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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 August 2013 (15.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/119065 A1

(51) International Patent Classification:
G06F 21/44 (2013.01) *G06F 9/06* (2006.01)
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/KR2013/001013

(22) International Filing Date:
7 February 2013 (07.02.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/371,195 10 February 2012 (10.02.2012) US
10-2012-0104031
19 September 2012 (19.09.2012) KR

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-742 (KR).

(72) Inventors: **BRUTCH, Tasneem**; C/O 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-742 (KR). **ACIICMEZ, Onur**; C/O 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-742 (KR).

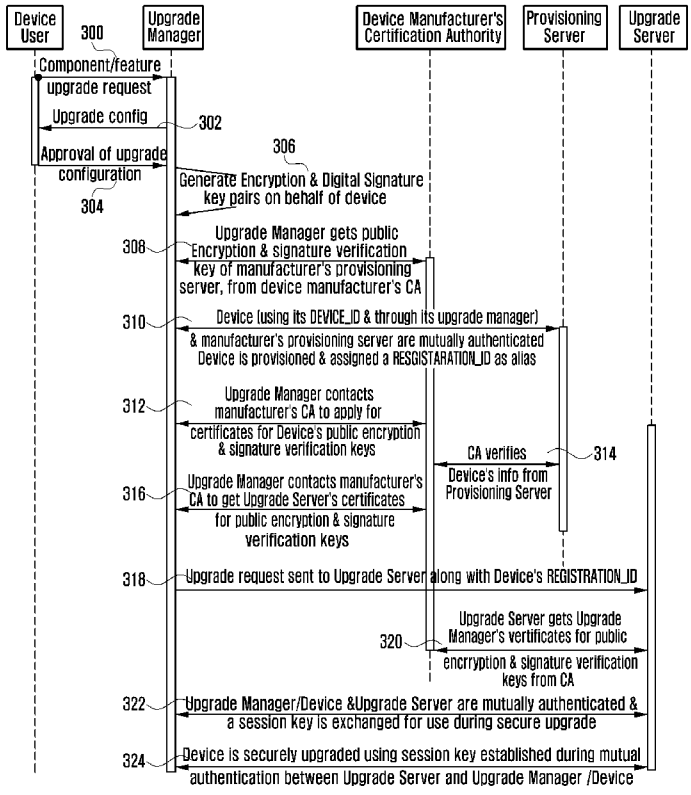
(74) Agent: **YOON, Dong Yol**; Yoon & Lee International Patent & Law Firm, 3rd Fl, Ace Highend Tower-5, 226, Gasan Digital 1-ro, Geumcheon-gu, Seoul 153-803 (KR).

(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, IS, JP, KE, KG, KM, KN, KP, 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, 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, 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, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURELY UPGRADING OR DOWNGRADING PLATFORM COMPONENTS



(57) Abstract: A method for securely altering a platform component is provided, comprising: assigning certificates for public encryption and signature verification keys for the device; assigning certificates for public encryption and signature verification keys for an upgrade server; mutually authenticating a device containing the platform component and the upgrade server; causing the device and the upgrade server to exchange a session key; and providing an alteration to be made to the platform component from the upgrade server to the device using the session key.

WO 2013/119065 A1

Published:

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

Description

Title of Invention: SECURELY UPGRADING OR DOWNGRADING PLATFORM COMPONENTS

Technical Field

[1] The present invention relates generally to electronic platform components. More specifically, the present invention relates to securely upgrading or downgrading platform components.

Background Art

[2] Electronic component platforms include electronic devices that include multiple levels of components or functionality. These components can either be built into the individual platform by the same manufacturer as the platform, or the components can be built by different manufacturers and later combined into a platform. An example of the former may be a computer processor, which can contain different layers of functionality (e.g., main processing components, multiple cores, built-in memory, graphics acceleration, mathematical calculation acceleration, etc.). An example of the latter may be a computer system, where a company such as Dell™ may assemble a computer using components from various manufacturers.

[3] Consumers purchase such electronic platforms once and cannot upgrade individual components at there will unless they buy a new component and replace an existing one. In some cases, it may even be impossible for the consumer to upgrade an individual component without replacing the entire platform. In the case of a computer processor, for example, it is not possible for a consumer to purchase an upgrade to the built-in memory without either replacing the entire computer processor or using a different component entirely (such as a memory slot built into a separate motherboard). This creates a problem for customers who wish to upgrade some portions of their components but not others. This also creates a problem for manufacturers, who have customers who are willing to pay for certain upgrades but are unable to deliver such upgrades without requiring the customers to purchase additional, unwanted, components or portions of components, which generally results in lost sales.

[4] What is needed is a solution that addresses these issues.

Disclosure of Invention

Technical Problem

[5] The present invention has been made in view of the above problems, and provides a system and a method for securely upgrading or downgrading platform components.

