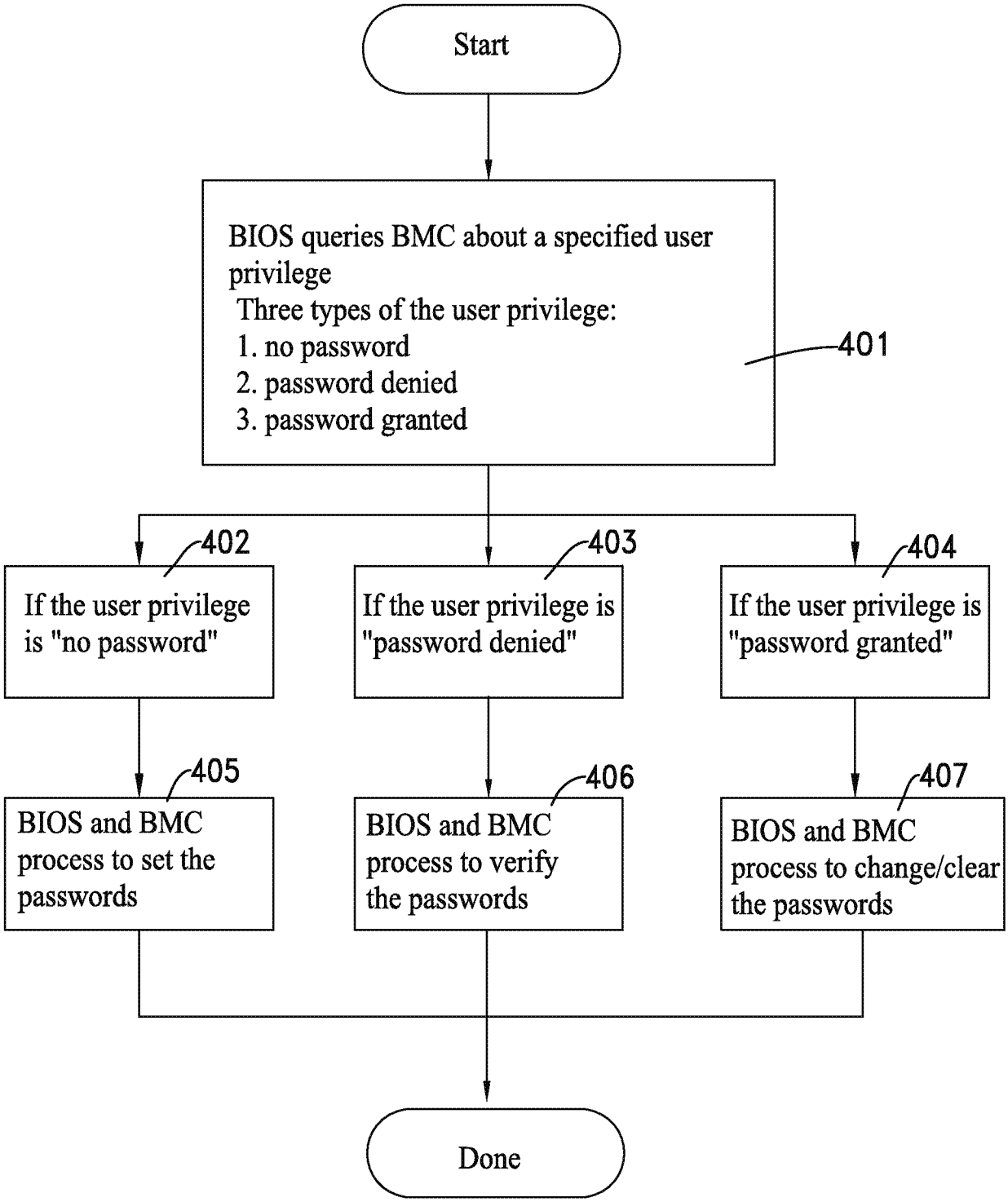
Start
BIOS queries BMC about a specified user privilege
Three types of the user privilege:
1. no password
2. password denied
3. password granted
401
402
If the user privilege is "no password"
403
If the user privilege is "password denied"
404
If the user privilege is "password granted"
405
BIOS and BMC process to set the passwords
406
BIOS and BMC process to verify the passwords
407
BIOS and BMC process to change/clear the passwords
Done

