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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2010 (15.04.2010)

PCT

(10) International Publication Number
WO 2010/040407 A1

(51) International Patent Classification:
G06F 21/22 (2006.01)

(21) International Application Number:
PCT/EP2008/063491

(22) International Filing Date:
8 October 2008 (08.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TAKALA, Janne** [FI/FI]; Omakatu 34 as 13, FIN-33500 Tampere (FI). **VAINIO, Juha Johannes** [FI/FI]; Katajarinne 3A, FIN-37470 Vesilahti (FI). **BUCHHOLTZ, Mikael** [DK/DK]; Ravnsborggade 20 A, 4. th, DK-2200 København N (DK).

(74) Agents: **JOHANSSON, Anna Olivia** et al.; 20 Little Britain, London EC1A 7DH (GB).

(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, BR, BW, BY, BZ, CA, CH, 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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

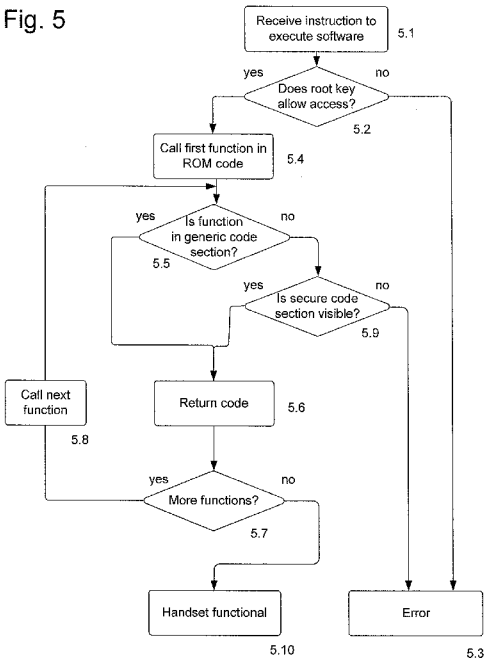
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,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

Published:

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

(54) **Title**: MEMORY ACCESS CONTROL

Fig. 5



(57) **Abstract**: An apparatus comprising: a memory having at least two sections; a security element associated with at least one of said at least two sections; and a processor for controlling access to at least one of the at least two sections of the memory in dependence on a value of the security element. The apparatus may be an integrated circuit and the memory may be a read-only-memory storing generic code in one of the sections and code specific to a mobile communication device provider in the second section. The security element may be a permanently programmed memory element programmed by the IC manufacturer.

WO 2010/040407 A1

Memory Access Control

Technical Field

The invention relates to an apparatus, a method and a computer program for controlling access to memory. More particularly, but not exclusively, the invention relates to the control of read only memory code of an integrated circuit.

Background

Users of mobile communication devices and content providers for the mobile communication devices expect the devices to be provided with a suite of software that makes the operation of the mobile communication device secure and the handling of the content fair to the content providers. Mobile communication device providers also want to protect their software from being copied and modified by other mobile communication device providers or users. Mobile communication device providers or manufacturers therefore include security mechanisms in their devices and in their software that put restrictions on the software that can be used in the devices and stop the software from being modified to, for example, circumvent subscriber identity module (SIM) lock and digital rights management (DRM) protection mechanisms.

One way of protecting software is for mobile communication device providers to encrypt their software images and to program the integrated circuits (ICs) of their mobile devices with a root key related to a key certificate comprising a key for decrypting the software image. Another way involves providing the software image without encryption but adding a digital signature to it. The signature is then compared to a key in the key certificate associated with the root key of the IC. Encrypting or signing the software ensures that only a device programmed with the right key can run the software. If the manufacture of ICs is outsourced, the manufacturer of the ICs can program the ICs with the key of the mobile communication device provider to which the ICs are sold.

Mobile communication device providers may also instruct the IC manufacturer to program the IC with code needed for booting up the system and critical system libraries.

The invention was made in this context.

Summary

According to an embodiment of the invention, there is provided an apparatus comprising: a memory having at least two sections; a security element associated with at least one of said at least two sections; and a processor for controlling access to the at least one of the at least two sections of the memory in dependence on a value of the security element.

The security element may be a permanently programmed memory element. The memory may be a read-only-memory.

The processor may be configured to control a memory map to render the at least one section visible when the security element has a predetermined value.

The processor may further be operable to run a computer program and said memory may be configured to store secure code for calling by said program. The apparatus may further store information indicative of a key, the processor being operable to only run said computer program if it has been signed with said key.

The security element may be a one time programmable bit.

According to an embodiment of the invention, there is also provided an integrated circuit comprising the apparatus.