Solution to Problem

[6] In a first embodiment of the present invention, a method for securely altering a

platform component is provided, comprising: assigning certificates for public encryption and signature verification keys for the device; assigning certificates for public encryption and signature verification keys for an upgrade server; mutually authenticating a device containing the platform component and the upgrade server; causing the device and the upgrade server to exchange a session key during the mutual authenticating; and providing an alteration to be made to the platform component from the upgrade server to the device using the session key exchanged during the mutual authenticating.

[7] In a second embodiment of the present invention, a method for securely altering a platform component is provided, comprising: generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered; obtaining public encryption and signature verification keys of a provisioning server from a certification authority; mutually authenticating the device and the provisioning server using the public encryption and signature verification keys; contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for the device; contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server; sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager's certificates for public encryption and signature verification keys from the certification authority; mutually authenticating the device and the upgrade server; causing the device and the upgrade server to exchange a session key; and providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

[8] In a third embodiment of the present invention, a system is provided comprising: a device containing a platform component; an upgrade manager; a certification authority; a provisioning server; and an upgrade server; wherein the upgrade manager is designed to generate encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered; obtain public encryption and signature verification keys of a provisioning server from a certification authority; perform one side of mutual authentication between the device and the provisioning server using the public encryption and signature verification keys of the provisioning server; contact the certification authority for assigned certificates for public encryption and signature verification keys for the device; contact the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server; send an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager's certificates for

public encryption and signature verification keys from the certification authority; perform one side of mutual authentication between the device and the upgrade server; send a session key to the upgrade server; and receive an alteration to be made to the platform component from the upgrade server to the device using the session key; wherein the certification authority is designed to: provide the encryption and signature verification keys of the provisioning server to the upgrade manager; assign certificates for the device's public encryption and signature verification keys; and assign certificates for the upgrade server's public encryption and signature verification keys; wherein the provisioning server is designed to: perform the other side of mutual authentication between the device and the provisioning server using the public encryption and signature verification keys of the provisioning server; and verify the device's information; and wherein the upgrade server is designed to: obtain the upgrade manager's certificates for public encryption and signature verification keys from the certification authority; perform the other side of mutual authentication between the device and the upgrade server using the upgrade server's pubic encryption and signature verification keys; exchange the session key with the upgrade manager; and send the alteration to be made to the platform component to the upgrade manager using the session key.

[9] In a fourth embodiment of the present invention, a system for securely altering a platform component is provided, comprising: means for generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered; means for obtaining public encryption and signature verification keys of a provisioning server from a certification authority; means for mutually authenticating the device and the provisioning server using the public encryption and signature verification keys; means for contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for the device; means for contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server; means for sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority; means for mutually authenticating the device and the upgrade server; means for causing the device and the upgrade server to exchange a session key; and means for providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

[10] In a fifth embodiment of the present invention, a program storage device readable by a machine tangibly embodying a program of instructions executable by the machine to perform a method for securely altering a platform component is provided, the method

comprising: generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered; obtaining public encryption and signature verification keys of a provisioning server from a certification authority; mutually authenticating the device and the provisioning server using the public encryption and signature verification keys; contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for the device; contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server; sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager's certificates for public encryption and signature verification keys from the certification authority; mutually authenticating the device and the upgrade server; causing the device and the upgrade server to exchange a session key; and providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

Advantageous Effects of Invention

[11] The present invention also enables development of new business models where platform and component manufacturers can generate a stream of revenue from the same hardware component across the duration of a user's ownership of a platform, after the initial sale. The secure, on-demand, in-field upgrade of devices allows for such a continued revenue stream.

[12] As will be appreciated to one of ordinary skill in the art, the aforementioned example architectures can be implemented in many ways, such as program instructions for execution by a processor, as software modules, microcode, as computer program product on computer readable media, as logic circuits, as application specific integrated circuits, as firmware, as consumer electronic device, etc. and may utilize wireless devices, wireless transmitters/receivers, and other portions of wireless networks. Furthermore, embodiment of the disclosed method and system for displaying multimedia content on multiple electronic display screens can take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment containing both software and hardware elements.

Brief Description of Drawings

[13] FIG. 1 is a block diagram illustrating a system for securely upgrading a platform component in accordance with an embodiment of the present invention.

[14] FIG. 2 is a diagram illustrating basic features of secure execution domains leveraged to support secure component upgrade in accordance with an embodiment of the present invention.

[15] FIG. 3 is a sequence diagram illustrating various steps of device provisioning and upgrade in accordance with an embodiment of the present invention.

Mode for the Invention

[16] Reference will now be made in detail to specific embodiments of the invention including the best modes contemplated by the inventors for carrying out the invention. Examples of these specific embodiments are illustrated in the accompanying drawings. While the invention is described in conjunction with these specific embodiments, it will be understood that it is not intended to limit the invention to the described embodiments. On the contrary, it is intended to cover alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims. In the following description, specific details are set forth in order to provide a thorough understanding of the present invention. The present invention may be practiced without some or all of these specific details. In addition, well known features may not have been described in detail to avoid unnecessarily obscuring the invention.

