



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
28.03.2012 Bulletin 2012/13

(51) Int Cl.:
G07C 9/00 (2006.01)

(21) Application number: **10178684.6**

(22) Date of filing: **23.09.2010**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
BA ME RS

• **Fyke, Steven Henry**
Waterloo Ontario N2L 3W8 (CA)

(74) Representative: **Roberts, Gwilym Vaughan et al**
Kilburn & Strode LLP
20 Red Lion Street
London WC1R 4PJ (GB)

(71) Applicant: **Research In Motion Limited**
Waterloo, ON N2L 3W8 (CA)

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

(72) Inventors:
• **Griffin, Jason Tyler**
Waterloo Ontario N2L 3W8 (CA)

(54) **Security system providing temporary personnel access based upon near-field communication and related methods**

(57) A security system may include a plurality of electronic devices, each having a unique identification (ID) associated therewith and configured to generate a temporary security code based upon the unique ID. The system may further include at least one mobile wireless communications device including a first Near-Field Communication (NFC) circuit, and a mobile controller configured to receive the temporary security code from a given electronic device from among the plurality of electronic de-

vices. The system may also include an access control device associated with a personnel access position and including a second NFC circuit and a security controller. The security controller may be configured to receive the temporary security code from the first NFC circuit via NFC communications, selectively grant personnel access based upon the received temporary security code, and determine the unique ID associated with the given electronic device.

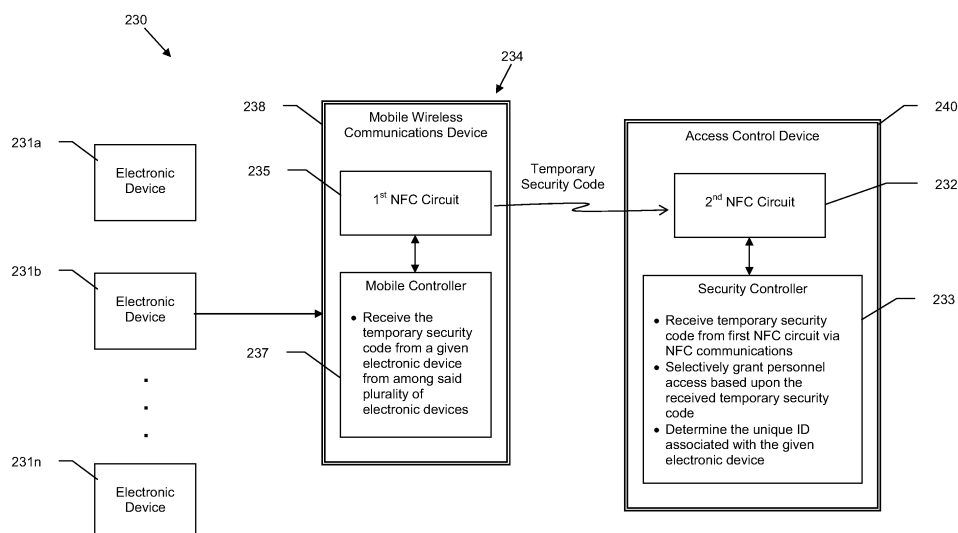


FIG. 7

Description

Technical Field

[0001] This application relates to the field of communications, and more particularly, to electronic devices and related methods that use near-field communication (NFC).

Background

[0002] Mobile communication systems continue to grow in popularity and have become an integral part of both personal and business communications. Various mobile devices now incorporate Personal Digital Assistant (PDA) features such as calendars, address books, task lists, calculators, memo and writing programs, media players, games, etc. These multi-function devices usually allow electronic mail (email) messages to be sent and received wirelessly, as well as access the Internet via a cellular network and/or a wireless local area network (WLAN), for example.

[0003] Some mobile devices incorporate contactless card technology and/or near field communication (NFC) chips. NFC technology may be used for contactless short-range communications using magnetic field induction to enable communication between electronic devices, including mobile wireless communications devices. These short-range communications include payment and ticketing, electronic keys, identification, device set-up service and similar information sharing. This short-range high frequency wireless communications technology exchanges data between devices over a short distance, such as only a few centimeters.

Brief Description of the Drawings

[0004] FIG. 1 is a schematic block diagram of a security system in accordance with one example embodiment.

[0005] FIG. 2 is a schematic block diagram of the mobile wireless communications device of the system of FIG. 1 shown in greater detail.

[0006] FIG. 3 is a schematic block diagram in which a plurality of mobile wireless communications devices are shown for use with the security system of FIG. 1.

[0007] FIG. 4 is a schematic block diagram of an alternative embodiment of the mobile wireless communications devices of FIG. 3.

[0008] FIGS. 5 and 6 are flow diagrams illustrating method aspects associated with the system of FIG. 1 and mobile wireless communications devices of FIGS. 2 through 4.

[0009] FIG. 7 is a schematic block diagram of another security system in accordance with an example embodiment.

[0010] FIG. 8 is a schematic block diagram of an alternative embodiment of the system of FIG. 7.

[0011] FIGS. 9 and 10 are flow diagrams illustrating

method aspects associated with the systems of FIGS. 7 and 8.

[0012] FIG. 11 is a schematic block diagram illustrating an example mobile wireless device components that may be used with the mobile wireless communications devices of the example embodiments.

Detailed Description

[0013] The present description is made with reference to the accompanying drawings, in which example embodiments are shown. However, many different embodiments may be used, and thus the description should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete. Like numbers refer to like elements throughout, and prime notation is used to indicate similar elements or steps in alternative embodiments.

[0014] Generally speaking, a security system is disclosed herein, the security system may include a plurality of electronic devices, each having a unique identification (ID) associated therewith and configured to generate a temporary security code based upon the unique ID. The system may further include at least one mobile wireless communications device comprising a first Near-Field Communication (NFC) sensor, and a mobile controller configured to receive the temporary security code from a given electronic device from among the plurality of electronic devices. The system may also include an access control device associated with a personnel access position and comprising a second NFC sensor configured to receive the temporary security code from the first NFC sensor via NFC communications and a security controller. The security controller may be, configured to selectively grant personnel access based upon the received temporary security code, and determine the unique ID associated with the given electronic device. Thus, the system may conveniently be used to provide personnel access at a secured location from a mobile wireless communications device with NFC communications, and while allowing for tracking of the electronic device which provided the temporary security code.

[0015] The security controller may be configured to further selectively grant personnel access also based upon the determined unique ID. In addition, the security controller may also be configured to update a log of the determined unique ID.

[0016] In some embodiments, each of the plurality of electronic devices may be further configured to generate an event notification, and to communicate the temporary security code to the at least one mobile wireless communications device along with the event notification. Furthermore, the event notification may have a scheduled event time associated therewith, and the security controller may be configured to selectively grant personnel access further based upon the scheduled event time.

[0017] By way of example, the temporary security code

may comprise a single-use security code. In some embodiments, at least one of the plurality of electronic devices may also comprise a mobile wireless communications device. Furthermore, each of the plurality of electronic devices may further comprise a third NFC sensor, and the mobile controller may be configured to receive the temporary security code via the third NFC sensor. In addition, the at least one mobile wireless communications device may further include a wireless transceiver coupled to the mobile controller and configured to receive the temporary security code from the given electronic device. By way of example, the wireless transceiver may comprise a cellular transceiver, a Wireless Local Area Network (WLAN) transceiver, etc.

[0018] A related access control device, such as the one described briefly above, and security method are also provided. The method may include generating a temporary security code at a given electronic device based upon the unique ID associated therewith, receiving the temporary security code at the at least one mobile wireless communications device from the given electronic device, and receiving the temporary security code at the access control device from the first NFC sensor via NFC communications. The method may further include selectively granting personnel access via the access control device based upon the received temporary security code, and determining the unique ID associated with the given electronic device at the access control device.

[0019] A related computer-readable medium is also provided having computer-executable instructions for causing an access control device to perform steps including receiving the temporary security code from the first NFC sensor via NFC communications, selectively granting personnel access based upon the received temporary security code, and determining the unique ID associated with the given electronic device.

[0020] Referring initially to FIGS. 1 and 2, a security system 30 is first described. By way of background, NFC is a short-range wireless communications technology in which NFC-enabled devices are "swiped," "bumped" or otherwise moved in close proximity to communicate. In one non-limiting example implementation, NFC may operate at 13.56 MHz and with an effective range of about 10cm, but other suitable versions of near-field communication which may have different operating frequencies, effective ranges, etc., for example, may also be used.

[0021] The system 30 illustratively includes an access control device associated with a personnel access position. In the illustrated example, the personnel access position is at a security door 31 which is locked to prevent unauthorized access to a particular area. In other embodiments, however, the personnel access position may correspond to a security gate or turnstile, or to a secure object such as a safe, locker, or a vehicle, for example. The access control device illustratively includes a first NFC sensor (e.g., an NFC transceiver) 32, and a controller 33, which will be referred to as a security controller herein for clarity of reference. These components may

be co-located or separately located in different embodiments. For example, the NFC sensor 32 may be located at the personnel access position, and the security controller 33 may be co-located therewith or remotely connected to the NFC sensor, such as over a local area network (LAN), wireless communications link, the Internet, etc.