Furthermore, according to an embodiment of the invention, there is provided a mobile terminal comprising the apparatus. The security element may be programmed in dependence on the manufacturer of the mobile terminal.

Yet further, according to an embodiment of the invention, there is provided a method comprising: determining a value of a security element associated with a section of a memory having at least two sections, the memory storing code for calling by a computer program; and controlling access to said section of said memory in dependence on said value.

The security element may be a permanently programmed memory element. The memory may be a read only memory.

Controlling access may comprise controlling a memory map to only make said section visible to the program when the security element has a predetermined value.

The method may further comprise running said program only if said program has been signed with a key matching a key indicated by stored information.

The security element may be a one-time programmable bit.

The memory and the security element may be provided in an integrated circuit. The security element may be programmed in dependence on a provider of a device comprising the integrated circuit.

According to an embodiment of the invention, there is also provided a computer program comprising instructions that when executed by a processor cause the processor to execute the method. A computer readable medium storing the computer program is also provided according to an embodiment of the invention.

Brief Description of Drawings

Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:-

Figure 1 is a view of a mobile telephone handset according to an embodiment of the invention;

Figure 2 is a schematic diagram of the major circuitry components of the handset of Figure 1;

Figure 3 is a schematic diagram of the components of the integrated circuit of Figure 2;

Figure 4a and 4b illustrate how access to memory of the integrated circuit is controlled;

Figure 5 illustrates a method of executing a computer program in the mobile telephone handset.

Detailed Description

Referring to Figure 1, a mobile terminal in the form of a mobile telephone handset 1 includes a microphone 2, keypad 3, with soft keys 4 which can be programmed to perform different functions, an LCD display 5, an ear-piece 6, an antenna configuration 7 which is contained within its housing and a battery 8 behind a battery cover. The antenna configuration 7 may include one or more separate antennas for communicating signals of different frequencies.

The handset 1 is operable to communicate, through cellular radio apparatus 9 with one or more individual land mobile networks 10, some of which may be packet switched networks, such as, but not limited to GSM, GPRS and CDMA networks.

Figure 2 illustrates the major circuit components of the handset 1. The components may be mounted on a printed wire board or a printed circuit board. Signal processing is carried out under the control of a processing unit provided by an IC 11, which will be described in more detail below, with respect to Figure 3. The IC may execute stored instructions in response to signals from the keypad and soft keys 3, 4. The IC also controls operation of the LCD display 5. Electrical analogue audio signals are produced by microphone 2 and amplified by

amplifier 15. Similarly, analogue audio signals are fed to earpiece 6 through an amplifier 13.

Information concerning the identity of the user is held on a smart card 14 in the form of, for example, a GSM SIM. The SIM card is removably received in a SIM cardholder 15.

In addition to memory internal to the IC 11, which will be described in more detail with respect to Figure 3, the handset also comprises external memory 16. The external memory 16 may include a permanent non-removable memory, such as flash memory and a random access memory (RAM). The operating system and application programs of the mobile communication device may be stored in the flash memory. The external memory 16 may also comprise removable memory in the form of, for example, a memory card such as a CompactFlash card, a Multimedia Card (MMC) or a Memory Stick.

The handset circuitry includes a codec 17 and a radio frequency (RF) interface 18 connected to the antenna configuration 7. The codec 17 receives analogue signals from the microphone amplifier 12, digitises them into, for example, a GSM signal format and feeds them to the RF interface 18 for transmission through the antenna configuration 7 to the network 10. Data signals are also fed to the RF interface 18 for transmission through the antenna 7 to the networks 10. Signals received from the network 10 are fed through the antenna configuration 7 to be demodulated in the RF interface 18. Audio signals are fed to codec 17, so as to produce analogue signals fed to the amplifier 13 and the earpiece 6 and data signals are fed to the processor integrated circuit 11, the memory 16 and display 5. All the components of Figure 2 draw power from a battery 8.

With reference to Figure 3, the IC 11 comprises at least one central processor (CPU) 19 connected to on-chip read only memory (ROM) 20 and on-chip

random access memory (RAM) 21. It further comprises a root key 22, a security element 23 and security logic 24.

The on-chip ROM 20 stores, for example, code needed for booting up the mobile device and critical system libraries called by the software image stored in the external memory 16. The ROM code is programmed during the manufacture of the IC and cannot be changed. In some embodiments of the invention, the ROM code comprises two sections, a first section 20a for storing generic code and a second section 20b for storing customer specific code. A mobile telephone handset provider or manufacturer may instruct the manufacturer of the IC to program the second section 20b with code specific to the handset provider. The first and the second sections will hereinafter be referred to as a generic code section 20a and a secure code section 20b. However, these labels should not be interpreted as limiting. The first and second sections of the ROM code 20 could also be used to store other types of code and data.