[17] In accordance with the present invention, the components, process steps, and/or data structures may be implemented using various types of operating systems, programming languages, computing platforms, computer programs, and/or general purpose machines. In addition, those of ordinary skill in the art will recognize that devices of a less general purpose nature, such as hardwired devices, field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein. The present invention may also be tangibly embodied as a set of computer instructions stored on a computer readable medium, such as a memory device.

[18] In an embodiment of the present invention, a mechanism is provided for secure registration and provisioning of a component of an electronic component platform. A mutual authentication protocol is then defined to mutually authenticate the component and a provisioning server. A manufacturer can build into the component certain features which are not enabled when originally sold. A customer can then elect to later upgrade the component by using the secure mutual authentication. A similar mechanism can be used for the manufacturer to "push" certain upgrades, such as software upgrades, patches, or fixes, to the electronic component platform in a secure manner.

[19] The secure and fault tolerant mechanism allows for on-demand, in-field, component upgrades. It utilizes a secure partition and privileged domain(s) to execute sensitive code, to establish secure communication channels, and to handle authentication and updates in a secure and reliable fashion. An embodiment of the present invention may

be applied to different processor based platforms, including, but not limited to, platforms with ARM processors, Samsung™ Reconfigurable Processors (SRPs), and x86 processors. Of course, the present invention is not limited to application only on processor based platforms, and can generally be applied to any electronic component platform.

[20] FIG. 1 is a block diagram illustrating a system for securely upgrading a platform component in accordance with an embodiment of the present invention. A device 100 contains a platform component 102 to be upgraded. An upgrade manager 104 is utilized to coordinate this upgrade. It should be noted that while this figure depicts upgrade manager 104 as being on a separate device than device 100, in some embodiments the upgrade manager 104 may be located on device 100. An example of the former may be where the platform component is contained on a mobile device and the corresponding upgrade manager is located on a desktop device to which the mobile device synchronizes. An example of the latter may be where the platform component and the upgrade manager are both located on a desktop device.

[21] A certification authority 106 may represent an outside authority by which mutual authentication certificates can be authorized. In one example, it is operated by the device s manufacturer. A provisioning server 108 is then used to verify device information. Finally, an upgrade server 110 contains the upgrade itself and, once mutual authentication is established between the upgrade server 110 and the device 100 (or upgrade manager 104), then the upgrade is transmitted to the device 100 (or upgrade manager 104).

[22] FIG. 2 is a diagram illustrating basic features of secure execution domains leveraged to support secure component upgrade in accordance with an embodiment of the present invention. A secure provisioning and mutual authentication mechanism is provided between an upgrade manager (on behalf of the component being upgraded) and a provisioning server/online upgrade server. A secure partition 200 is used to support the secure upgrade. The secure partition 200 provides a secure data store 202, a secure key store 204, and native cryptographic functions 206, which are only accessible from the secure monitor in a privileged mode 208 (through a secure monitor 210). The secure key store 204 is used to store cryptographic keys, a platform id, and secrets associated with provisioning, authenticating, and ensuring data integrity and confidentiality. Access to keying material requires correct authorization.

[23] The secure data store 202 is provided for storing downloaded software (and for software backup, to allow for rollback if needed). Native cryptographic functions 206 residing in the secure domain 200 are only accessible through a secure interface. Available functions include a random number generator 212, a hash generator 214, a cryptographic key generator 216, and a digital signature and encryption-decryption

engine 218.

[24] The present invention further allows for entirely new business models for manufacturers and vendors. With this secure system, it becomes possible for manufacturers to remotely upgrade a user' components, thus allowing the manufacturer to charge for more features as the user becomes more and more familiar (and perhaps reliant) on the component. Furthermore, a new type of hardware subscription business model may be introduced, where rather than (or in addition to) an upfront cost for hardware, firmware, and/or software purchases, the user pays a monthly fee (and/or a one-time cost) for a particular level of performance and/or enabling of certain components. Different levels of service may be provided based upon the amount the user is willing to pay. For example, a user needing full access to all components and the highest speed for a processor may pay to have a "gold" subscription, whereas a user who perhaps does not need as much speed or access to all of the components may subscribe to a "silver" subscription.

[25] In an embodiment of the present invention, a certification authority (CA) infrastructure is available for management and distribution of public encryption and signature verification keys. Each device may have its own device identification associated with it, for identification. The CA establishes trust between the entities in the system. The CA verifies the identity of the claimant, and issues a public key certificate, establishing an association between the identity of the claimant (e.g., upgrade manager, registration server, upgrade server) and the value of its public key. The upgrade manager then registers the device or component to be upgraded with the CA.

[26] For registration and provisioning, the upgrade manager acquires copies of the provisioning server's public encryption and signature keys from a mutually trusted certification authority. The upgrade manager then generates its key pairs for encryption/decryption and digital signatures, using the platform's cryptographic functions. The upgrade manager's private encryption and digital signature keys may be stored in the platform's secure key store. The upgrade manager, on behalf of the device or component being upgraded, provides a copy of the public encryption and digital signature keys to a mutually trusted certification authority. The upgrade manager registers the identity (e.g., device identification) of the component being upgraded, and configuration information, with the provisioning server. Upon successful registration, the provisioning server can send a registration identification to the upgrade manager, which is used during mutual authentication between the upgrade server and the upgrade manager as an alias.