[0022] The security system 30 also illustratively includes a mobile wireless communications device 34 (also referred to as a "mobile device" herein) which comprises a second NFC sensor 35, a wireless receiver or transceiver 36 which communicates via a wireless communications network 39, and a controller 37, which will be referred to as the "mobile controller" herein for clarity of reference since it is located in the mobile device. By way of example, the wireless transceiver 36 may comprise a cellular transceiver, a Wireless Local Area Network (WLAN) transceiver, etc. The mobile device 34 components may be carried by a portable housing 38. By way of example, the security controller 33 and the mobile controller 37 may be implemented using a combination of hardware (e.g., microprocessor, etc.) and non-transitory computer readable medium components including computer-readable instructions for causing the various operations discussed herein to be performed. Example mobile devices may include portable or personal media players (e.g., MP3 players, video players, etc.), remote controls (e.g., television or stereo remotes, etc.), portable gaming devices, portable or mobile telephones, smartphones, etc.

[0023] In its current implementation, NFC is a short range variant of radio-frequency identification (RFID), typically operating at approximately 13.56 MHz. NFC technology allows a wireless connection to be established between a mobile device that has an embedded NFC chipset and an NFC reader terminal (e.g., 14443A/B, Felica, ISO 15693) at a range of about 10cm, so that the devices are "swiped", "bumped", "tapped", or otherwise moved relative to one another to be in close proximity to communicate. NFC is a standardized technology that may be used in various applications such as mobile banking, ticketing, secure physical access, etc. However, it should be noted that, as used herein, "NFC" includes other similar short-range wireless communication formats that may have a different operating frequency, effective range, etc. The first and second NFC sensors 32, 35 may be passive tags or active readers depending upon the given implementation.

[0024] Referring additionally to FIG. 5, operation of the security system 30 is now further described. Beginning at Block 50, the mobile controller 37 is configured to communicate a security code, which may be valid or invalid, via the second NFC sensor 35 to the first NFC sensor 32 based upon proximity therewith (i.e., when they are within NFC communication range), at Block 51. By way of example, the security code may comprise a series of alphanumeric characters, and in some embodiments the security code may be encrypted to provided enhanced

security. The security controller **33** is configured to selectively grant personnel access based upon receiving a valid security code from the first NFC sensor **32**, at Blocks **52** and **53**, which illustratively concludes the method shown in FIG. 5 at Block **54**. However, if the mobile controller **37** instead provides an invalid security code, then the security controller **33** denies personnel access and generates at least one access denial electronic message, at Block **55**. The mobile controller **37** is configured to receive the at least one denial electronic message (e.g., electronic mail (email) message, Short Message Service (SMS) message, etc.) from the security controller **36** via the second NFC sensor **35** or the wireless transceiver **36** based upon communicating the invalid security code, at Block **56**.

[0025] In this way, the person attempting to obtain access may advantageously be informed as to the reason that access was denied. For example, a particular security code may only be valid during certain times of the day, or certain days of the week, but invalid outside of those times. Another example is that a security code may be valid for a particular access point (e.g., the front of a building), but not other access points (e.g., a back entrance to the building). The denial message may also inform the user who the appropriate contact is to obtain access.

[0026] Turning now additionally to FIGS. 3 and 4, in some embodiments one or more mobile devices **134a**, **134b** may be used. It should be noted that in the illustrated embodiments the components which are similar to those already described above with reference to FIG. 2 are indicated by increments of one-hundred (e.g., the wireless transceiver **36** is similar to the wireless transceivers **136a**, **136b**, etc.) for convenience of reference. Not only does the use of multiple mobile devices **134a**, **134b** allow them to individually communicate with the access control device to gain personnel access, but this may also allow one mobile device to exchange a security code with the other device. That is, one of the mobile devices **134a** may advantageously receive a valid security code from the other mobile device **134b**.

[0027] Thus, for example, the mobile device **134b** may have an authorized valid security code assigned thereto (such as for an employee, etc.), and the mobile controller **137b** may provide a temporary or single-use (i.e., "one-time") code to the other mobile device **134a** (see Block **51'**, FIG. 6), such as to allow guest or visitor access, for example. In one use case, the mobile device **134b** may provide a valid security code to the mobile device **134a** for an event by tapping the devices together, or sending an email or SMS message with the appropriate information. That is, in some embodiments the mobile controller **137a** may be configured to receive the valid security code via the second NFC sensor **135a**, as seen in FIG. 3. In other embodiments, the mobile controller **137a'** may be configured to receive the valid security code via the wireless transceiver **136a** and the wireless communications network **139'**, as seen in FIG. 4.

[0028] Referring additionally to FIG. 6, in some embodiments it may be desirable to grant personnel access based not only on provision of a valid security code, but also based upon additional authentication data from the wireless transceiver **36**, such as biometric data (e.g., fingerprint, iris, retina, etc.), a password or personal identification number (PIN), etc., at Block **57'**. In one example implementation, when the mobile device **34** is swiped or bumped to begin NFC communication, a prompt may be provided (such as on a display of the mobile device) to authenticate the mobile device, and the mobile controller **37** may communicate with the security controller **33** via the wireless transceiver **36** to thereby provide access upon receiving the correct additional authentication information.

[0029] Turning now to FIGS. 7 through 10, in accordance with another advantageous embodiment a security system **230** illustratively includes a plurality of electronic devices **231a-231n**, each having a unique identification (ID) associated therewith. By way of example, the electronic devices **231a-231n** may comprise computers (e.g., PCs, Macs, etc.), mobile devices such as those noted above, etc. Beginning at Blocks **250**, **250'**, each electronic device **231a-231n** is configured to generate a temporary security code based upon the unique ID, at Blocks **251**, **251'**. By way of example, the unique ID may be a unique alphanumeric code associated with the electronic device, such as an Internet Protocol (IP) address, a Uniform Resource Locator (URL) address, an International Mobile Equipment Identity (IMEI) number, a mobile device PIN, a phone number, etc. In other embodiments, the unique ID may instead be associated with a user to which the given electronic device **231** is assigned, such as an employee ID or PIN, etc.

[0030] The temporary security code may be a series of alphanumeric characters as described above, and may be used to provide temporary (e.g., single-use) access to a secure area, such as a building, office, storage area or locker, etc. The temporary security code may be generated using the unique ID as a key seed, such as with a cryptographic algorithm, or may instead be incorporated within or included as part of the temporary security code, for example. The temporary security code provides the requisite information for an access control device **240** to grant personnel access.

[0031] The system **230** further illustratively includes one or more mobile devices **234** comprising a first NFC sensor **235**, and a mobile controller **237** configured to receive the temporary security code from a given electronic device, namely the electronic device **231b** in FIG. 7, from among the plurality of electronic devices **231a-231n**, at Blocks **252**, **252'**. The temporary security code may be communicated to the mobile controller **237** via a third NFC sensor **241'** in an NFC-enabled electronic device **231a'**, or via a wireless communications network **239'** from an electronic device such as a mobile device **231b'** comprising a wireless transceiver (e.g., cellular, WLAN, WiMAX, etc.), as seen in FIG. 8.

[0032] The access control device **240** is associated with a personnel access position, as noted above, and it illustratively includes a second NFC sensor **232** and a security controller **233**. The security controller **233** is configured to receive the temporary security code from the first NFC sensor **235** via NFC communications, at Blocks **253**, **253'**, selectively grant personnel access based upon the received temporary security code, at Block **254**, and determine the unique ID associated with the given electronic device, at Block **255**, thus concluding the method illustratively shown in FIG. 9. This advantageously allows one user to grant temporary access to another, such as to enter a building for a meeting, etc., while also allowing the security controller **233** to track the user who granted the temporary access. To this end, the access control device **240'** shown in FIG. 8 further illustratively includes a security database **242'** coupled to the security controller **233'** and configured to update or maintain a log of unique IDs used for granting temporary access. The log may also include an indication of the mobile device **234'** to which access was granted, date/time of access, etc.

[0033] The determination as to whether to grant personnel access may be based upon factors other than whether a valid temporary security code is presented to the security controller **233**, at Block **257'** (FIG. 10). For example, the security controller **233** may also be configured to further selectively grant personnel access also based upon the determined unique ID. More particularly, the security controller **233'** may check to see whether the unique ID is valid, at Block **258'**. By way of example, a unique ID may no longer be valid if it corresponds to a user that is no longer an employee or is no longer authorized to grant access. Even though the unique ID may have been issued by an electronic device **231** having a valid unique ID at the time the temporary security code was issued, if the unique ID is no longer valid at the time access by the mobile device **234** is requested, then it may be desirable to exclude the temporary personnel access in some implementations.

