



- (51) **International Patent Classification:**  
G06Q 20/40 (2012.01) G06F 9/44 (2006.01)
- (71) **International Application Number:**  
PCT/KR2013/007387
- (22) **International Filing Date:**  
16 August 2013 (16.08.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
10-2012-0089665 16 August 2012 (16.08.2012) KR
- (71) **Applicant: SAMSUNG ELECTRONICS CO., LTD.**  
[KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 443-742 (KR).
- (72) **Inventor: RYU, Jae-min;** 489, 6-ban, Ssangyong 2-ri, Seo-myeon, Yeongwol-gun, Gangwon-do 230-835 (KR).
- (74) **Agent: Y.P.LEE, MOCK & PARTNERS;** 12F Daelim Acrotel, 13 Eonju-ro 30-gil, Gangnam-gu, Seoul 135-971 (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,

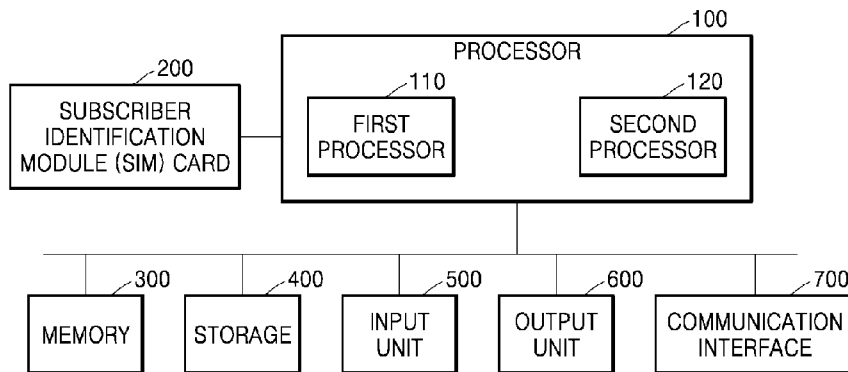
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, 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, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

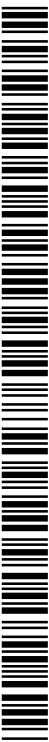
**Published:**

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) **Title:** DEVICE AND METHOD FOR PROCESSING TRANSACTION REQUEST IN PROCESSING ENVIRONMENT OF TRUST ZONE



(57) **Abstract:** Provided is a device and method for processing a transaction request in a processing environment of a trust zone. The method for processing a transaction request in a processing environment of a trust zone includes confirming whether a transaction request by an operation of an application is performed in the processing environment of the secure world, and, based on the confirmation, requesting an output unit for an output of notification information, wherein the operation of the application is performed in at least one of the processing environment of the secure world and a processing environment of a normal world, and as the transaction request is performed in the processing environment of the secure world, the notification information about the safety of the transaction request is output in the output unit.



## Description

### **Title of Invention: DEVICE AND METHOD FOR PROCESSING TRANSACTION REQUEST IN PROCESSING ENVIRONMENT OF TRUST ZONE**

#### **Technical Field**

- [1] The present invention relates to a method and device for safely processing a transaction request from an application in a processing environment of a trust zone.

#### **Background Art**

- [2] With the development of communications and network technology, transaction techniques using a device have been commercialized. Also, installing a transaction application in a device and using a payment service through the installed transaction application by users have increased. However, there are various kinds of transaction applications, and the security of the transaction applications is controlled by software, thus the transaction applications have a problem of being vulnerable to hacking. In particular, if a transaction application is infected by a virus such as malware, an execution screen of the transaction application can be forged, and through the forged screen, transaction information stored in a subscriber identification module (SIM) card of a device is put in danger of exposure. Thus, it is required to develop a technique to strengthen the security of a transaction application and to effectively notify whether the transaction application safely operates.

#### **Disclosure of Invention**

##### **Solution to Problem**

- [3] The present invention provides a method and device for processing a transaction request in a processing environment of a trust zone, wherein the safety of the transaction request is notified, based on the transaction request by an application, performed in a processing environment of a secure world.
- [4] The present invention also provides a method and device for processing a transaction request in a processing environment of a trust zone, wherein transaction information is obtained from a subscriber identification module (SIM) card, based on the transaction request by an application, performed in a processing environment of a secure world.

##### **Brief Description of Drawings**

- [5] The above and other features and advantages of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:
- [6] FIG. 1 is a block diagram of a device according to an embodiment of the present

invention;

[7] FIG. 2 is a block diagram illustrating a method of a device for processing a transaction request by an application, according to an embodiment of the present invention;

[8] FIG. 3 is flowchart illustrating a method of a device for outputting notification information according to a transaction request, according to an embodiment of the present invention;

[9] FIG. 4 is a flowchart illustrating a method of a device for obtaining transaction information from a subscriber identification module (SIM) card according to a transaction request, according to an embodiment of the present invention;

[10] FIG. 5 is block diagram illustrating a method of a device for storing a security key provided by an application in a SIM card, according to an embodiment of the present invention; and

[11] FIGS. 6 and 7 illustrate an example where a device outputs notification information, according to an embodiment of the present invention.