[27] Mutual authentication allows systems to protect themselves against fraudulent accesses, and to link resource usage with identified entities. It helps enforce accountability, access control, and non-repudiation. This helps alleviate some of the

security issues related to component update servers that only unilaterally authenticate the customer. For example, many operating systems allow for the remote updating of their software via the Internet. An installed version of the operating system identifies itself to an update server, which authenticates the software and then updates the operating system accordingly. However, since the server can tell the client to install binary files, such a system is vulnerable to a man-in-the-middle attack, where a spoof server can tell the client to install compromising binaries. For example, the user may be fooled into attempting to update their operating system software from a malicious website, thinking that it is the real software developer. In such instances, identification of the client alone is no sufficient.

[28] Additionally, such systems are also vulnerable to a denial-of-service attack, where a rogue client can send requests requiring large processing time on the server to the server, such as by passing an unbounded set of parameters. The present invention helps alleviate these security concerns by providing for entity authentication and data origin authentication, using public key encryption and digital signatures. Entity authentication and data origin authentication is performed between the platform's upgrade manager and the upgrade server. Public key encryption is used to mutually authenticate the devic's upgrade manager and upgrade server.

[29] Communication confidentiality and data integrity are guaranteed by using a symmetric session key established during the mutual authentication phase between the upgrade manager/device and the upgrade server, to maintain authenticity of claimants during communication. The session key is stored in the platform's secure key store, and is used to decrypt the downloaded software on the platform. Data integrity and non-repudiation of origin are provided by using digital signatures.

[30] Domain separation is established by using a registration identification as an alias for the device to be upgraded.

[31] A signed and encrypted copy of any new software is downloaded to the secure data store. The digital signature of the downloaded software is verified, using the signature verification key. It should be noted that the term "software" shall be interpreted broadly to include software intended to upgrade or patch other software, as well as software intended to upgrade or patch hardware (e.g., "firmware") The key is stored in the secure key store. A signed copy of the software being upgrade from can be stored in the secure data store, or in another secure partition, to allow for upgrade rollback. The downloaded software is decrypted using the session key and is verified. This key is stored in the secure key store, during mutual authentication between the device's upgrade manager and the upgrade server. The component or device is then upgraded using the downloaded software. In case of an error, the user can rollback to the original software.

[32] FIG. 3 is a sequence diagram illustrating various steps of device provisioning and upgrade in accordance with an embodiment of the present invention. At 300, the device user requests a component or feature upgrade from the upgrade manager. At 302, the upgrade manager sends a configuration of the upgrade to the user for approval. At 304, the user approves the upgrade configuration.

[33] At 306, the upgrade manager generates encryption and digital signature key pairs on behalf of the device. At 308, the upgrade manager gets public encryption and signature verification keys of a manufacturer's provisioning server from the device manufacturer's certification authority. At 310, the device, using its device identification and through its upgrade manager and the manufacturer's provisioning server are mutually authenticated. The device is provisioned and assigned a registration identification as an alias. At 312, the upgrade manager contacts the manufacturer's certification authority to apply for certificates for the device's public encryption and signature verification keys. At 314, the certification authority verifies the device's information from the provisioning server. At 316, the upgrade manager contacts the manufacturer's certification authority to get the upgrade server's certificates for public encryption and signature verification keys.

[34] At 318, an upgrade request is sent from the upgrade manager to the upgrade server along with the device's registration identification. At 320, the upgrade server gets the upgrade manager's certificates for public encryption and signature verification keys from the certification authority. At 322, the upgrade manager/device and the upgrade server are mutually authenticated and a session key is exchanged for use during the secure upgrade. At 324, the device is securely upgraded using the session key established during mutual authentication between the upgrade server and the upgrade manager/device.

[35] It should be noted that while the above embodiments describe mutual authentication used to securely upgrade a component or device, a similar mechanism can be used to securely downgrade a component or device. For example, a user having the aforementioned "gold" membership plan may downgrade service to a "silver" level if he or she determines that the extra processing power or functionality is not needed.

[36] The present invention enables platform component upgrades to occur in the field, and under the control of the platform and the component manufacturers. This may include activation or deactivation of individual cores in a multi-core CPU or GPU in the field, as well as activation, deactivation, or configuration of features and technologies in platform components (such as hyperthreading, virtualization, remote management, etc.) after initial sale of the device.

[37] The term "computer readable medium" is used generally to refer to media such as main memory, secondary memory, removable storage, hard disks, flash memory, disk

drive memory, CD-ROM and other forms of persistent memory. It should be noted that program storage devices, as may be used to describe storage devices containing executable computer code for operating various methods of the present invention, shall not be construed to cover transitory subject matter, such as carrier waves or signals. Program storage devices and computer readable medium are terms used generally to refer to media such as main memory, secondary memory, removable storage disks, hard disk drives, and other tangible storage devices or components.