[0034] In some embodiments, the temporary security code may be exchanged as part of, or along with, an event notification generated by a given electronic device, which in the embodiment of FIG. 8 is the mobile device **231b'**. For example, a user may issue an event invitation from a PC or Mac computer, such as through Microsoft® Outlook, for example, and invite one or more participants to an event in the user's building at a scheduled event time (i.e., a given date and time). The event invitation may include a temporary security code that allows event attendees to temporarily access the building at the time of, or within a time window of (e.g., 15 minutes prior to the start time), the event. Depending upon the given embodiment, the temporary security code may be included as part of an initial event invitation, or may be provided in response to an acceptance of an event invitation, for example. If the temporary security code or unique ID is not valid, or it is not the scheduled time (or within a window

of the scheduled time), then personnel access may be denied, which concludes the method illustrated in FIG. 10 (Block **256'**). Otherwise, personnel access may be granted, at Block **254'**.

[0035] A related computer-readable medium is also provided having computer-executable instructions for causing the access control device **240** to perform steps including receiving the temporary security code from the first NFC sensor **235** via NFC communications, selectively granting personnel access based upon the received temporary security code, and determining the unique ID associated with the given electronic device (i.e., the device **231b** in FIG. 7). The computer-readable medium may further include computer-executable instructions for performing the additional steps described above.

[0036] Example components of a mobile device **1000** that may be used in accordance with the above-described embodiments are further described below with reference to FIG. 11. The device **1000** illustratively includes a housing **1200**, a keyboard or keypad **1400** and an output device **1600**. The output device shown is a display **1600**, which may comprise a full graphic LCD. Other types of output devices may alternatively be utilized. A processing device **1800** is contained within the housing **1200** and is coupled between the keypad **1400** and the display **1600**. The processing device **1800** controls the operation of the display **1600**, as well as the overall operation of the mobile device **1000**, in response to actuation of keys on the keypad **1400**.

[0037] The housing **1200** may be elongated vertically, or may take on other sizes and shapes (including clam-shell housing structures). The keypad may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

[0038] In addition to the processing device **1800**, other parts of the mobile device **1000** are shown schematically in FIG. 11. These include a communications subsystem **1001**; a short-range communications subsystem **1020**; the keypad **1400** and the display **1600**, along with other input/output devices **1060**, **1080**, **1100** and **1120**; as well as memory devices **1160**, **1180** and various other device subsystems **1201**. The mobile device **1000** may comprise a two-way RF communications device having data and, optionally, voice communications capabilities. In addition, the mobile device **1000** may have the capability to communicate with other computer systems via the Internet.

[0039] Operating system software executed by the processing device **1800** is stored in a persistent store, such as the flash memory **1160**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the random access memory (RAM) **1180**. Communications signals received by the mobile device may also be stored in the RAM **1180**.

[0040] The processing device 1800, in addition to its operating system functions, enables execution of software applications **1300A-1300N** on the device 1000. A predetermined set of applications that control basic device operations, such as data and voice communications **1300A** and **1300B**, may be installed on the device 1000 during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM may be capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application may also be capable of sending and receiving data items via a wireless network 1401. The PIM data items may be seamlessly integrated, synchronized and updated via the wireless network 1401 with corresponding data items stored or associated with a host computer system.

[0041] Communication functions, including data and voice communications, are performed through the communications subsystem 1001, and possibly through the short-range communications subsystem. The communications subsystem 1001 includes a receiver 1500, a transmitter 1520, and one or more antennas 1540 and 1560. In addition, the communications subsystem 1001 also includes a processing module, such as a digital signal processor (DSP) 1580, and local oscillators (LOs) 1601. The specific design and implementation of the communications subsystem **1001** is dependent upon the communications network in which the mobile device **1000** is intended to operate. For example, a mobile device **1000** may include a communications subsystem **1001** designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communications networks, and also designed to operate with any of a variety of voice communications networks, such as AMPS, TDMA, CDMA, WCDMA, PCS, GSM, EDGE, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device **1000**. The mobile device **1000** may also be compliant with other communications standards such as 3GSM, 3GPP, UMTS, 4G, etc.

[0042] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore typically involves use of a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0043] When required network registration or activation procedures have been completed, the mobile device 1000 may send and receive communications signals over the communication network 1401. Signals received from the communications network 1401 by the antenna 1540 are routed to the receiver 1500, which provides for signal amplification, frequency down conversion, filtering, chan-

nel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP 1580 to perform more complex communications functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network **1401** are processed (e.g. modulated and encoded) by the DSP **1580** and are then provided to the transmitter **1520** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **1401** (or networks) via the antenna **1560**.

[0044] In addition to processing communications signals, the DSP **1580** provides for control of the receiver **1500** and the transmitter **1520**. For example, gains applied to communications signals in the receiver **1500** and transmitter **1520** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **1580**.

[0045] In a data communications mode, a received signal, such as a text message or web page download, is processed by the communications subsystem **1001** and is input to the processing device **1800**. The received signal is then further processed by the processing device **1800** for an output to the display 1600, or alternatively to some other auxiliary I/O device **1060**. A device may also be used to compose data items, such as e-mail messages, using the keypad **1400** and/or some other auxiliary I/O device **1060**, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communications network **1401** via the communications subsystem **1001**.

[0046] In a voice communications mode, overall operation of the device is substantially similar to the data communications mode, except that received signals are output to a speaker **1100**, and signals for transmission are generated by a microphone **1120**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device **1000**. In addition, the display 1600 may also be utilized in voice communications mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[0047] The short-range communications subsystem enables communication between the mobile device **1000** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, NFC or a Bluetooth™ communications module to provide for communication with similarly-enabled systems and devices.

[0048] Many modifications and other embodiments will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that various modifications and embodiments are intended to be included within the scope of the ap-

pending claims.

Claims

1. A security system comprising:

a plurality of electronic devices, each having a unique identification (ID) associated therewith and configured to generate a temporary security code based upon the unique ID;
at least one mobile wireless communications device comprising
a first Near-Field Communication (NFC) sensor, and
a first controller configured to receive the temporary security code from a given electronic device from among said plurality of electronic devices; and
an access control device associated with a personnel access position and comprising
a second NFC sensor configured to receive the temporary security code from said first NFC sensor via NFC communications, and
a second controller coupled to said second NFC sensor and configured to
selectively grant personnel access based upon the received temporary security code, and
determine the unique ID associated with the given electronic device.

2. The security system of Claim 1 wherein said second controller is configured to further selectively grant personnel access also based upon the determined unique ID.

3. The security system of Claim 1 wherein said second controller is configured to update a log of the determined unique ID.

4. The security system of Claim 1 wherein each of said plurality of electronic devices is further configured to generate an event notification, and to communicate the temporary security code to said at least one mobile wireless communications device along with the event notification.

5. The security system of Claim 4 wherein the event notification has a scheduled event time associated therewith; and wherein said second controller is configured to selectively grant personnel access further based upon the scheduled event time.

6. The security system of Claim 1 wherein the temporary security code comprises a single-use security code.

7. The security system of Claim 1 wherein at least one

of said plurality of electronic devices also comprises a mobile wireless communications device.

8. The security system of Claim 1 wherein each of said plurality of electronic devices further comprises a third NFC sensor; and wherein said first controller is configured to receive the temporary security code via the third NFC sensor.

9. The security system of Claim 1 wherein said at least one mobile wireless communications device further comprises a wireless receiver coupled to said first controller and configured to receive the temporary security code from said given electronic device.

10. The security system of Claim 9 wherein said wireless receiver comprises a cellular receiver.

11. A security method for a plurality of electronic devices, each having a unique identification (ID) associated therewith, at least one mobile wireless communications device comprising a first Near-Field Communication (NFC) circuit, and an access control device associated with a personnel access position and comprising a second NFC sensor, the method comprising:

generating a temporary security code at a given electronic device based upon the unique ID associated therewith;
receiving the temporary security code at the at least one mobile wireless communications device from the given electronic device;
receiving the temporary security code at the access control device from the first NFC sensor via NFC communications;
selectively granting personnel access via the access control device based upon the received temporary security code; and
determining the unique ID associated with the given electronic device at the access control device.

12. The method of Claim 11 wherein selectively granting further comprises selectively granting personnel access also based upon the determined unique ID.

13. The method of Claim 11 further comprising updating a log of the determined unique ID.

14. The method of Claim 11 wherein each of the plurality of electronic devices is further configured to generate an event notification, and further comprising communicating the temporary security code from the given electronic device to the at least one mobile wireless communications device along with the event notification.

15. The method of Claim 11 wherein the event notification has a scheduled event time associated therewith; and wherein selectively granting further comprises selectively granting personnel access based upon the scheduled event time.

Amended claims in accordance with Rule 137(2) EPC.

1. A security system (230) comprising:

a plurality of electronic devices (231a-231n), each having a unique identification ID associated therewith and configured to generate a temporary security code based upon the unique ID; at least one mobile wireless communications device (234) comprising a first Near-Field Communication NFC sensor (235), and a first controller (237) configured to receive the temporary security code from a given electronic device (231b) from among said plurality of electronic devices; and an access control device (240) associated with a personnel access position and comprising a second NFC sensor (232) configured to receive the temporary security code from said first NFC sensor via NFC communications, and a second controller (233) coupled to said second NFC sensor and configured to selectively grant personnel access based upon the received temporary security code, and determine the unique ID associated with the given electronic device.

2. The security system (230) of Claim 1 wherein said second controller (233) is configured to further selectively grant personnel access also based upon the determined unique ID.