The on-chip RAM 21 is used for running some of the software stored in the external memory 16. The software image is typically divided into user code and public and secure kernel code. The secure kernel code is run in the on-chip RAM 21 in a CPU secure mode while the user code and the public kernel code is typically run in RAM in the external memory 16. The generic code section 20a of the ROM code may store functionality for copying secure kernel code from the external memory 16 to the on-chip RAM 21.

The root key 22, the security element 23 and the security logic 24 are provided to determine which software images can run on the IC 11 and to control access to customer specific code in the ROM 20. The processor 19 executes the security logic 24 when the mobile device is switched on and sometimes during run-time. The handset provider may instruct the IC manufacturer to program the root key 22 and the security element 23 such that software images provided by the handset provider can execute on the IC 11. The handset provider may also instruct the IC manufacturer to program the security logic 24 to store

instructions for controlling access to the software images and customer specific code in the ROM 20 based on the root key 22 and the security element 23.

In more detail, the manufacturer of the ICs may sell ICs 11 to a plurality of handset providers or handset operators. Each handset provider or operator may encrypt or sign their software with their own keys to prevent their software from being used and modified by people not entitled to use and modify the software. The root key 22 stored in the IC corresponds to the signature of a key certificate comprising the key used to sign the software. The root key 22 ensures that software signed with one or more specific keys can be run on the computer. The IC 11 is programmed by the IC manufacturer to have the root key of the handset provider to which the IC is sold.

According to embodiments of the invention, the IC is also provided with an additional level of security. The secure code section 20b of the ROM code, which comprises the customer specific code, is protected by the security element 23. The security element 23 may be a one-time programmable (OTP) bit, which can be implemented in a variety of ways depending on the IC technology used. For example, the OTP bit may be an efuse. The OTP bit is set by the manufacturer of the IC. The OTP controls the memory map of the device, so that the secure code section 20b of the ROM code is only visible when the bit is set. When access to the code in the secure code section 20b is required, the processor 19 performs a read operation with respect to the secure code section 20b. If the bit 23 is set, this read operation returns the contents of the ROM, which will then be used by the processor (either as code or data). If the bit is not set, then random data, or data corresponding to "no operation" code, can be returned. Alternatively or additionally, a bus error or abort can be issued and the mobile handset can switch off.

Consequently, the handset provider can protect the code in the secure code section 20b of the ROM 20. The code specific to the handset provider is only visible if the bit is set and the bit is only set if the IC is sold to the handset

provider. If a third party purchases the IC, the bit is not set and the code specific to the handset provider cannot be accessed or modified. The OTP therefore provides an extra level of security when a third party attempts to clone a handset provided by the handset provider or when a third party attempts to modify a handset provided by the handset provider.

It should be realised that although it is described that the ROM code in the secure section 20b is only visible when the bit is set, the ROM code could also be visible only when the bit is not set. Additionally, the one time programmable bit can have more than one set value and the ROM code in the secure section may only be visible when the one time programmable bit is set to have one or more specific values.

Figures 4a and 4b illustrate how memory is accessed when the security element 23 is set and when it is not set. With reference to Figure 4a, if the handset provider buys an IC 11 from the IC manufacturer, the manufacturer programs the IC with the root key 22 of the handset provider and sets the OTP bit 23 to make the secure code section 20b of the ROM code visible. The software image, once it has been verified that it is signed with a key associated with the root key of the IC, can then access all required functions in both the generic code section 20a and the secure code section 20b of the ROM 20.

A third party can also buy an IC, programmed with the third party's root key, from the IC manufacturer, mount it in their own handset, which has been designed to look like the handset of a handset provider, and download an illegal copy of the software image of the handset provider. The third party can then easily re-sign the illegal copy of the software image with a key related to its own root key 22 to allow the IC to access and modify the software of the handset provider. In conventional phones, since all the ROM code is available on the IC, the cloned handset would then be able to execute all the functions of the software image of the handset provider and operate like a handset sold by the handset provider. However, with reference to Figure 4b, the IC manufacturer

has set the OTP 23 to hide the ROM code specific to the handset provider and only the software calling generic functions in the ROM code can run properly. Consequently, the cloned handset does not run like the handsets provided by the handset provider.