[38] Although only a few embodiments of the invention have been described in detail, it should be appreciated that the invention may be implemented in many other forms without departing from the spirit or scope of the invention. Therefore, the present embodiments should be considered illustrative and not restrictive and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

Claims

[Claim 1] A method for securely altering a platform component, comprising:
assigning certificates for public encryption and signature verification keys for the device;
assigning certificates for public encryption and signature verification keys for an upgrade server;
mutually authenticating a device containing the platform component and the upgrade server;
causing the device and the upgrade server to exchange a session key during the mutual authenticating; and
providing an alteration to be made to the platform component from the upgrade server to the device using the session key exchanged during the mutual authenticating.

[Claim 2] The method of claim 1, wherein the alteration is an upgrade or a downgrade.

[Claim 3] The method of claim 1, wherein the alteration is a downgrade.

[Claim 4] The method of claim 1, wherein the platform component is a processor.

[Claim 5] The method of claim 1, wherein the platform component is one core in a multi-core processor.

[Claim 6] The method of claim 1, wherein the platform component is a discrete or integrated hardware component on the device.

[Claim 7] The method of claim 1, wherein the platform component is a firmware or software component on the device.

[Claim 8] The method of claim 1, wherein the method is performed in response to a change in a subscription level, wherein the subscription level defines a component upgrade level and periodic price to be paid for performance matching the component upgrade level.

[Claim 9] A method for securely altering a platform component, comprising:
generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered;
obtaining public encryption and signature verification keys of a provisioning server from a certification authority;
mutually authenticating the device and the provisioning server using the public encryption and signature verification keys;
contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification

keys for the device;
contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server;
sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority;
mutually authenticating the device and the upgrade server;
causing the device and the upgrade server to exchange a session key; and
providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

[Claim 10] The method of claim 9, wherein the platform component is located in the field.

[Claim 11] The method of claim 9, wherein the method is performed in response to a change in a subscription level, wherein the subscription level defines a component upgrade level and periodic price to be paid for performance matching the component upgrade level.

[Claim 12] A system comprising:
a device containing a platform component;
an upgrade manager;
a certification authority;
a provisioning server; and
an upgrade server ;
wherein the upgrade manager is designed to:
generate encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered;
obtain public encryption and signature verification keys of a provisioning server from a certification authority;
perform one side of mutual authentication between the device and the provisioning server using the public encryption and signature verification keys of the provisioning server;
contact the certification authority for assigned certificates for public encryption and signature verification keys for the device;
contact the certification authority for assigned certificates for public en-

cryption and signature verification keys for an upgrade server;
send an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority;
perform one side of mutual authentication between the device and the upgrade server;
send a session key to the upgrade server; and
receive an alteration to be made to the platform component from the upgrade server to the device using the session key;
wherein the certification authority is designed to:
provide the encryption and signature verification keys of the provisioning server to the upgrade manager;
assign certificates for the device s public encryption and signature verification keys; and
assign certificates for the upgrade server s public encryption and signature verification keys;
wherein the provisioning server is designed to:
perform the other side of mutual authentication between the device and the provisioning server using the public encryption and signature verification keys of the provisioning server; and
verify the device s information; and
wherein the upgrade server is designed to:
obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority;
perform the other side of mutual authentication between the device and the upgrade server using the upgrade server s pubic encryption and signature verification keys;
exchange the session key with the upgrade manager; and
send the alteration to be made to the platform component to the upgrade manager using the session key.

[Claim 13] The system of claim 11, wherein the upgrade manager is located on the device.

[Claim 14] The system of claim 11, wherein the device contains:
a secure partition including a secure key store, a secure data store, and native cryptographic functions.

[Claim 15] The system of claim 13, wherein the cryptographic functions include:
a random number generator;

a hash generator;
a cryptographic key generator; and
a digital signature and encryption/decryption engine.

[Claim 16] The system of claim 14, wherein the secure partition is only accessible in a privileged mode.

[Claim 17] The system of claim 16, wherein the device further contains a secure monitor designed to determine if the device is in a privileged mode.

[Claim 18] A system for securely altering a platform component, comprising:
means for generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component being altered;
means for obtaining public encryption and signature verification keys of a provisioning server from a certification authority;
means for mutually authenticating the device and the provisioning server using the public encryption and signature verification keys;
means for contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for the device;
means for contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server;
means for sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority;
means for mutually authenticating the device and the upgrade server;
means for causing the device and the upgrade server to exchange a session key; and
means for providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

[Claim 19] The system of claim 18, wherein the platform component is a computer processor.