3. The security system (230) of Claim 1 wherein said second controller (233) is configured to update a log of the determined unique ID.

4. The security system (230') of Claim 1 wherein each of said plurality of electronic devices (231a'-231n') is further configured to generate an event notification, and to communicate the temporary security code to said at least one mobile wireless communications device (234') along with the event notification.

5. The security system (230') of Claim 4 wherein the event notification has a scheduled event time associated therewith; and wherein said second controller (233') is configured to selectively grant personnel access further based upon the scheduled event time.

6. The security system (230) of Claim 1 wherein the temporary security code comprises a single-use security code.

7. The security system (230) of Claim 1 wherein at least one of said plurality of electronic devices (231a-231n) also comprises a mobile wireless communications device.

8. The security system (230') of Claim 1 wherein each of said plurality of electronic devices (231a'-231n') further comprises a third NFC sensor (241'); and wherein said first controller (237') is configured to receive the temporary security code via the third NFC sensor.

9. The security system (230') of Claim 1 wherein said at least one mobile wireless communications device (234') further comprises a wireless receiver (236') coupled to said first controller (237') and configured to receive the temporary security code from said given electronic device (231a', 231b').

10. The security system (230') of Claim 9 wherein said wireless receiver (236') comprises a cellular receiver.

11. A security method for a plurality of electronic devices (231a-231n), each having a unique identification (ID) associated therewith, at least one mobile wireless communications device (234) comprising a first Near-Field Communication (NFC) sensor (235), and an access control device (240) associated with a personnel access position and comprising a second NFC sensor (232), the method comprising:

generating a temporary security code at a given electronic device (231b) based upon the unique ID associated therewith;
receiving the temporary security code at the at least one mobile wireless communications device from the given electronic device;
receiving the temporary security code at the access control device from the first NFC sensor via NFC communications;
selectively granting personnel access via the access control device based upon the received temporary security code; and
determining the unique ID associated with the given electronic device at the access control device.

12. The method of Claim 11 wherein selectively granting further comprises selectively granting personnel access also based upon the determined unique ID.

13. The method of Claim 11 further comprising up-

dating a log of the determined unique ID.

14. The method of Claim 11 wherein each of the plurality of electronic devices (231a'-231n') is further configured to generate an event notification, and further comprising communicating the temporary security code from the given electronic device (231a', 231b') to the at least one mobile wireless communications device (234') along with the event notification. 5 10

15. The method of Claim 11 wherein the event notification has a scheduled event time associated therewith; and wherein selectively granting further comprises selectively granting personnel access based upon the scheduled event time. 15 20 25 30 35 40 45 50 55