### **Best Mode for Carrying out the Invention**

[12] According to an aspect of the present invention, there is provided a method for processing a transaction request in a processing environment of a trust zone, the method including confirming whether a transaction request by an operation of an application is performed in a processing environment of a secure world, and, based on the confirmation, requesting an output unit for an output of notification information, whereby the operation of an application is performed in at least one of the processing environment of a secure world and a processing environment of a normal world, and as the transaction request is performed in the processing environment of a secure world, the notification information about the safety of the transaction request is output in the output unit.

[13] Confirming and requesting for the output of the notification information may be performed by a processor corresponding to the processing environment of a secure world.

[14] A processor corresponding to the processing environment of a secure world and a processor corresponding to the processing environment of a normal world are included in one processor and may be distinguished logically.

[15] As the transaction request is performed in the processing environment of a secure world, information necessary for transaction may be obtained from a subscriber identification module (SIM) card controlled in the processing environment of a secure world.

[16] Also, the method includes receiving a security key from the application, and

providing the received security key to the SIM card controlled in the processing environment of a secure world, whereby upon confirming that the application is an application authenticated in the processing environment of a secure world, the security key received may be provided to the SIM card.

- [17] The output unit is a light-emitting diode (LED) lamp, and the LED lamp may be lighted in response to the request for the output of the notification information.
- [18] The output unit is a display unit, and the output unit may display the notification information in the display unit in response to the request for the output of the notification information.
- [19] According to another aspect of the present invention, there is provided a device for processing a transaction request in a processing environment of a trust zone, the device including a processor confirming whether a transaction request performed by an operation of an application is performed in a processing environment of a secure world, and based on the confirmation requesting for an output of notification information; and an output unit outputting the notification information in response to the request, whereby as the transaction request is performed in the processing environment of a secure world, the notification information about the safety of the transaction request is output by the output unit.
- [20] The processor includes a first processor corresponding to the processing environment of a secure world and a second processor corresponding to a processing environment of a normal world, and the first processor may provide the output of the notification information to the output unit.
- [21] The first processor and the second processor are included in one processor and may be distinguished logically.
- [22] The operation of the application may be divided into an operation performed in the processing environment of a secure world and an operation performed in the processing environment of a normal world.
- [23] As the transaction request is performed in the processing environment of a secure world, information necessary for transaction may be obtained from a subscriber identification module (SIM) card controlled in the processing environment of a secure world.
- [24] The processor receives a security key from the application, and if the application is an application authenticated in the processing environment of a secure world, the security key that is received may be provided to the SIM card controlled in the processing environment of a secure world.
- [25] The output unit may include at least one of LED and other screens included in the device.
- [26] According to another aspect of the present invention, there is provided a computer

readable medium having embodied thereon a computer program for the method.

### **Mode for the Invention**

- [27] The present invention will now be described more fully with reference to the accompanying drawings, in which exemplary embodiments of the present invention are shown. The present invention may, however, be embodied in many different forms and should not be construed as being limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the present invention. Furthermore, a detailed description of other parts will not be provided not to make the present invention unclear. Like reference numerals in the drawings refer to like elements throughout.
- [28] Throughout the specification, it will be understood that when an element is referred to as being “connected” to another element, it may be “directly connected” to the other element or “electrically connected” to the other element with intervening elements therebetween. It will be further understood that when a part “includes” or “comprises” an element, unless otherwise defined, the part may further include other elements, not excluding the other elements.
- [29] Hereinafter, the present invention will be described in detail by explaining exemplary embodiments of the invention with reference to the attached drawings.
- [30] FIG. 1 is a block diagram of a device according to an embodiment of the present invention.
- [31] As shown in FIG. 1, the device includes a processor 100, a subscriber identification module (SIM) card 200, a memory 300, a storage 400, an input unit 500, an output unit 600, and a communication interface 700. Also, the processor 100 may include a first processor of a secure world 110 and a second processor of a normal world 120.
- [32] In addition, the device operates in a processing environment of a “trust zone,” and may protect a processor circuit and memory of the device from a software attack. The processing environment of the “trust zone” may include a processing environment of a secure world and a processing environment of a normal world. Also, the processing environment of the normal world may not have an access to the processing environment of the secure world. Furthermore, a predetermined access to a hardware device may be set to be available only in the processing environment of the secure world.
- [33] The device may be a computing platform performing an application program. For example, the device may be a smart phone, a cellular phone, a personal digital assistant (PDA), a laptop, a media player, a global positioning system (GPS), or other mobile or non-mobile computing devices, but may not be restricted thereto. Also, the processor 100, the SIM card 200, the memory 300, the storage 400, the input unit 500, the output unit 600, and the communication interface 700 may respectively be connected to one

another via a system bus including more than one bus. When there are a plurality of buses, buses may be bridged by more than one bridge of bus (not shown).