In another scenario, a third party may buy a handset from the handset provider, replace the IC 11 comprising the root key 22 of the handset provider with an IC 11 bought directly from the IC manufacturer and comprising a root key 22 of the third party. In a conventional device, it would then be able to modify the software image of the handset provider. For example, it would be able to circumvent SIM lock and DRM protection mechanisms by overwriting the SIM lock and DRM protection mechanism code in a copy of the software with "no operation" instructions and then re-sign the software image with its own root key 22. However, with reference to Figure 4b, the IC manufacturer has set the OTP 23 to hide the ROM code specific to the handset provider and only the software calling generic functions in the ROM code can run properly. For the handset to be fully functional, the third party would have to make extensive modifications to the software image. The increase in work required would reduce the business value of copying the software of the handset provider.

For example, to make the handset operational, the third party would have to write his own code to implement the functionality in the secure section 20b of the ROM code to which access is denied. The new code would typically form part of the secure kernel code and would have to be run in the on-chip RAM 21. However, the on-chip RAM 21 only provides limited memory space. Typically, since a larger RAM means larger manufacturing costs, the size of the RAM 21 is chosen to be just large enough to allow the secure kernel code in the external memory to be run properly. Fitting the extra code for implementing the functionality in the secure code section 20b of the ROM code into this limited memory space is not straightforward. In a handset sold by the handset provider, the code stored in the secure code section 20b of the ROM is run in the ROM 20 and the secure kernel code stored in the external memory 16 is run in the RAM

21. However, for the third party, both the third party's code corresponding to the code stored in the secure code section 20b and the secure kernel code must be run in the limited memory space available in the RAM 21. The difficulties involved in fitting the extra code into the RAM 21 may deter an attacker from trying to use the software of the handset provider.

A process for executing software will now be described in more detail with respect to Figure 5. Instructions for performing at least some of the steps may be stored in the security logic 24. Instructions are received to execute the software image residing in the external flash memory at step 5.1. Step 5.1 may be triggered by powering the handset. Before executing the software, the processor 19 checks that the handset is authorised to execute the software. At step 5.2, the processor 19 checks whether a key in the key certificate associated with the root key matches the key used to sign the software image. If the software image is stored in flash memory in the external memory 16, the check can either be performed in the flash memory or the code can first be copied to RAM and checked while in the RAM. If the code is secure kernel code, the check is performed after the secure kernel code has been copied to the on-chip RAM 21. If the key in the certificate associated with the root key 22 does not match the key used to sign the software image, an error function is triggered at step 5.3. However, if there is a match, the code starts executing, the process proceeds to step 5.4 and a first function specified by a program of the software image is called in the ROM code 20.

When calling a function, the processor performs a read operation of the memory address specified in the ROM 20. If the memory address is in the generic code section 20a ('yes' at step 5.5), the read operation returns the contents of the ROM at the memory address at step 5.6 for use by the processor 19.

It is subsequently checked whether the program needs to call additional functions in the ROM 20 at step 5.7 and, if there are additional functions to call, the next function is called at step 5.8.

If the memory address is in the secure code section 20b ('no' at step 5.5) and the OTP bit is set for this section ('yes' at step 5.9), the read operation also returns the ROM code. When there are no more functions to call, the process ends at step 5.10 and the handset is ready to be used.

In contrast, if the memory address is in the secure code section 20b ('no' at step 5.5) and the OTP 23 is not set so that the secure code section 20b is not visible ('no' at step 5.9), the read operation returns an error at step 5.3. The error function triggered by the secure code section not being accessible may not be the same as the error function triggered by the software image not being signed with the right key. If the software image calls a function in the secure section 20b and the OTP is not set, the read operation may return random data or data corresponding to "no operation" instructions. The processor may then restart the mobile communication device or ensure in a suitable way that the mobile device is unusable.

After the software has been checked at start-up as described with respect to Figure 5, the process of comparing the signature of the software image with a key associated with the root key 22 and calling code in the secure code section 20b of the ROM can be repeated occasionally, while the handset is operational, in order to provide extra security.

It will be appreciated that many modifications may be made to the embodiments described above. Although the ROM code has been described to be divided into two parts, it should be understood that it can be divided into more than two parts and a single security element can control more than one section of the ROM code or the IC can comprise one security element for each secure code section. Moreover, although the security logic 24 is shown in Figure 3 to be separate from the ROM 20, the instructions for controlling access to the software image and the secure code section 20b of the ROM code could also be stored in the ROM 20 of the IC. Alternatively or additionally, at least some of

the instructions could be stored in the external memory 16. Furthermore, although the above described embodiment of the invention includes both a security element and a root key, it should be understood that the IC may not include a root key. Additionally, although an embodiment of the invention has been described with respect to a mobile terminal in the form of a mobile telephone handset, it should further be realised that the security mechanism provided by the security element 23 could of course be used in any type of electronic apparatus.