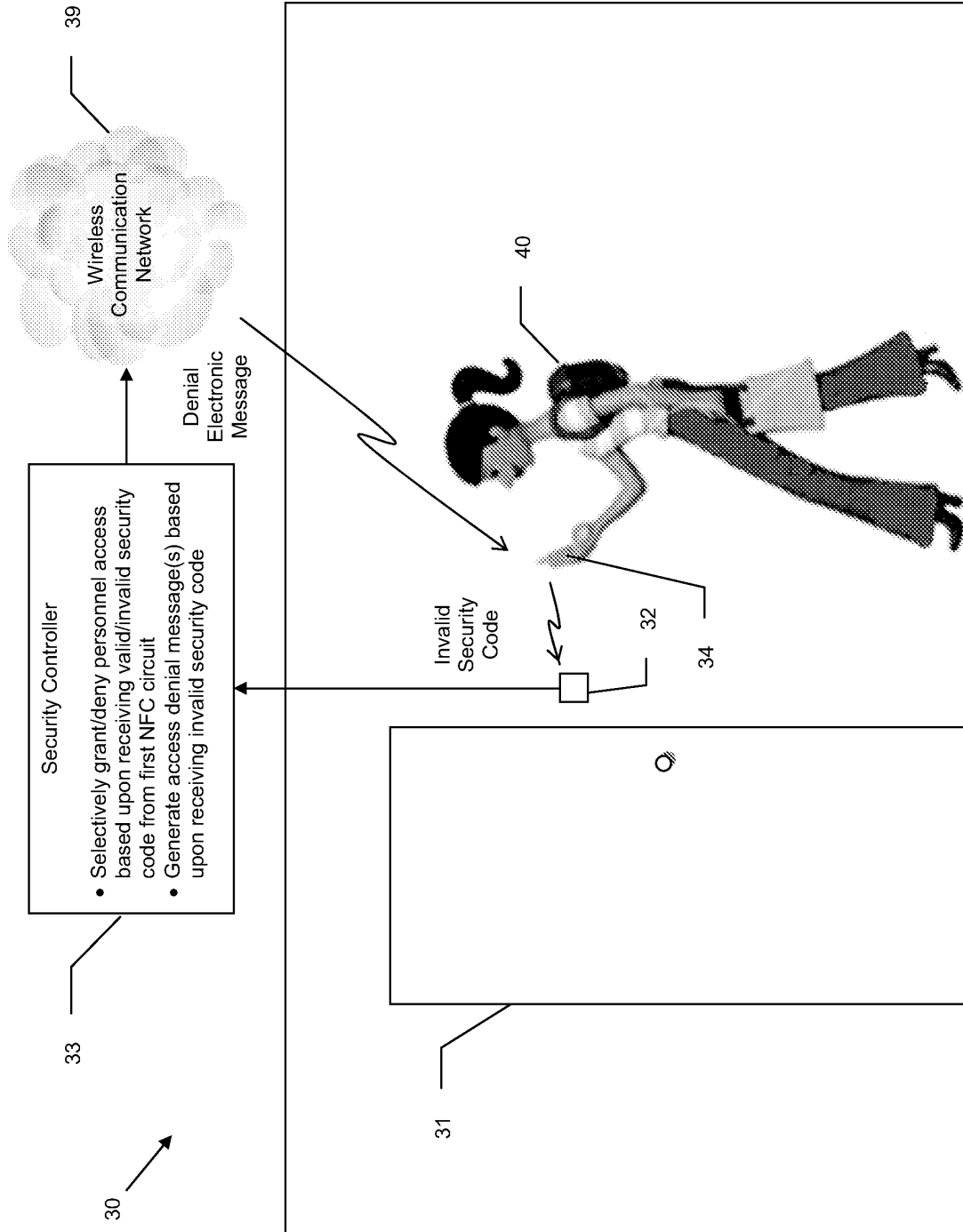


FIG. 1

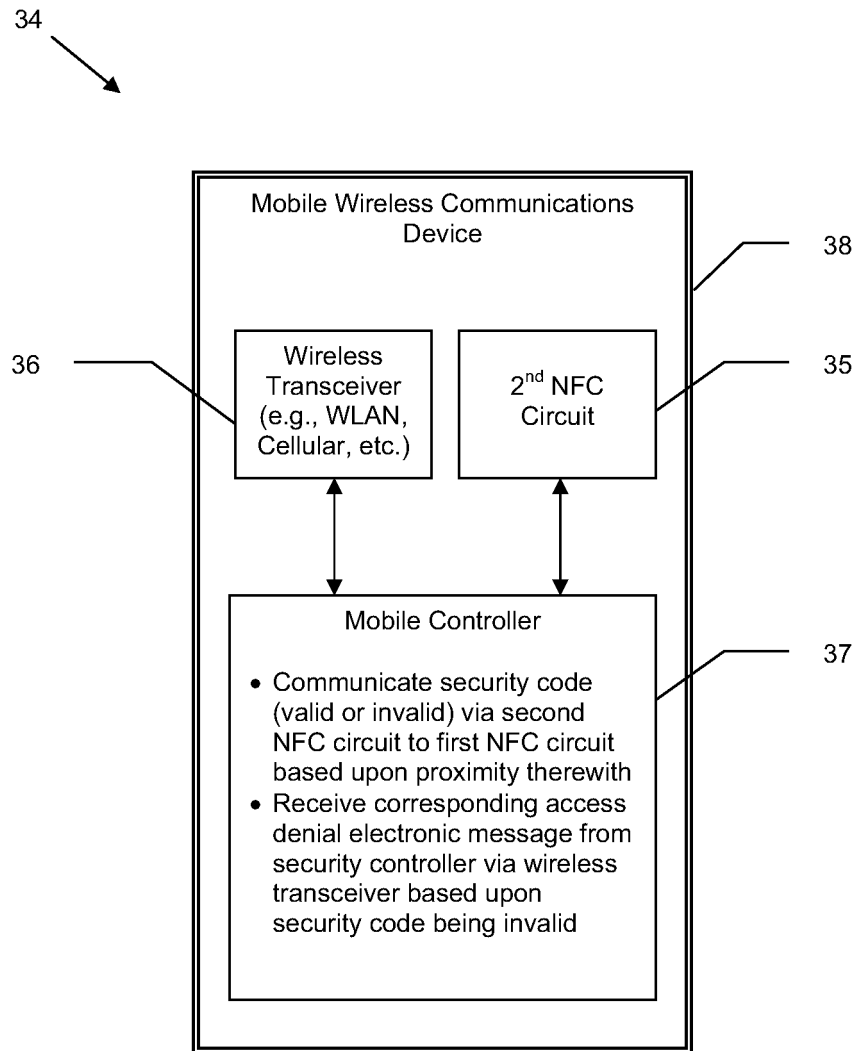


FIG. 2

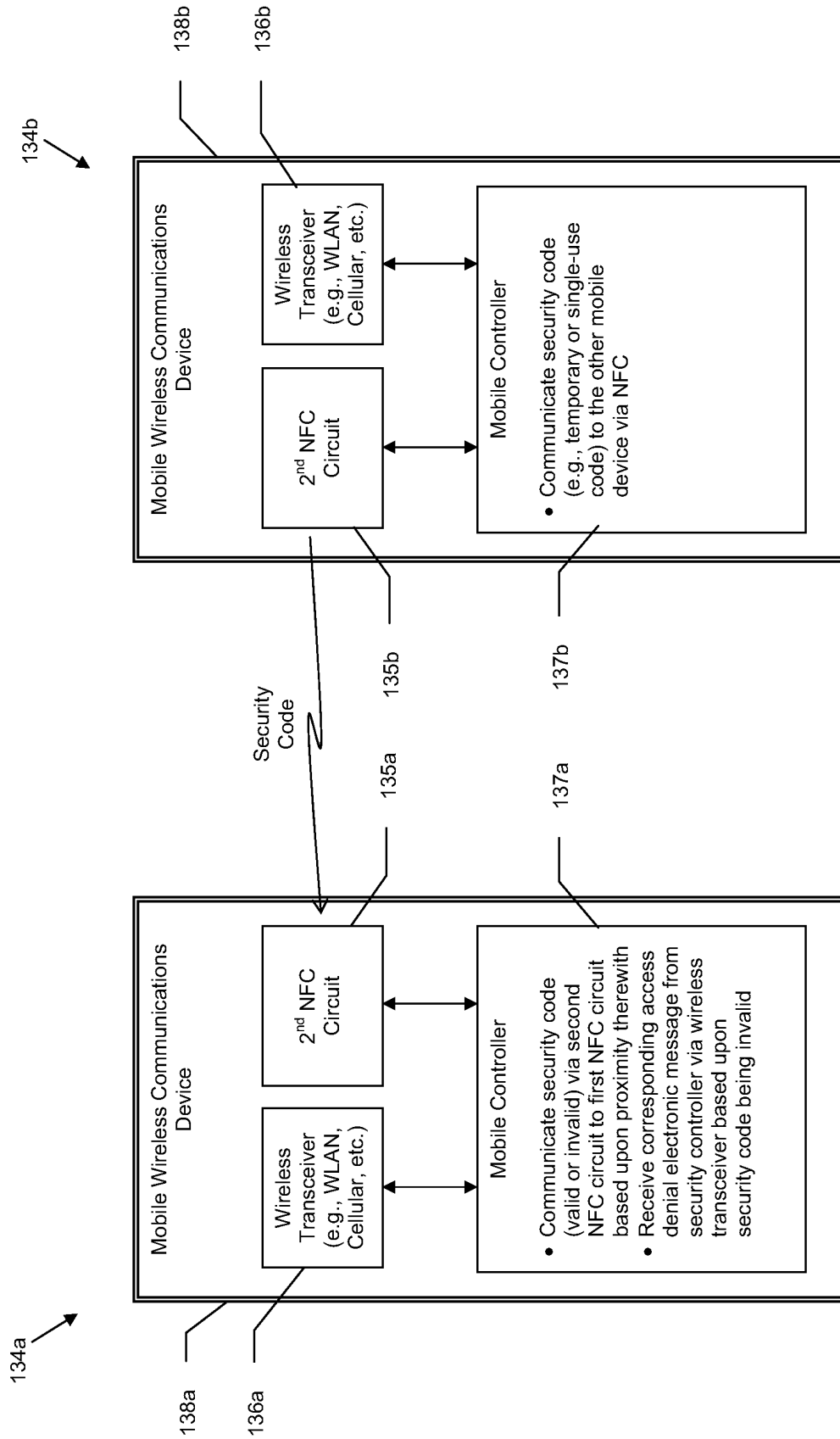