[34] The processor 100 may be a central processing unit (CPU) having an architecture based on a secure structure type of a "trust zone." The processing environment of the "trust zone" may protect a processor circuit and memory from a software attack. The processing environment of the "trust zone" may display data and security code, and may divide secure data and normal data to be separately processed separately with the help of hardware. The processor 100 may include the first processor of the secure world 110 and the second processor of the normal world 120. The first processor of the secure world 110 may perform a secure operation, and the second processor of the normal world 120 may perform a normal operation. Also, the first processor 110 may be separated from an access from the outside and be protected from an unauthorized control of the second processor 120. In addition, the first processor 110 and the second processor 120 may be separate processors physically, but may not be restricted thereto. The first processor 110 and the second processor 120 are included in one processor and may be distinguished logically.

[35] Furthermore, an operation of an application according to an embodiment of the present invention may be divided into an operation in a processing environment of a secure world and an operation in a processing environment of a normal world. For example, an operation related to transaction among operations of the application may be configured to be performed in a processing environment of a secure world, and an operation less related to a security such as a control of a user interface (UI) may be configured to be performed in a processing environment of a normal world. In this case, based on an input through the UI in the processing environment of the normal world, a transaction operation may be requested to the processing environment of the secure world.

[36] The processor 100 confirms whether a transaction request by an operation of an application is performed in a processing environment of a secure world. The processor 100 confirms whether the transaction request is performed by the first processor 110 corresponding to the processing environment of the secure world, thereby confirming that the transaction request by the operation of the application is performed in the processing environment of the secure world.

[37] Also, whether the transaction request is performed in the processing environment of the secure world may be confirmed in the processing environment of the secure world. For example, the first processor 110 among the first processor 110 and the second processor 120 included in the processor 100 may confirm whether the transaction request is performed in the processing environment of the secure world.

[38] Upon confirming that the transaction request is performed in the processing en-

vironment of the secure world, the processor 100 may request an output unit 600 that will be described later on for an output of notification information about the safety of the transaction request. For example, when the application is hacked into and the transaction request is performed by the hacked application in a processing environment of a normal world, the processor 100 may confirm that the transaction request is not performed in the processing environment of the secure world and ignore the transaction request.

- [39] Upon confirming that the transaction request is performed in the processing environment of the secure world, the processor 100 may extract transaction information from a subscriber identification module (SIM) card 200 that will be described later on. The transaction information, for example, may include device user's user information, card information, and authentication information. Also, the SIM card 200 may be controlled in the processing environment of the secure world.
- [40] In addition, the processor 100 may receive a security card from the application and store the received security card in the SIM card 200. In this case, the processor 100 may authenticate an application, and when the application is authenticated, the processor 100 may store the received security card in the SIM card 200. Also, the authentication of the application may be performed in the processing environment of the secure world. For example, the application may be authenticated by the first processor 110 corresponding to the processing environment of the secure world.
- [41] The SIM card 200 stores transaction information and stores the security key received from the application. The SIM card 200 may be controlled by the processor 100 in the processing environment of the secure world. Also, the SIM card 200 may be connected to the first processor 110 corresponding to the processing environment of the secure world, but may not be restricted thereto.
- [42] The memory 300 may store an instruction and data used for performing an operation and function of the processor 100. The memory 300, for example, may include a random access memory (RAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), a synchronous dynamic random access memory (SDRAM), and a double data rate random access memory (DDRRAM), but may not be restricted thereto. The memory 300 may include more than one code and/or data sequence and be referred to as an operating memory. The code sequence may be a machine instruction set or a machine instruction group indicating more than one function call, subroutine, or operation. In this specification, a program may individually refer to one among these, or a combination of more than one of these.
- [43] The storage 400 may indicate a non-volatile storage storing permanent data. A non-volatile storage denotes a storing medium maintaining the value even if the power of the storage device is removed. The permanent data denotes data that is maintained

even if the power provided to the device is stopped. For example, the permanent data may include a system file, an operating system, a program file, and a configuration file. Also, the storage 400 may include a disk and a related drive (for example, a magneto-optical drive), a universal serial bus (USB) and a related port, a flash memory, a read-only memory (ROM), and a non-volatile solid state drive.