It should be realised that the foregoing examples should not be construed as limiting. Other variations and modifications will be apparent to persons skilled in the art upon reading the present application. Such variations and modifications extend to features already known in the field, which are suitable for replacing the features described herein, and all functionally equivalent features thereof. Moreover, the disclosure of the present application should be understood to include any novel features or any novel combination of features either explicitly or implicitly disclosed herein or any generalisation thereof and during the prosecution of the present application or of any application derived therefrom, new claims may be formulated to cover any such features and/or combination of such features.

Claims

1. An apparatus comprising:

a memory having at least two sections;

a security element associated with at least one of said at least two sections; and

a processor configured to control access to the at least one of the at least two sections of the memory in dependence on a value of the security element.

2. An apparatus according to claim 1, wherein the security element is a permanently programmed memory element

3. An apparatus according to claim 1 or 2, wherein the processor is configured to control a memory map to render the at least one section visible when the security element has a predetermined value.

4. An apparatus according to claim 1, 2 or 3, wherein the processor is further operable to run a computer program and said memory is configured to store secure code for calling by said program.

5. An apparatus according to claim 4 further storing information associated with a key, the processor being operable to only run said computer program if it has been signed with said key.

6. An apparatus according to any one of the preceding claims, wherein said memory is a read-only-memory.

7. An apparatus according to any one of the preceding claims, wherein the security element is a one time programmable bit.

8. An integrated circuit comprising the apparatus according to any one of claims 1 to 7.

9. A mobile terminal comprising the apparatus according to any one of claims 1 to 7.

10. A mobile terminal according to claim 9, wherein the security element is programmed in dependence on the manufacturer of the mobile terminal.

11. A method comprising:

determining a value of a security element associated with a section of a memory having at least two sections, the memory storing code for calling by a computer program; and

controlling access to said section of said memory in dependence on said value.

12. A method according to claim 11, wherein the security element is a permanently programmed memory element

13. A method according to claim 11 or 12, wherein controlling access comprises controlling a memory map to only make said section visible to the program when the security element has a predetermined value.

14. A method according to claim 11, 12 or 13, further comprising

running said program only if said program has been signed with a key matching a key indicated by stored information.

15. A method according to any one of claims 11 to 14, wherein said security element is a one-time programmable bit.

16. A method according to any one of claims 11 to 15 wherein the memory is a read only memory.

17. A method according to any one of claims 11 to 16, wherein the memory and the security element are provided in an integrated circuit.

18. A method according to claim 17, wherein the security element is programmed in dependence on a provider of a device comprising the integrated circuit.

19. A computer program comprising instructions that when executed by a processor causes the processor to execute the method of any one of claims 11 to 18.

20. An integrated circuit comprising:

read only memory code;

a permanently programmed memory element associated with the read only memory code, and

security logic to control access to the read-only memory code in dependence on the value of the permanently programmed memory element.