FIG. 3

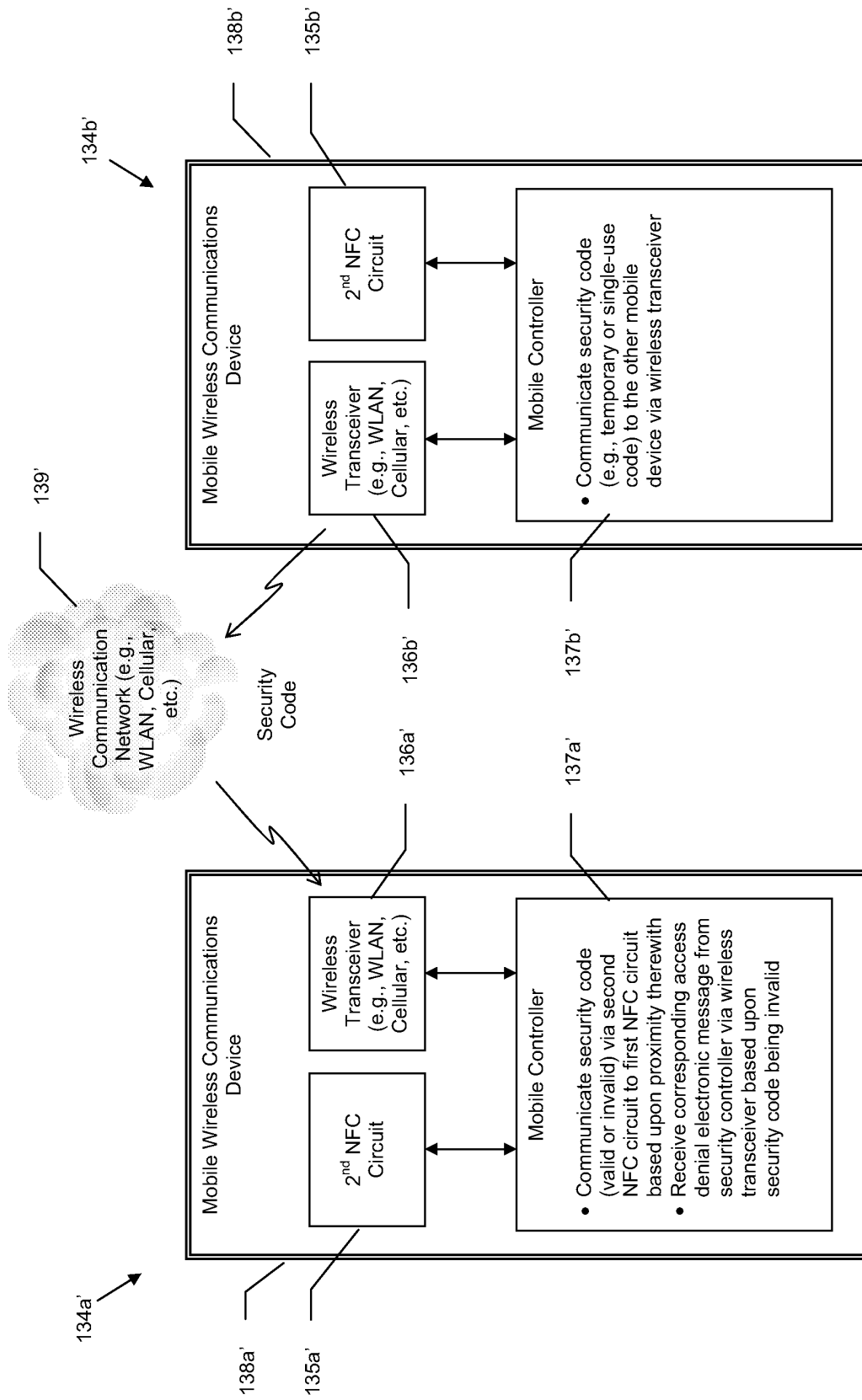


FIG. 4

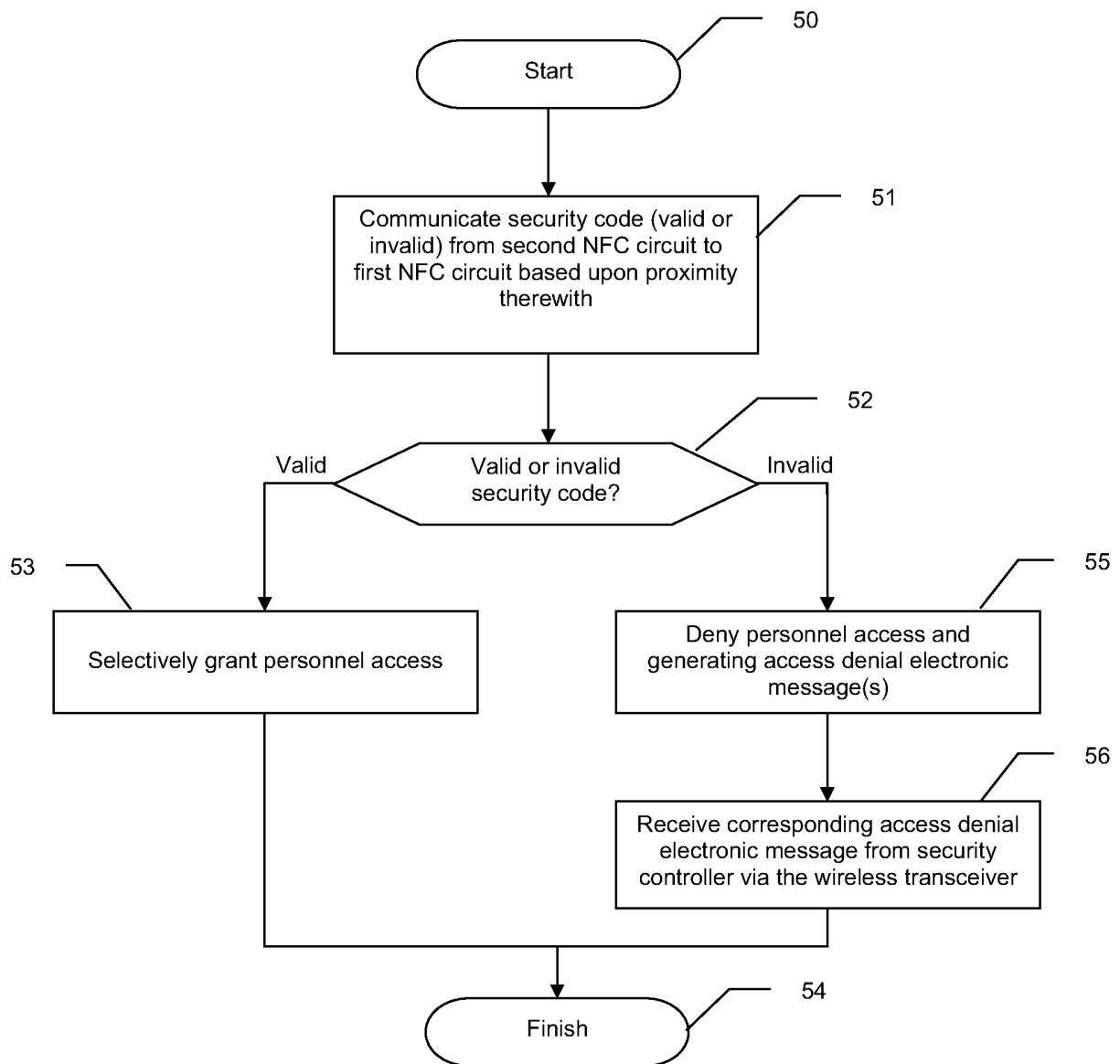


FIG. 5

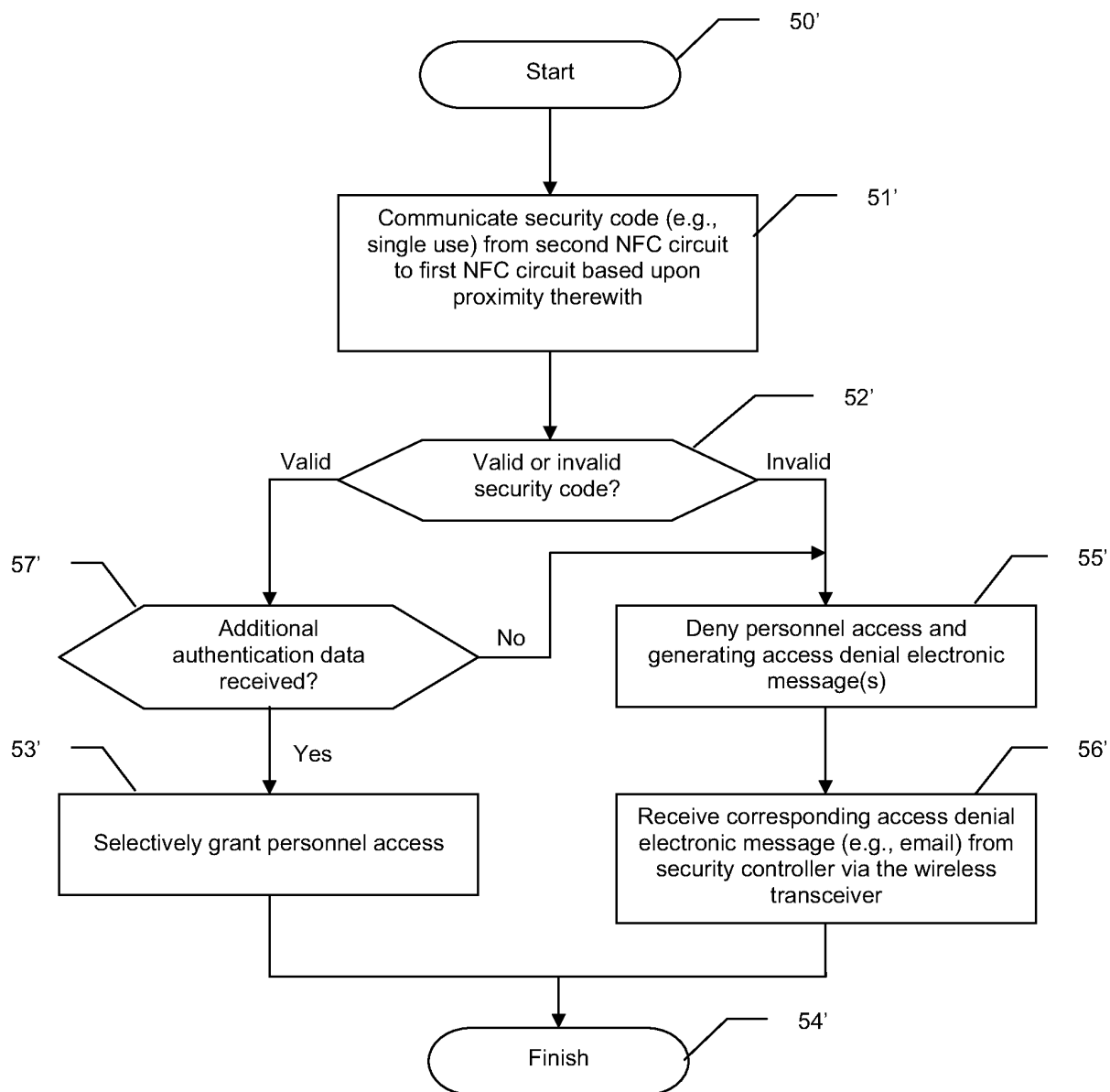