- [44] The input unit 500 generates an input signal input into the device based on an input by a user. The input unit 500, for example, may include a keyboard, a mouse, a touch screen, and a keypad, but may not be restricted thereto.
- [45] The output unit 600 outputs an output signal generated from the device. The output unit 600 may output at least one of an audio signal and a video signal, but may not be restricted thereto. The output unit 600, for example, may include a display unit, a speaker, a vibration sensor, and a light-emitting diode (LED) lamp.
- [46] When a transaction request is performed in the processing environment of the secure world, the output unit 600 may output notification information about the safety of the transaction request. For example, if the output unit 600 is an LED lamp, the notification information about the safety of the transaction request may be output by the LED lamp flickering in certain colors and texture patterns. Also, if the output unit 600 is a display unit, the notification information about the safety of the transaction request may be output by certain texts displayed on the display unit.
- [47] In addition, the output unit 600 may be set to be controlled only in the processing environment of the secure world.
- [48] The communication interface 700 enables the device to communicate with other devices through a network. The communication interface 700, for example, may include a network interface card, and a modem, but may not be restricted thereto.
- [49] FIG. 2 is a block diagram illustrating a method of a device for processing a transaction request by an application, according to an embodiment of the present invention.
- [50] As shown in FIG. 2, an operation of a transaction application may be performed in at least one of a processing environment of a secure world and a processing environment of a normal world. Also, an operation performed in the processing environment of the secure world and an operation performed in the processing environment of the normal world may be pre-set. For example, the transaction request may be set to be performed by the transaction application in the processing environment of the secure world.
- [51] If the transaction application operates normally and the transaction request is performed in the processing environment of the secure world, a trust zone protection controller (TZPC) may request the output unit 600 for an output of notification information about the safety of the transaction request.
- [52] If the transaction application is hacked into and the transaction request is performed



by the transaction application in the processing environment of the normal world, the TZPC may ignore the transaction request from the transaction application. However, it may not be restricted thereto, and the TZPC may request the output unit 600 for an output of notification information about the unsafety of the transaction request.

[53] FIG. 3 is a flowchart illustrating a method of a device for outputting notification information according to a transaction request, according to an embodiment of the present invention.

[54] In operation S300, the device confirms the transaction request of an application. The application installed in the device may generate a request signal for transaction information from the SIM card 200 to perform transaction, and the device may confirm the transaction request performed by the application.

[55] In operation S302, the device determines whether the transaction request is performed in a processing environment of a secure world. The device may determine whether the transaction request by the application is performed in the processing environment of the secure world, or a processing environment of a normal world. For example, the device may determine whether the transaction request is performed by the first processor 110 of the device or by the second processor 120 of the device, but may be not restricted thereto.

[56] If the application is hacked into and the transaction request is performed by the application, the device may determine that the transaction request is performed in the processing environment of the normal world.

[57] In operation S302, if it is determined that the transaction request is performed in the processing environment of the secure world, the device requests the output unit 600 for an output of notification information in operation S304. The notification information is about the safety of the transaction request, and pre-set notification information according to the kinds of the output unit 600 may be output. For example, if the output unit 600 is an LED lamp, the notification information about the safety of the transaction request may be output by the LED lamp flickering in certain colors and texture patterns. Also, if the output unit 600 is a display unit, the notification information about the safety of the transaction request may be output by certain texts displayed on the display unit.

[58] In addition, in operation S302, if it is determined that the transaction request is not performed in the processing environment of the secure world, the device may ignore the transaction request.

[59] Operations S303 to S304 may be performed in the processing environment of the secure world, but may not be restricted thereto. Operations S300 to S304 may be partially performed in the processing environment of the normal world.

[60] FIG. 4 is a flowchart illustrating a method of a device for obtaining transaction in-

formation from an SIM card according to a transaction request, according to an embodiment of the present invention.

- [61] In operation S400, the device confirms the transaction request of an application. The application installed in the device may generate a request signal for transaction information to be obtained from the SIM card 200 to perform transaction, and the device may confirm the transaction request by the application.
- [62] In operation S402, the device determines whether the transaction request is performed in a processing environment of a secure world. The device may determine whether the transaction request from the application is performed in the processing environment of the secure world or a processing environment of a normal world. For example, the device may determine whether the transaction request is performed by the first processor 110 of the device or by the second processor 120 of the device, but may not be restricted thereto.
- [63] If the application is hacked into and the transaction request is performed by the application, the device may determine that the transaction request is performed in the processing environment of the normal world.
- [64] In operation S402, if it is determined that the transaction request is performed in the processing environment of the secure world, the device extracts transaction information from the SIM card 200, in operation S404. For example, the transaction information may include a device user's user information, card information, and authentication information. Also, The SIM card 200 may be controlled in the processing environment of the secure world.
- [65] In addition, in operation S402, if it is determined that the transaction request is not performed in the processing environment of the secure world, the device may ignore the transaction request.
- [66] Operations S400 to S404 may be performed in the processing environment of the secure world, but may not be restricted thereto. Operations S400 to S404 may be partially performed in the processing environment of the normal world.
- [67] FIG. 5 is block diagram illustrating a method of a device for storing a security key provided by an SIM card, according to an embodiment of the present invention.
- [68] In operation S500, the device receives the security key from a transaction application. The processor 100 of the device may receive the security key from the transaction application installed in the device. The security key may be generated by the transaction application or received from the outside by the transaction application, but may not be restricted thereto.
- [69] In operation S502, the device authenticates the transaction application in a processing environment of a secure world. The first processor 110 corresponding to the processing environment of the secure world may confirm whether the transaction application is an

authenticated application.