[Claim 20] A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine to perform a method for securely altering a platform component, the method comprising:
generating encryption and digital signature key pairs by an upgrade manager on behalf of a device containing the platform component

being altered;

obtaining public encryption and signature verification keys of a provisioning server from a certification authority;

mutually authenticating the device and the provisioning server using the public encryption and signature verification keys;

contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for the device;

contacting, by the upgrade manager, the certification authority for assigned certificates for public encryption and signature verification keys for an upgrade server;

sending an alteration request from the upgrade manager to the upgrade server, causing the upgrade server to obtain the upgrade manager s certificates for public encryption and signature verification keys from the certification authority;

mutually authenticating the device and the upgrade server;

causing the device and the upgrade server to exchange a session key; and

providing an secure alteration to be made to the platform component from the upgrade server to the device via the upgrade manager using the session key.

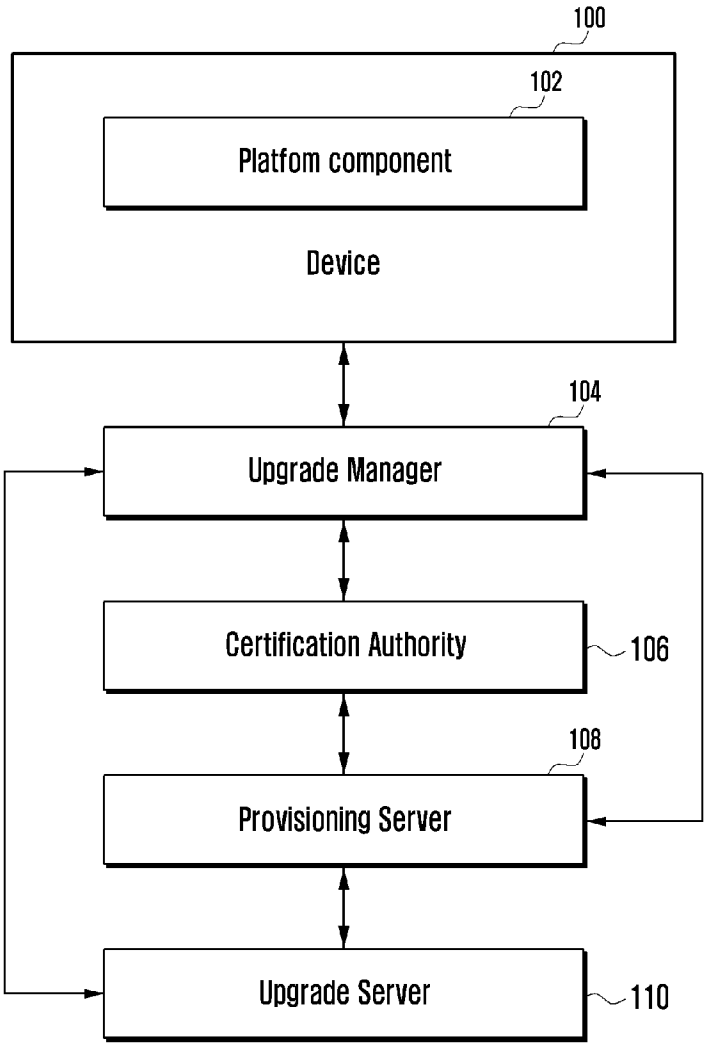
[Claim 21] The program storage device of claim 20, wherein the platform component is a feature of a hardware component.

[Claim 22] The program storage device of claim 21, wherein the feature is hyper-threading.

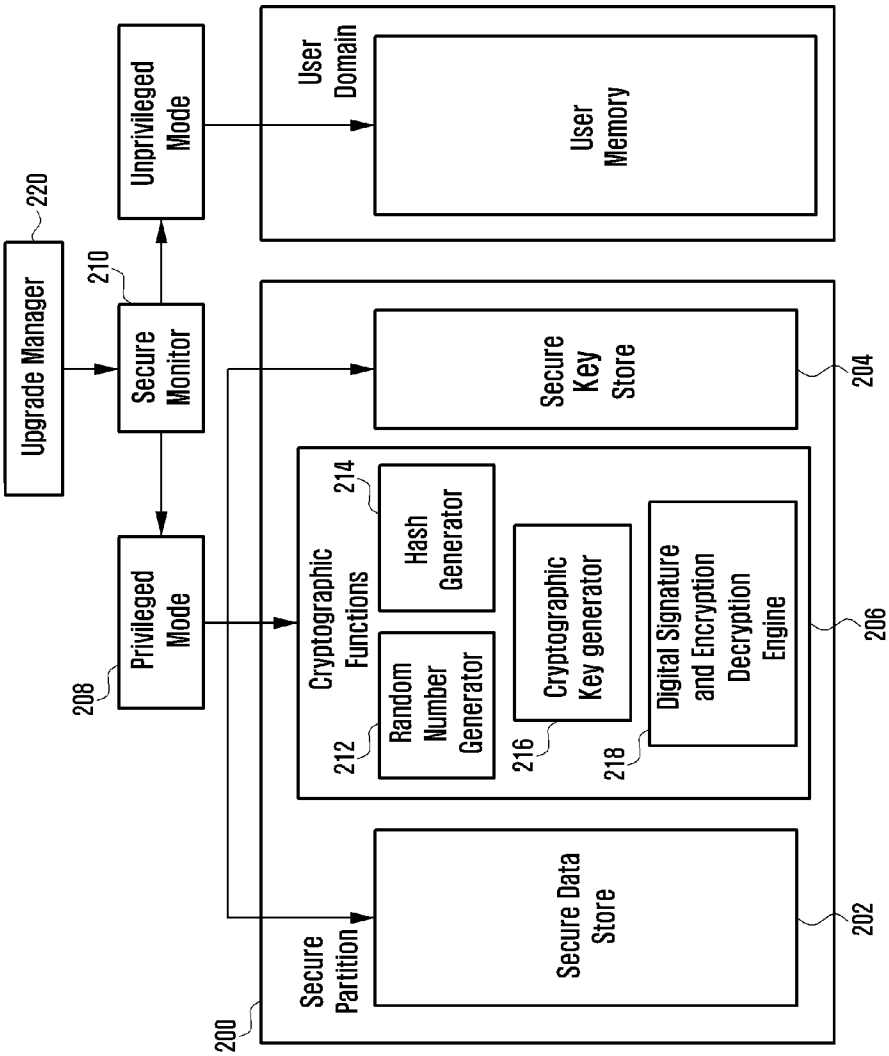
[Claim 23] The program storage device of claim 21, wherein the feature is virtualization technology.