FIG. 6

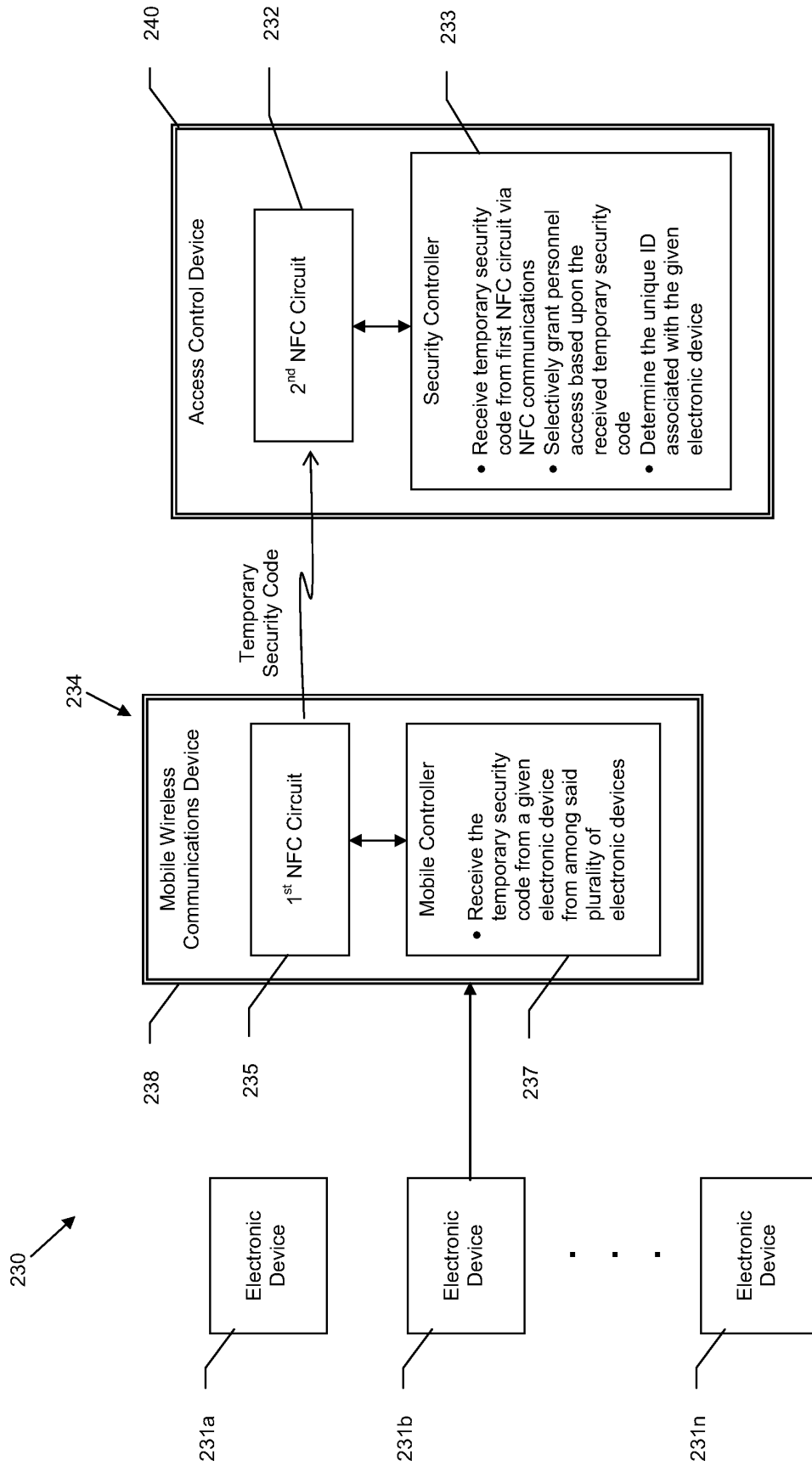


FIG. 7

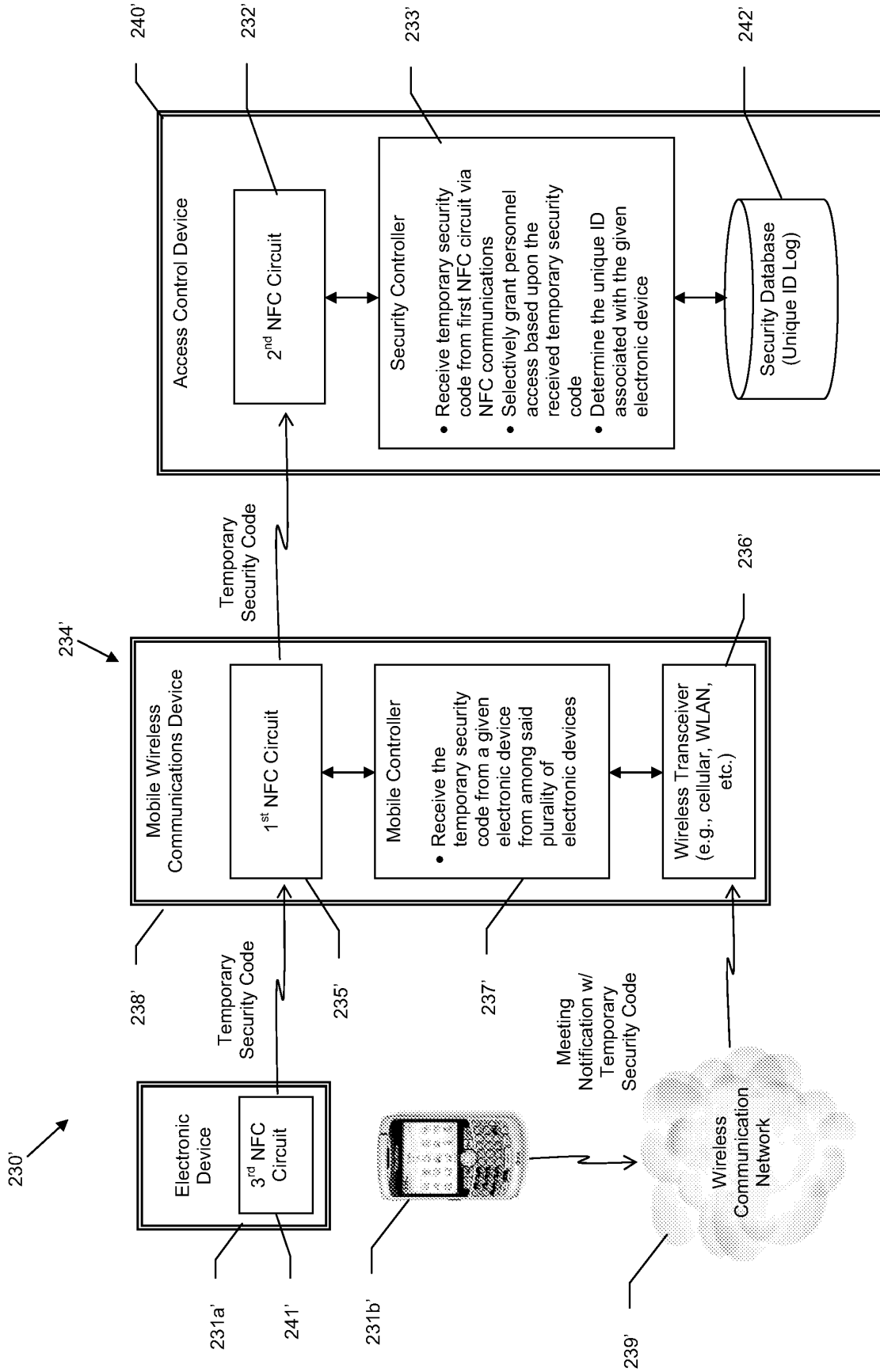
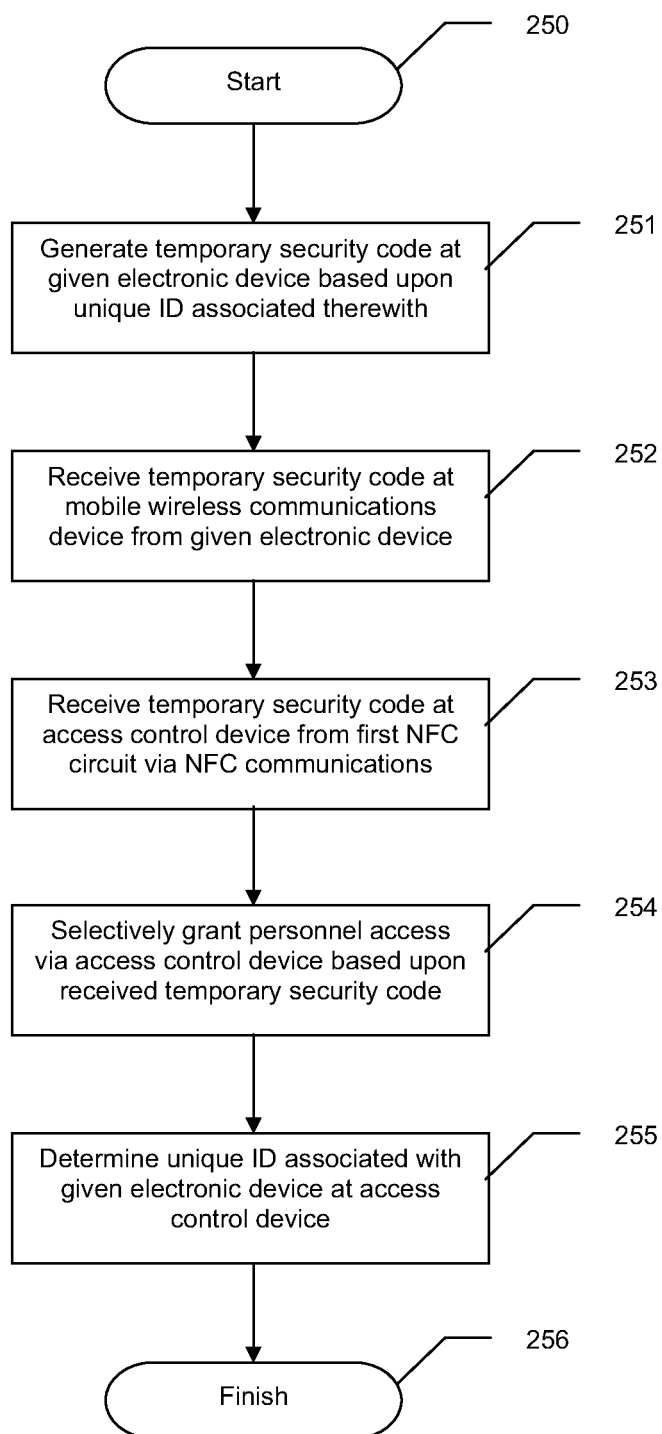