- [70] If the transaction application is an authenticated application, the device stores the security key in the SIM card 200, in operation S504. The SIM card 200 may be controlled by the processor 100 in the processing environment of the secure world. In this case, the security key may be stored in the SIM card 200 by using a NFC controller or a call processor operated in the processing environment of the secure world.
- [71] FIG. 5 illustrates an example where a security key of a transaction application is stored in a SIM card 200, but may not be restricted thereto. When a SIM client (not shown) operating in a processing environment of a normal world sends an application protocol data unit (APDU) command to an APDU agent (not shown) operating in a processing environment of a secure world, the APDU agent (not shown) may authenticate the SIM client (not shown). Also, if the SIM client (not shown) is authenticated, the APDU agent (not shown) may access the SIM card 200 by the NFC controller or the call processor operating in the processing environment of the secure world.
- [72] FIGS. 6 and 7 illustrate an example where a device outputs notification information, according to an embodiment of the present invention.
- [73] As shown in FIG. 6, when a transaction request is performed in a processing environment of a secure world, the device may notify about the safety of the transaction request by lighting an LED lamp 60 in pre-determined colors and texture patterns.
- [74] Also, as shown in FIG. 7, when the transaction request is performed in the processing environment of the secure world, the device may display the text notifying about the safety of the transaction request on a screen of the device 70.
- [75] The one or more embodiments of the present invention may be embodied as a recording medium, e.g., a program module to be executed in computers, which include computer-readable commands. The computer storage medium may include any usable medium that may be accessed by computers, volatile and non-volatile media, and detachable and non-detachable media. Also, the computer storage medium may include a computer storage medium and a communication medium. The computer storage medium includes all of volatile and non-volatile media, and detachable and non-detachable media which are designed to store information including computer readable commands, data structures, program modules, or other data. The communication medium includes computer-readable commands, a data structure, a program module, and other transmission mechanisms, and includes other information transmission media.
- [76] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by one of ordinary skill in the

art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims. Hence, it will be understood that the embodiments described above are not limiting of the scope of the invention. For example, each component described in a single type may be executed in a distributed manner, and components described distributed may also be executed in an integrated form.

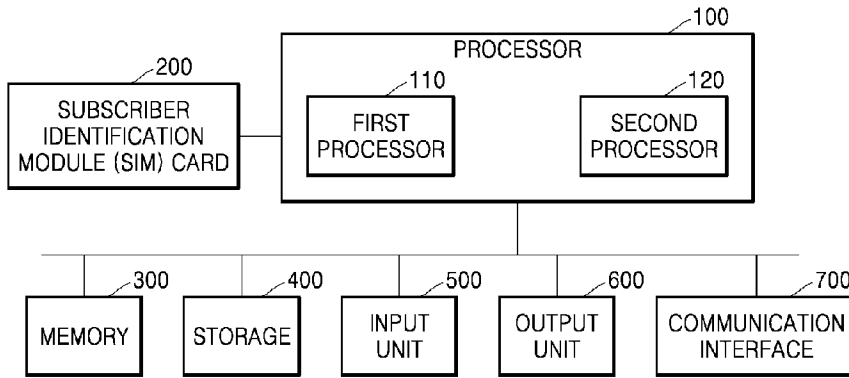
[77] The scope of the invention is defined not by the detailed description of the invention but by the appended claims, and all differences within the scope will be construed as being included in the present invention.