FIG. 4

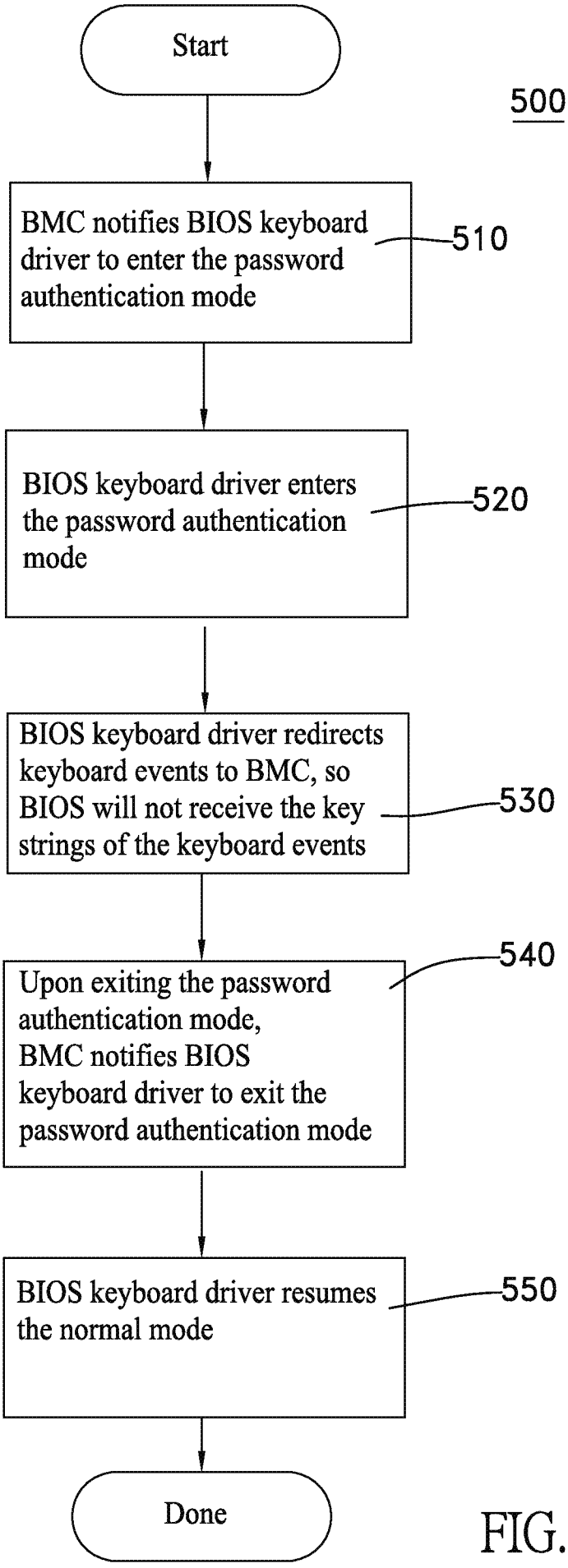
Start
500
BMC notifies BIOS keyboard driver to enter the password authentication mode
510
BIOS keyboard driver enters the password authentication mode
520
BIOS keyboard driver redirects keyboard events to BMC, so BIOS will not receive the key strings of the keyboard events
530
Upon exiting the password authentication mode, BMC notifies BIOS keyboard driver to exit the password authentication mode
540
BIOS keyboard driver resumes the normal mode
550
Done

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/049232

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/46(2013.01)i, G06F 15/16(2006.01)i

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)
G06F 21/46; G06F 13/38; H04L 9/32; G06F 1/00; H04L 9/00; G06F 15/177; G06F 21/00; G06F 13/00; G06F 15/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: BIOS, server, Baseboard Management Controller (BMC), Intelligent Platform Management Interface (IPMI), password

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008-0162956 A1 (JAMES J. BOZEK et al.) 03 July 2008 See paragraphs [0047]-[0048] and figure 5.	1-16
A	US 2011-0083003 A1 (MUHAMMED K. JABER et al.) 07 April 2011 See paragraphs [0015]-[0017] and figure 1.	1-16
A	US 2013-0091260 A1 (RANDALL L. MURPHY et al.) 11 April 2013 See paragraphs [0015], [0019] and figure 1.	1-16
A	JP 2013-161210 A (NEC COMPUTERTECHNO LTD.) 19 August 2013 See paragraphs [0048]-[0065] and figure 8.	1-16
A	US 2004-0268140 A1 (VINCENT J. ZIMMER et al.) 30 December 2004 See paragraphs [0066]-[0068] and figure 4.	1-16

☐ 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
09 April 2015 (09.04.2015)	**09 April 2015 (09.04.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. ++82 42 472 7140

Authorized officer
AHN, Jeong Hwan
Telephone No. +82-42-481-8440

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/049232

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0162956 A1	03/07/2008	CN 101222340 A	16/07/2008
		CN 101222340 B	12/10/2011
		US 2008-0162958 A1	03/07/2008
		US 7865746 B2	04/01/2011
		US 7873847 B2	18/01/2011
US 2011-0083003 A1	07/04/2011	US 8219792 B2	10/07/2012
US 2013-0091260 A1	11/04/2013	US 2013-091259 A1	11/04/2013
		US 8898345 B2	25/11/2014
		US 8903967 B2	02/12/2014
JP 2013-161210 A	19/08/2013	None	
US 2004-0268140 A1	30/12/2004	US 7587750 B2	08/09/2009