[Claim 24] The program storage device of claim 21, wherein the feature is remote management.

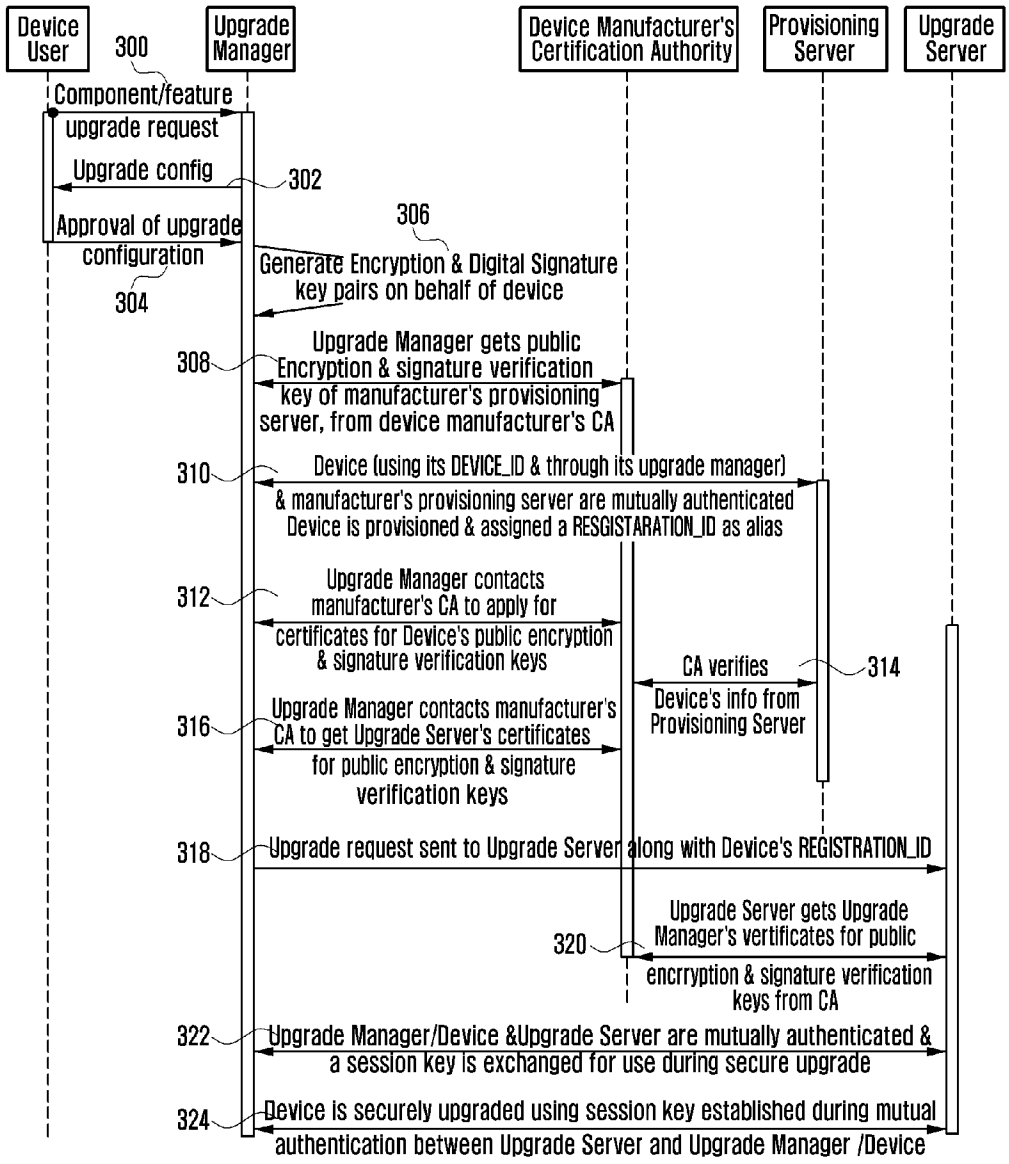
[Fig. 1]