## Claims

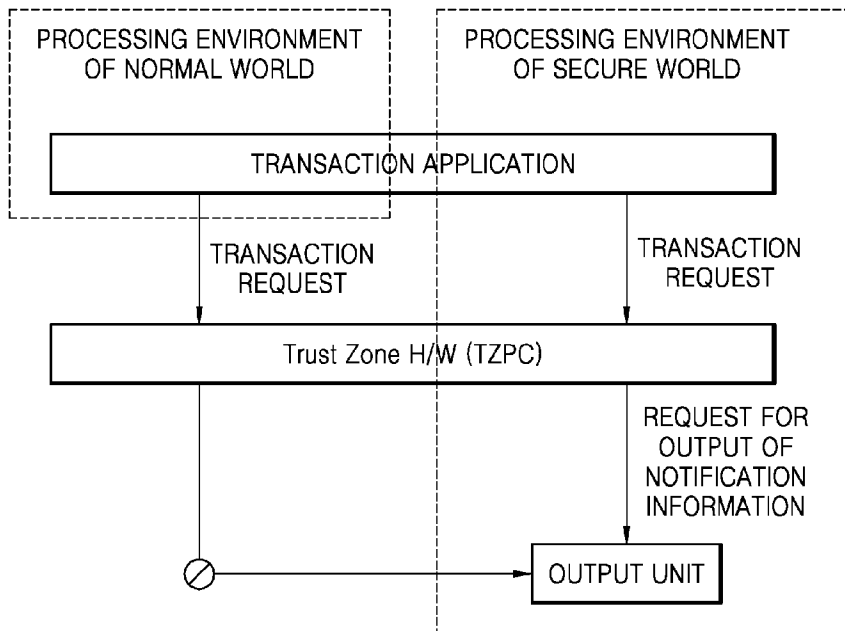
- [Claim 1] A method for processing a transaction request in a processing environment of a trust zone, the method comprising:  
confirming whether a transaction request by an operation of an application is performed in a processing environment of a secure world;  
and  
based on the confirmation, requesting an output unit for an output of notification information,  
wherein the operation of the application is performed in at least one of the processing environment of the secure world and a processing environment of a normal world, and as the transaction request is performed in the processing environment of the secure world, the notification information for notifying safety of the transaction request is output in the output unit.
- [Claim 2] The method of claim 1, wherein the confirming and the requesting for the output of the notification information are performed by a processor corresponding to the processing environment of the secure world.
- [Claim 3] The method of claim 1, wherein a processor corresponding to the processing environment of the secure world and a processor corresponding to the processing environment of the normal world are included in one processor and are distinguished logically.
- [Claim 4] The method of claim 1, wherein as the transaction request is performed in the processing environment of the secure world, information necessary for transaction is obtained from a subscriber identification module (SIM) card controlled in the processing environment of the secure world.
- [Claim 5] The method of claim 1, further comprising:  
receiving a security key from the application; and  
providing the received security key to the SIM card controlled in the processing environment of the secure world,  
wherein upon confirming that the application is an application authenticated in the processing environment of the secure world, the received security key is provided to the SIM card.
- [Claim 6] The method of claim 1, wherein the output unit is a light-emitting diode (LED) lamp, and the light-emitting diode (LED) lamp is lighted in response to the request for the output of the notification information.
- [Claim 7] The method of claim 1, wherein the output unit is a display unit, and

- the output unit displays the notification information on the display unit in response to the request for the output of the notification information.
- [Claim 8] A device for processing a transaction request in a processing environment of a trust zone, the device comprising:  
a processor confirming whether a transaction request performed by an operation of an application is performed in a processing environment of a secure world, and, based on the confirmation, requesting for an output of notification information; and  
an output unit outputting the notification information in response to the request,  
wherein as the transaction request is performed in the processing environment of the secure world, the notification information for notifying safety of the transaction request is output by the output unit.
- [Claim 9] The device of claim 8, wherein the processor comprises a first processor corresponding to the processing environment of the secure world and a second processor corresponding to a processing environment of a normal world, and the first processor provides the output of the notification information to the output unit.
- [Claim 10] The device of claim 9, wherein the first processor and the second processor are included in one processor and are distinguished logically.
- [Claim 11] The device of claim 8, wherein the operation of the application is divided into an operation performed in the processing environment of the secure world and an operation performed in a processing environment of a normal world.
- [Claim 12] The device of claim 8, wherein as the transaction request is performed in the processing environment of the secure world, information necessary for transaction is obtained from a subscriber identification module (SIM) card controlled in the processing environment of the secure world.
- [Claim 13] The device of claim 8, wherein the processor receives a security key from the application, and if the application is an application authenticated in the processing environment of the secure world, the received security key is provided to the SIM card controlled in the processing environment of the secure world.
- [Claim 14] The device of claim 8, wherein the output unit comprises at least one of a light-emitting diode (LED) and other screens included in the device.
- [Claim 15] A computer readable medium having embodied thereon a computer program for executing the method of claim 1.