FIG. 8

**FIG. 9**

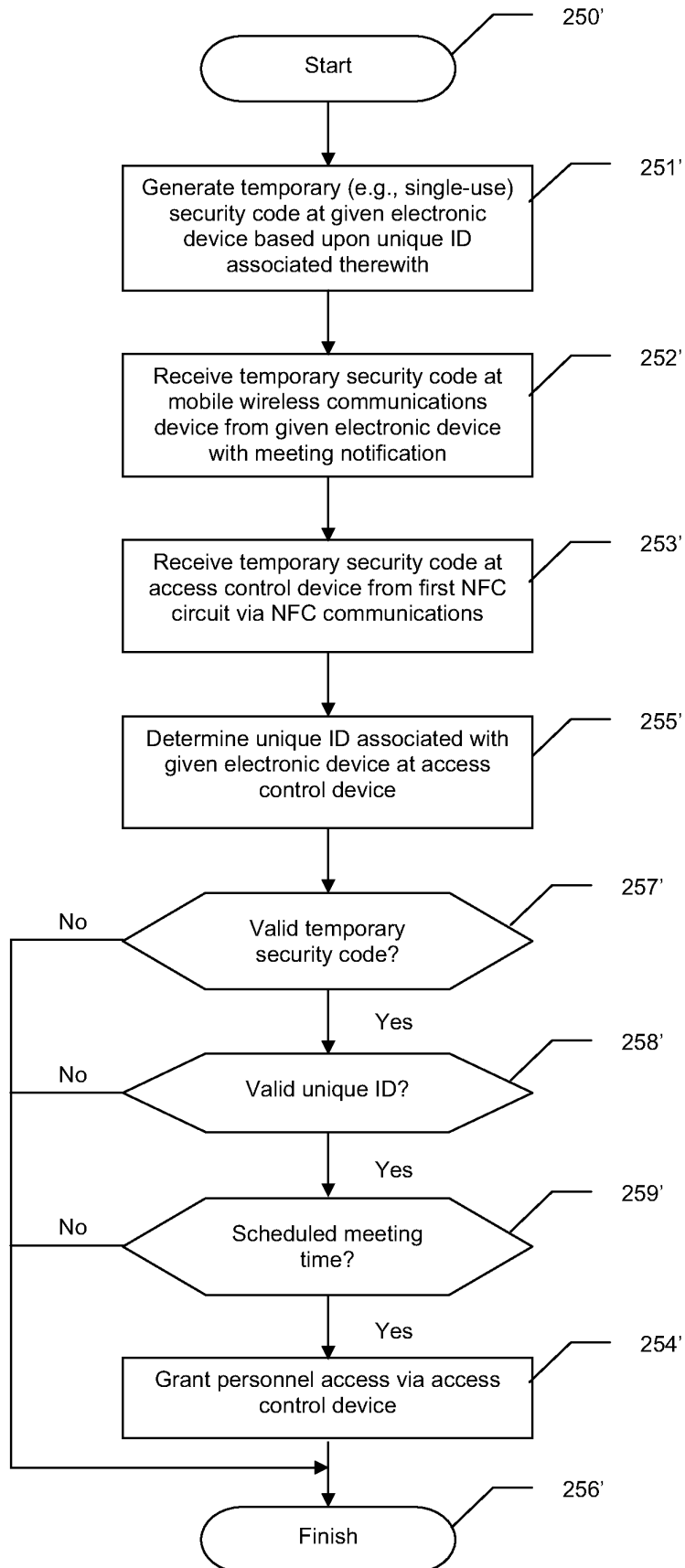


FIG. 10

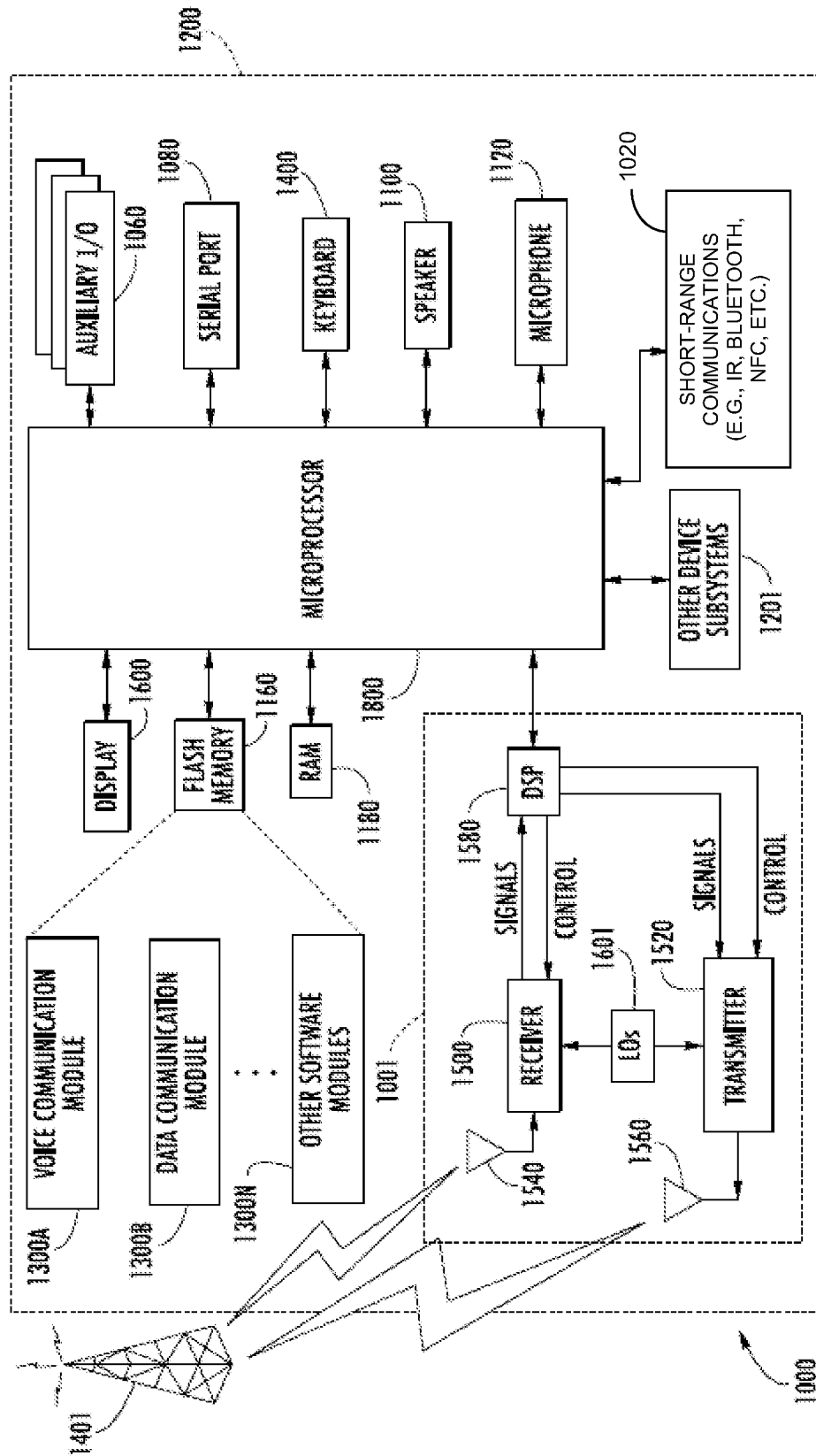


FIG. 11



EUROPEAN SEARCH REPORT

Application Number
EP 10 17 8684

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 02/31778 A1 (NOKIA CORP [FI]; NOKIA INC [US]) 18 April 2002 (2002-04-18) * abstract; figures 4,5 * * page 4, line 14 - page 7, line 5 * * page 8, line 1 - page 9, line 3 * * page 9, last paragraph * * page 10, last line - page 11, line 17 * * page 13, line 8 - page 14, line 5 * * page 19, paragraph 2 - page 20, paragraph 3 * * page 22, line 13 - page 28, line 15 * -----	1-15	INV. G07C9/00
X	WO 2008/076074 A1 (PHONIRO AB [SE]; KNUTSSON LARS [SE]; RUNESSON JONAS [SE]; BLIDING OLLE) 26 June 2008 (2008-06-26) * abstract; claims 1-3,5,20; figures 1,2,5 * * page 4, line 32 - page 5, line 12 * * page 6, lines 1-13 * * page 10, line 12 - page 14, line 2 * -----	1-15	
A	WO 2007/126375 A1 (SICS SWEDISH INST OF COMP SCIE [SE]; SADIGHI BABAK [SE]; CAO LING [SE]) 8 November 2007 (2007-11-08) * abstract; figure 6 * * page 4, lines 15-32 * * page 13, line 27 - page 14, line 21 * -----	1-15	TECHNICAL FIELDS SEARCHED (IPC) G07C
A	EP 2 096 240 A1 (PANASONIC CORP [JP]) 2 September 2009 (2009-09-02) * figures 1-5,15-17 * * paragraphs [0040] - [0054] * * paragraphs [0068] - [0071] * -----	1-15	
3 The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 22 February 2011	Examiner Buron, Emmanue1
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 10 17 8684

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-02-2011

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0231778	A1	18-04-2002	AT 414962 T	15-12-2008
			AU 9411501 A	22-04-2002
			EP 1325476 A1	09-07-2003
			FI 20002255 A	14-04-2002
			US 2006072755 A1	06-04-2006

WO 2008076074	A1	26-06-2008	EP 2122584 A1	25-11-2009
			SE 0602754 A	21-06-2008
			US 2010141381 A1	10-06-2010

WO 2007126375	A1	08-11-2007	EP 2016566 A1	21-01-2009
			SE 529849 C2	11-12-2007
			SE 0600959 A	29-10-2007
			US 2009183541 A1	23-07-2009

EP 2096240	A1	02-09-2009	WO 2008075423 A1	26-06-2008
			US 2010223465 A1	02-09-2010