100
102
Platfom component
Device
104
Upgrade Manager
Certification Authority
106
108
Provisioning Server
Upgrade Server
110

[Fig. 2]


Unprivileged Mode
User Domain
User Memory
220
Upgrade Manager
210
Secure Monitor
Secure Key Store
204
214
Hash Generator
Cryptographic Functions
Cryptographic Key generator
Digital Signature and Encryption Decryption Engine
206
Privileged Mode
208
212
Random Number Generator
216
218
Secure Partition
Secure Data Store
202
200

[Fig. 3]


Device User
Upgrade Manager
Device Manufacturer's Certification Authority
Provisioning Server
Upgrade Server
300
Component/feature upgrade request
Upgrade config
302
Approval of upgrade configuration
304
306
Generate Encryption & Digital Signature key pairs on behalf of device
308
Upgrade Manager gets public Encryption & signature verification key of manufacturer's provisioning server, from device manufacturer's CA
310
Device (using its DEVICE_ID & through its upgrade manager) & manufacturer's provisioning server are mutually authenticated Device is provisioned & assigned a RESGISTARATION_ID as alias
312
Upgrade Manager contacts manufacturer's CA to apply for certificates for Device's public encryption & signature verification keys
CA verifies
314
Device's info from Provisioning Server
316
Upgrade Manager contacts manufacturer's CA to get Upgrade Server's certificates for public encryption & signature verification keys
318
Upgrade request sent to Upgrade Server along with Device's REGISTRATION_ID
320
Upgrade Server gets Upgrade Manager's vertificates for public encrryption & signature verification keys from CA
322
Upgrade Manager/Device &Upgrade Server are mutually authenticated & a session key is exchanged for use during secure upgrade
324
Device is securely upgraded using session key established during mutual authentication between Upgrade Server and Upgrade Manager /Device

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/001013

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44(2013.01)i, G06F 15/16(2006.01)i, G06F 9/06(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 21/44; G06F 9/44; H04N 7/16; H04L 9/32; H04L 9/00

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: upgrade, component, mutual, authenticate and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2003-0229789 A1 (DINARTE R. MORAIS et al.) 11 December 2003 See paragraphs 13, 24-92; and figures 1, 6.	1-7 8-24
Y	US 2010-0058323 A1 (SHAHROKH SHAHIDZADEH et al.) 04 March 2010 See paragraphs 13, 28-39; and figures 1-2.	1-7
A	US 2012-0023334 A1 (ERNEST F. BRICKELL et al.) 26 January 2012 See paragraphs 26-29, 33-50; and figures 1, 3.	1-24
A	US 2008-0059799 A1 (VINCENT SCARLATA) 06 March 2008 See paragraphs 72-85; and figures 8-9.	1-24
A	US 2007-0107067 A1 (THOMAS D. FOUNTIAN) 10 May 2007 See paragraphs 37-41; and figures 5A, 5C.	1-24

☐ 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 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
15 May 2013 (15.05.2013)	**16 May 2013 (16.05.2013)**
Name and mailing address of the ISA/KR 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 BYUN, Sung Cheal Telephone No. 82-42-481-8262

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2013/001013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003-0229789 A1	11.12.2003	AT 339042 T	15.09.2006
		DE 60308099 D1	19.10.2006
		DE 60308099 T2	21.12.2006
		EP 1372292 A1	17.12.2003
		EP 1372292 B1	06.09.2006
		JP 2004-015813 A	15.01.2004
		US 7565537 B2	21.07.2009
US 2010-0058323 A1	04.03.2010	CN 101180608 A	14.05.2008
		DE 112006001308 T5	17.04.2008
		GB 0721237 D0	05.12.2007
		GB 2439889 A	09.01.2008
		GB 2439889 B	28.10.2009
		JP 05070206 B2	24.08.2012
		JP 2008-542882 A	27.11.2008
		KR 10-0962747 B1	10.06.2010
		KR 10-2008-0005567 A	14.01.2008
		TW I328189 A	01.08.2010
		US 2007-0006213 A1	04.01.2007
		US 7640541 B2	29.12.2009
		US 8375380 B2	12.02.2013
		WO 2006-127949 A1	30.11.2006
US 2012-0023334 A1	26.01.2012	WO 2012-018528 A2	09.02.2012
		WO 2012-018528 A3	05.04.2012
US 2008-0059799 A1	06.03.2008	US 7711960 B2	04.05.2010
US 2007-0107067 A1	10.05.2007	AU 2003-262857 A1	11.03.2004
		WO 2004-019182 A2	04.03.2004
		WO 2004-019182 A3	15.07.2004