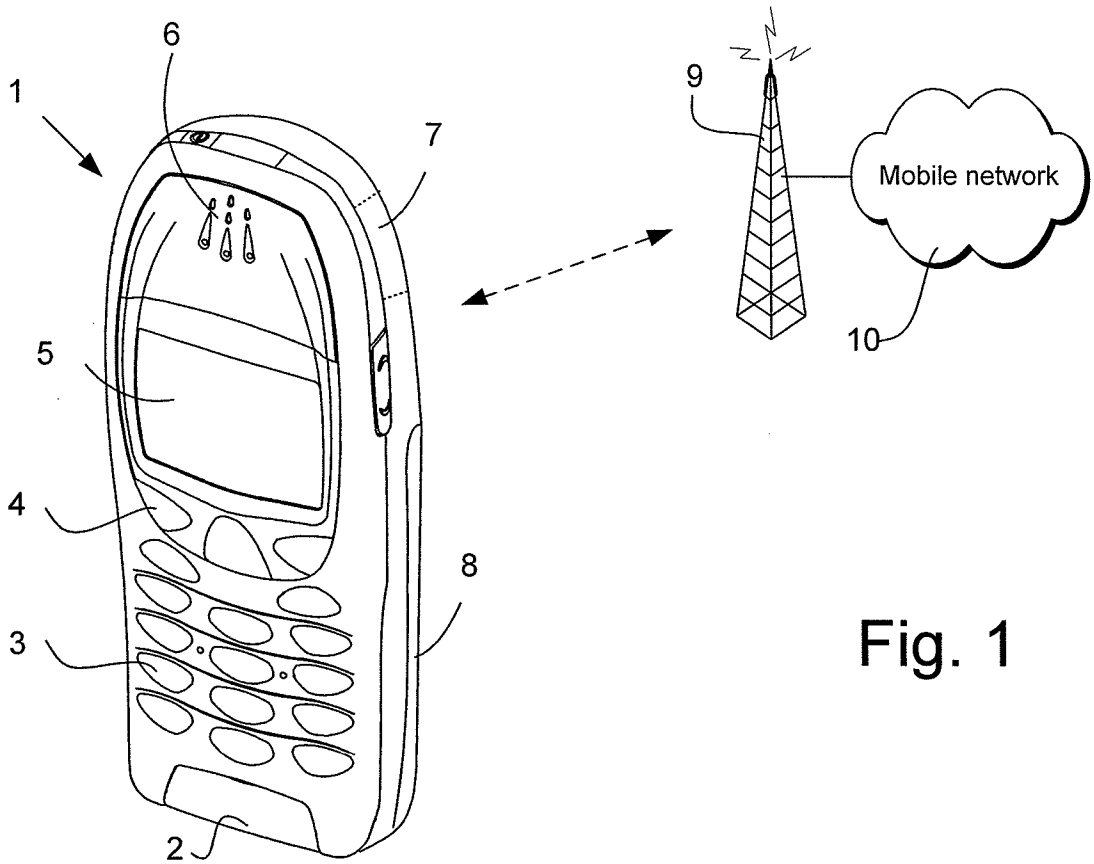

1
6
7
9
Mobile network
10
5
4
8
3
2

Fig. 1

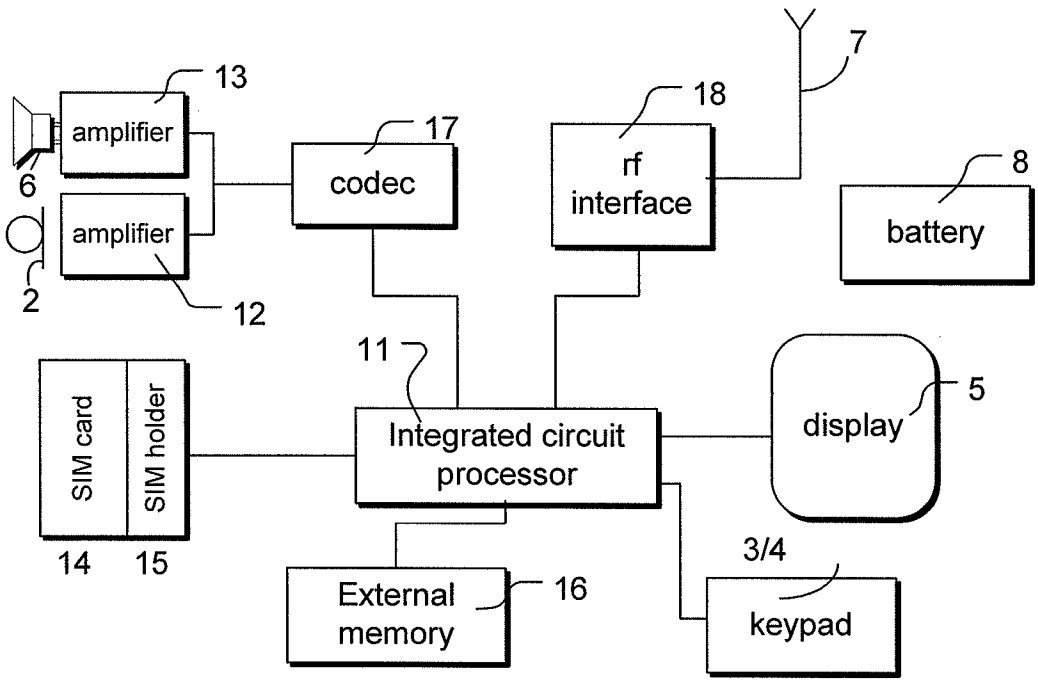

13
amplifier
6
amplifier
2
12
codec
17
18
rf interface
7
8
battery
11
SIM card
SIM holder
14
15
Integrated circuit processor
display
5
3/4
External memory
16
keypad