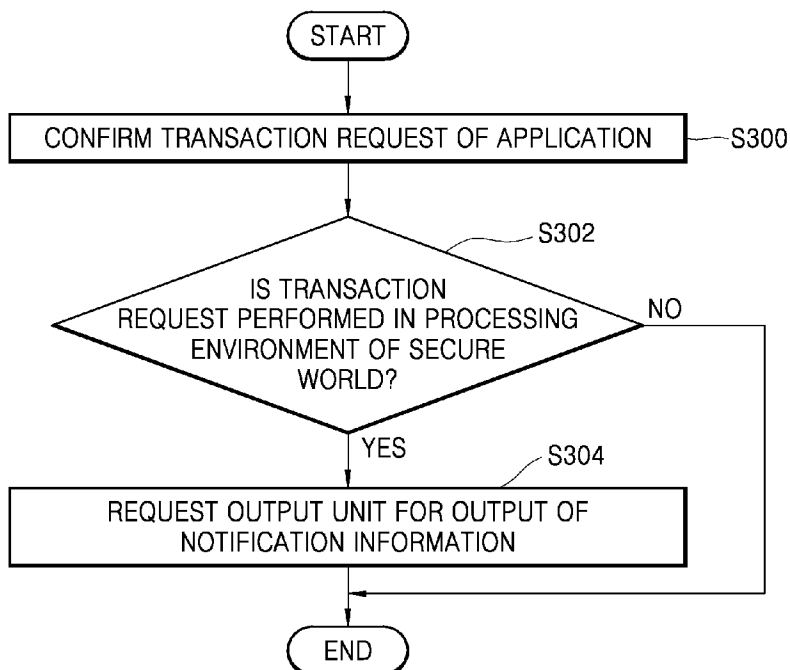
[Fig. 1]



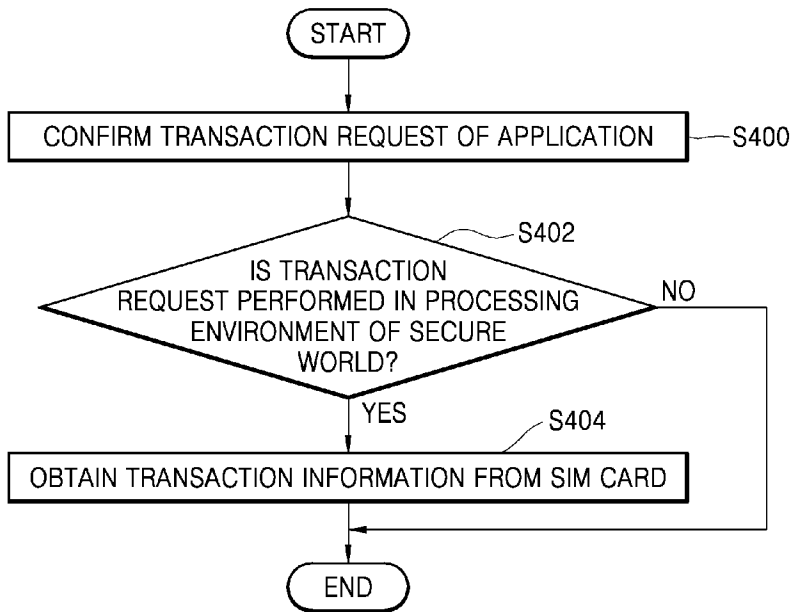
[Fig. 2]



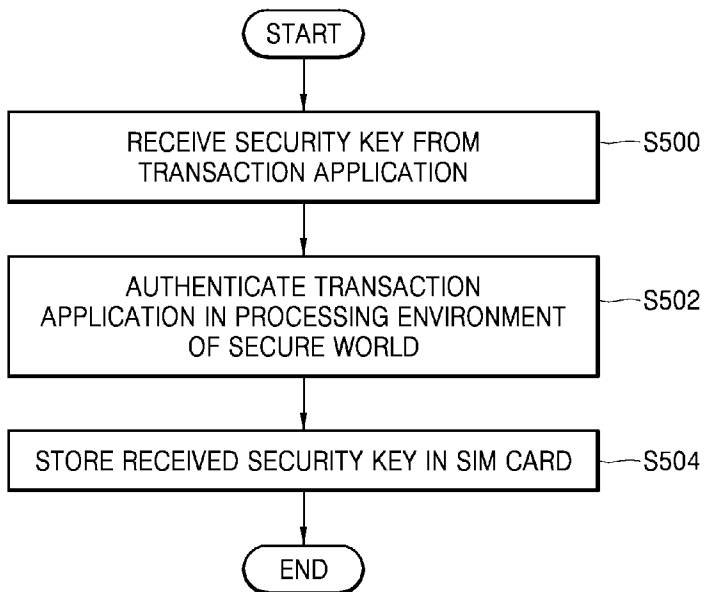
[Fig. 3]



[Fig. 4]

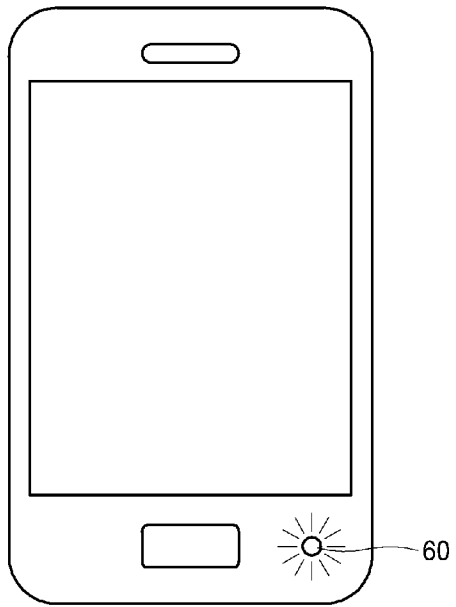


[Fig. 5]