Fig. 2

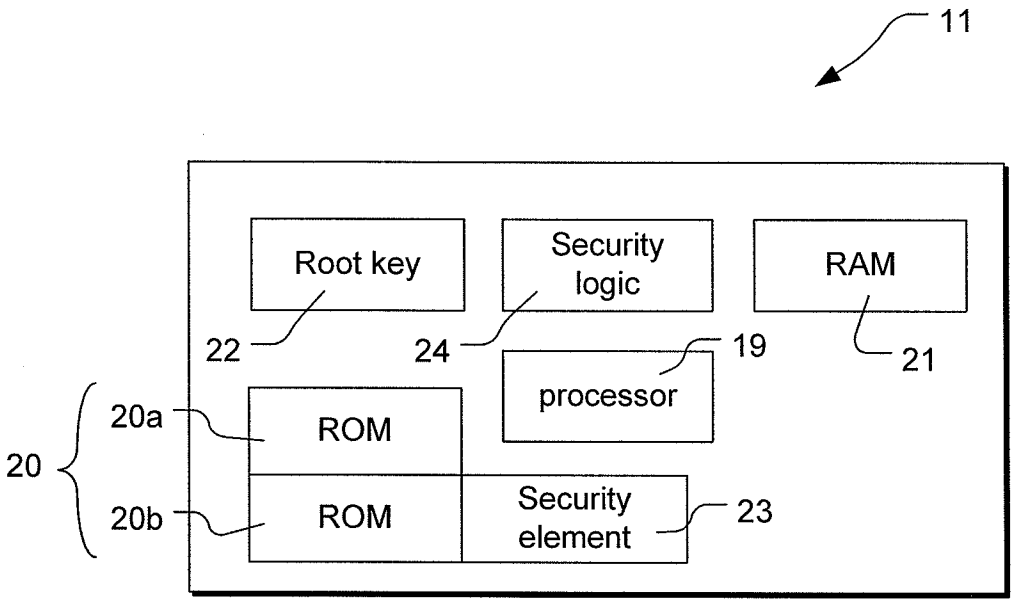


Fig. 3

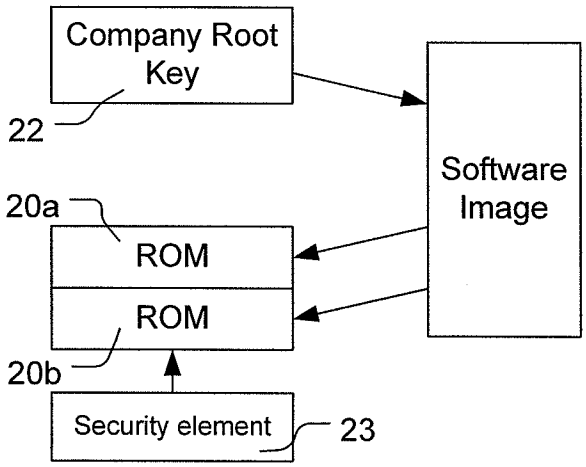


Fig. 4a

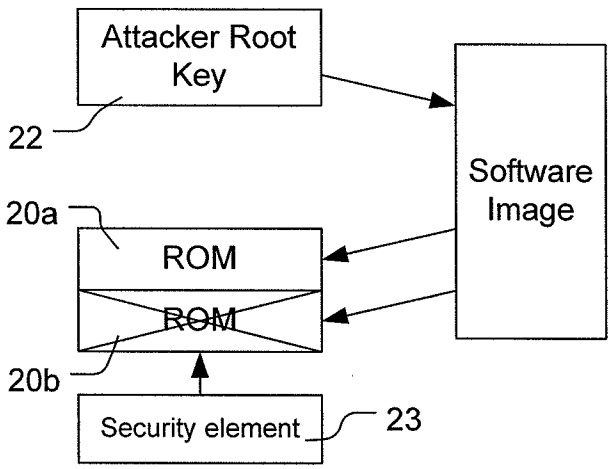
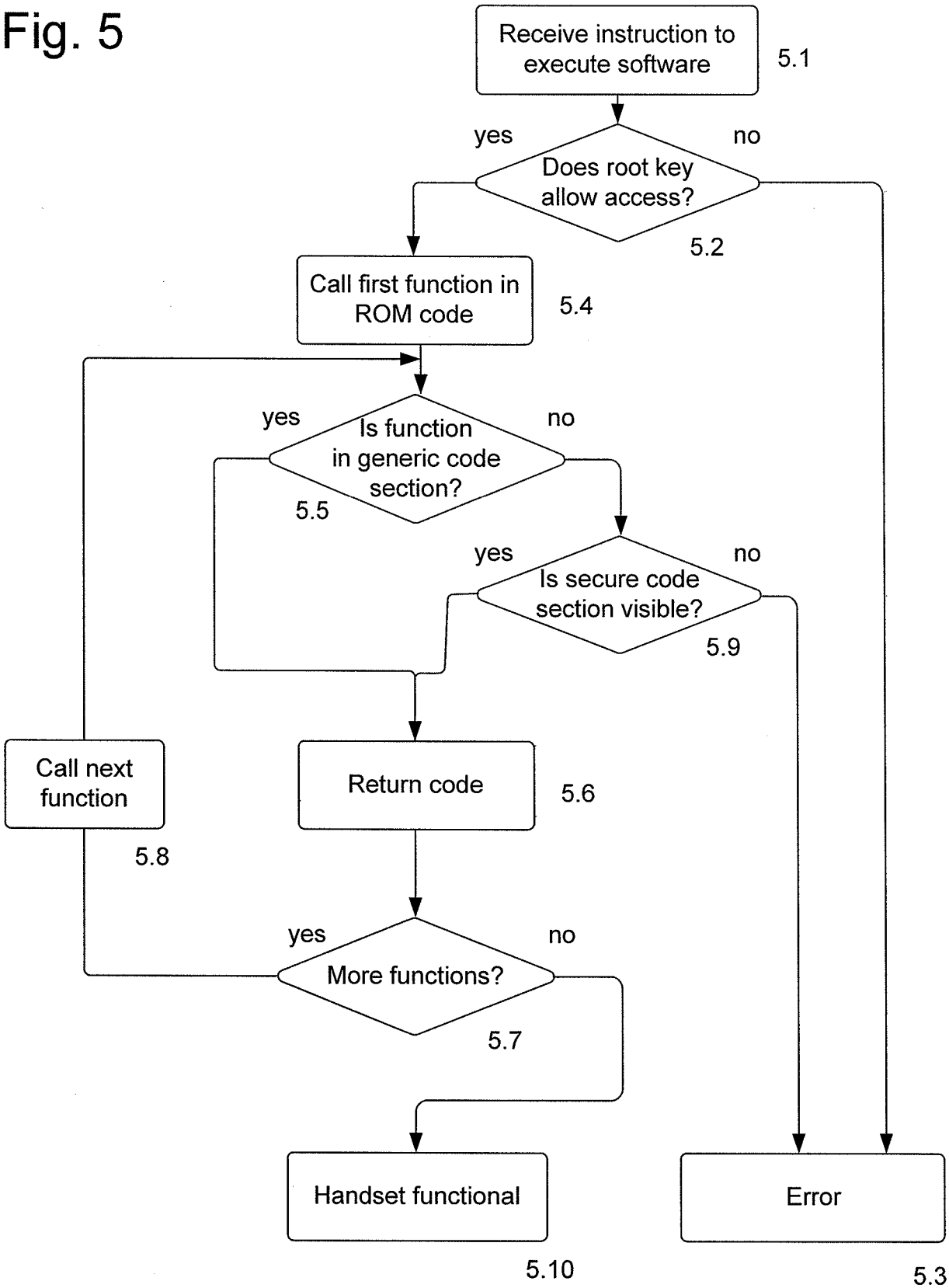


Fig. 4b

Fig. 5


Receive instruction to execute software
5.1
yes
no
Does root key allow access?
5.2
Call first function in ROM code
5.4
yes
no
Is function in generic code section?
5.5
yes
no
Is secure code section visible?
5.9
Call next function
5.8
Return code
5.6
yes
no
More functions?
5.7
Handset functional
5.10
Error
5.3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/063491

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/22

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 638 031 A (MICROSOFT CORP [US]) 22 March 2006 (2006-03-22) abstract paragraphs [0006] - [0018], [0031] - [0051] -----	1-20
X	RANKL W, EFFING W: "Handbu" 2002, HANSER VERLAG , MÜNCHEN , XP002533800 page 545, paragraph 4 - page 547, paragraph 1 -----	1,2,6-8, 10-13, 15,17,20
A	US 6 005 942 A (CHAN ALFRED [US] ET AL) 21 December 1999 (1999-12-21) column 1, line 32 - column 7, line 40 -----	1-20
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] 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 document 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
29 June 2009	15/07/2009

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/063491

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/044231 A (SANDISK IL LTD [IL]; CANYS JAVIER [ES]; MARDIKS EITAN [IL] SANDISK IL) 17 April 2008 (2008-04-17) page 4, line 1 - page 7, line 12	1-20
A	RANKL ET AL: "OPEN PLATFORM" HANDBUCH DER CHIPKARTEN, XX, XX, 1 January 2002 (2002-01-01), pages 295-329, XP002461435 the whole document	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/063491

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1638031 A	22-03-2006	CN 1740941 A	01-03-2006
		JP 2006065847 A	09-03-2006
		US 2006047958 A1	02-03-2006
US 6005942 A	21-12-1999	NONE	
WO 2008044231 A	17-04-2008	US 2008086614 A1	10-04-2008