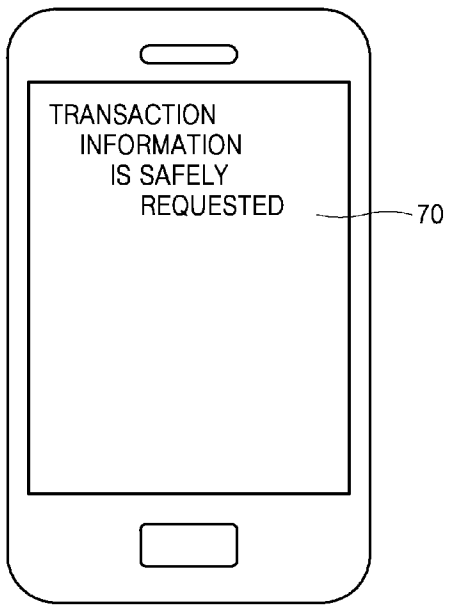




[Fig. 6]



[Fig. 7]



**A. CLASSIFICATION OF SUBJECT MATTER****G06Q 20/40(2012.01)i, G06F 9/44(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)

G06Q 20/40; H04K 1/00; G06F 9/445; H04N 7/16; G06F 12/14; H04L 9/32; H04B 1/40

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) &amp; Keywords: transaction, secure world, application, processor, SIM

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006-0075264 A1 (BRYAN MARK WILLMAN et al.) 06 April 2006 See abstract, paragraphs [0005]-[0006],[0051], claims 1-57, and figures 2-4.	1-3,6-11,14-15
Y		4-5,12-13
Y	KR 10-2003-0037830 A (LG ELECTRONICS INC.) 16 May 2003 See abstract, claims 1-4, and figure 1.	4,12
Y	KR 10-0646359 B1 (SK TELECOM CO., LTD.) 23 November 2006 See abstract, claims 1-6, and figure 3.	5,13
A	US 2006-0195907 A1 (ECKHARD DELFS et al.) 31 August 2006 See abstract, claims 1-31, and figure 1.	1-15
A	WO 03-090074 A2 (ADVANCED MICRO DEVICES, INC.) 30 October 2003 See abstract, claims 1-10, and figure 2.	1-15

 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

"&amp;" document member of the same patent family


Date of the actual completion of the international search

12 December 2013 (12.12.2013)

Date of mailing of the international search report

**12 December 2013 (12.12.2013)**

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

OH, Eung Gie

Telephone No. +82-42-481-8744



**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/KR2013/007387**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0075264 A1	06/04/2006	CN 1755639 A	05/04/2006
		CN 1755639 C0	05/04/2006
		EP 1643341 A2	05/04/2006
		JP 2006-107455 A	20/04/2006
		KR 10-2006-0050661 A	19/05/2006
		US 7574610 B2	11/08/2009
KR 10-2003-0037830 A	16/05/2003	None	
KR 10-0646359 B1	23/11/2006	None	
US 2006-0195907 A1	31/08/2006	CN 1794256 A	28/06/2006
		DE 102004062203 A1	13/07/2006
		DE 102004062203 B4	08/03/2007
		FR 2885424 A1	10/11/2006
		FR 2885424 B1	05/08/2011
		GB 0526370 D0	01/02/2006
		GB 2421610 A	28/06/2006
		JP 2006-179011 A	06/07/2006
		JP 2010-092485 A	22/04/2010
		KR 10-0774013 B1	08/11/2007
		KR 10-2006-0073474 A	28/06/2006
		WO 03-090074 A2	30/10/2003
AU 2003-231070 A1	03/11/2003		
CN 100339780 C0	26/09/2007		
CN 1285033 C0	15/11/2006		
CN 1647039 A	27/07/2005		
CN 1647039 C0	15/11/2006		
DE 60311441 D1	15/03/2007		
DE 60311441 T2	08/11/2007		
EP 1495394 A2	12/01/2005		
EP 1495394 B1	23/07/2008		
EP 1495401 A2	12/01/2005		
EP 1495401 B1	24/01/2007		
JP 04564756 B2	20/10/2010		
JP 04762494 B2	31/08/2011		
JP 2005-528677 A	22/09/2005		
JP 2005-528678 A	22/09/2005		
KR 10-0921779 B1	15/10/2009		
KR 10-0950102 B1	29/03/2010		
US 2004-0210760 A1	21/10/2004		
US 2004-0210764 A1	21/10/2004		
US 7603550 B2	13/10/2009		
US 7603551 B2	13/10/2009		
WO 03-090052 A2	30/10/2003		
WO 03-090052 A3	12/08/2004		
WO 03-090074 A3	19/08/2004		