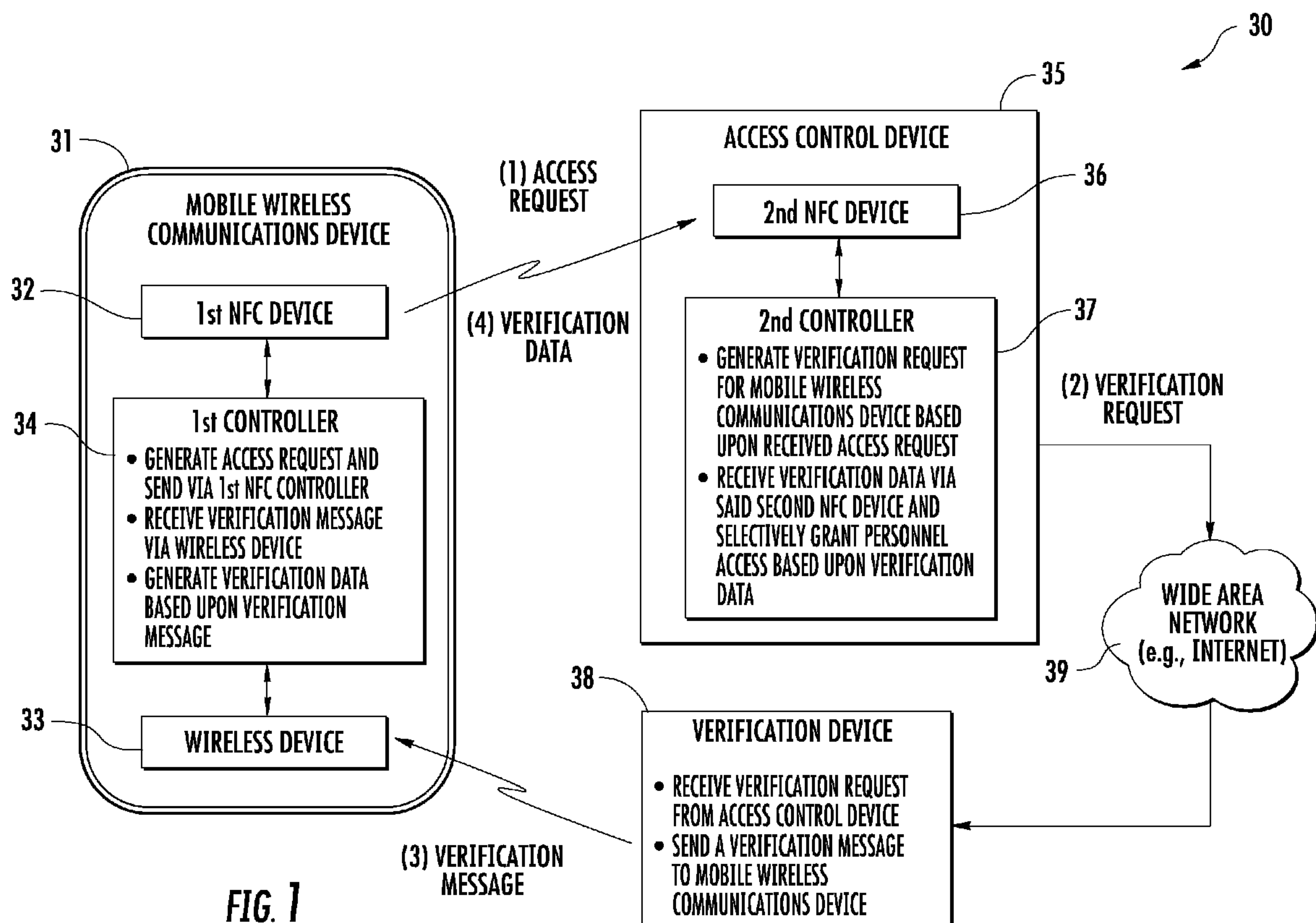




(86) Date de dépôt PCT/PCT Filing Date: 2012/02/23
(87) Date publication PCT/PCT Publication Date: 2012/08/30
(85) Entrée phase nationale/National Entry: 2013/08/22
(86) N° demande PCT/PCT Application No.: CA 2012/050110
(87) N° publication PCT/PCT Publication No.: 2012/113080
(30) Priorité/Priority: 2011/02/24 (EP11155796.3)

(51) Cl.Int./Int.Cl. *H04W 12/08* (2009.01),
H04W 4/12 (2009.01), *H04W 8/26* (2009.01),
H04W 84/18 (2009.01)
(71) Demandeur/Applicant:
BLACKBERRY LIMITED, CA
(72) Inventeurs/Inventors:
CARBONELL DUQUE, SANTIAGO, CO;
ZUBIRI, ALBERTO DANIEL, CA;
BUCZEK, TOMASZ, CA
(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME D'ACCES PERSONNEL A CARACTERISTIQUES DE VERIFICATION UTILISANT DES COMMUNICATIONS EN CHAMP PROCHE (NFC) ET PROCEDES ASSOCIES
(54) Title: PERSONNEL ACCESS SYSTEM WITH VERIFICATION FEATURES UTILIZING NEAR FIELD COMMUNICATION (NFC) AND RELATED METHODS



(57) Abrégé/Abstract:

A personnel access system may include a mobile device(s) comprising a first near field communication (NFC) device, a wireless device, and a first controller configured to generate an access request. An access control device may be associated with a

(57) **Abrégé(suite)/Abstract(continued):**

personnel access position and include a second NFC device configured to receive the access request, and a second controller configured to generate a verification request for the mobile device(s) based upon the received access request. A verification device may be configured to receive the verification request from the access control device, and send a verification message to the mobile device(s). The first controller may be configured to receive the verification message via the wireless device, and generate verification data based thereon. The second controller may be configured to selectively grant personnel access based upon the verification data.

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

(19) World Intellectual Property
Organization
International Bureau



WIPO | PCT



(10) International Publication Number
WO 2012/113080 A1

(43) International Publication Date
30 August 2012 (30.08.2012)

(51) International Patent Classification:

H04W 12/08 (2009.01) *H04W 8/26* (2009.01)
H04W 4/12 (2009.01) *H04W 84/18* (2009.01)

(21) International Application Number:

PCT/CA2012/050110

(22) International Filing Date:

23 February 2012 (23.02.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

11155796.3 24 February 2011 (24.02.2011) EP

(71) Applicant (for all designated States except US): **RE-SEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **CARBONELL DUQUE, Santiago** [CO/CO]; Carrera 7 #93 A - 05, Apt 603, Bogota (CO). **ZUBIRI, Alberto Daniel** [CA/CA]; 15063 - 4715 Tahoe Blvd, Mississauga, Ontario L4W 0B4 (CA). **BUCZEK, Tomasz** [CA/CA]; 14350 - 4715 Tahoe Blvd, Mississauga, Ontario L4W 0B4 (CA).

(74) Agent: **RIDOUT & MAYBEE LLP**; 225 King Street West, Toronto, Ontario M5V 3M2 (CA).

(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, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) Title: PERSONNEL ACCESS SYSTEM WITH VERIFICATION FEATURES UTILIZING NEAR FIELD COMMUNICATION (NFC) AND RELATED METHODS

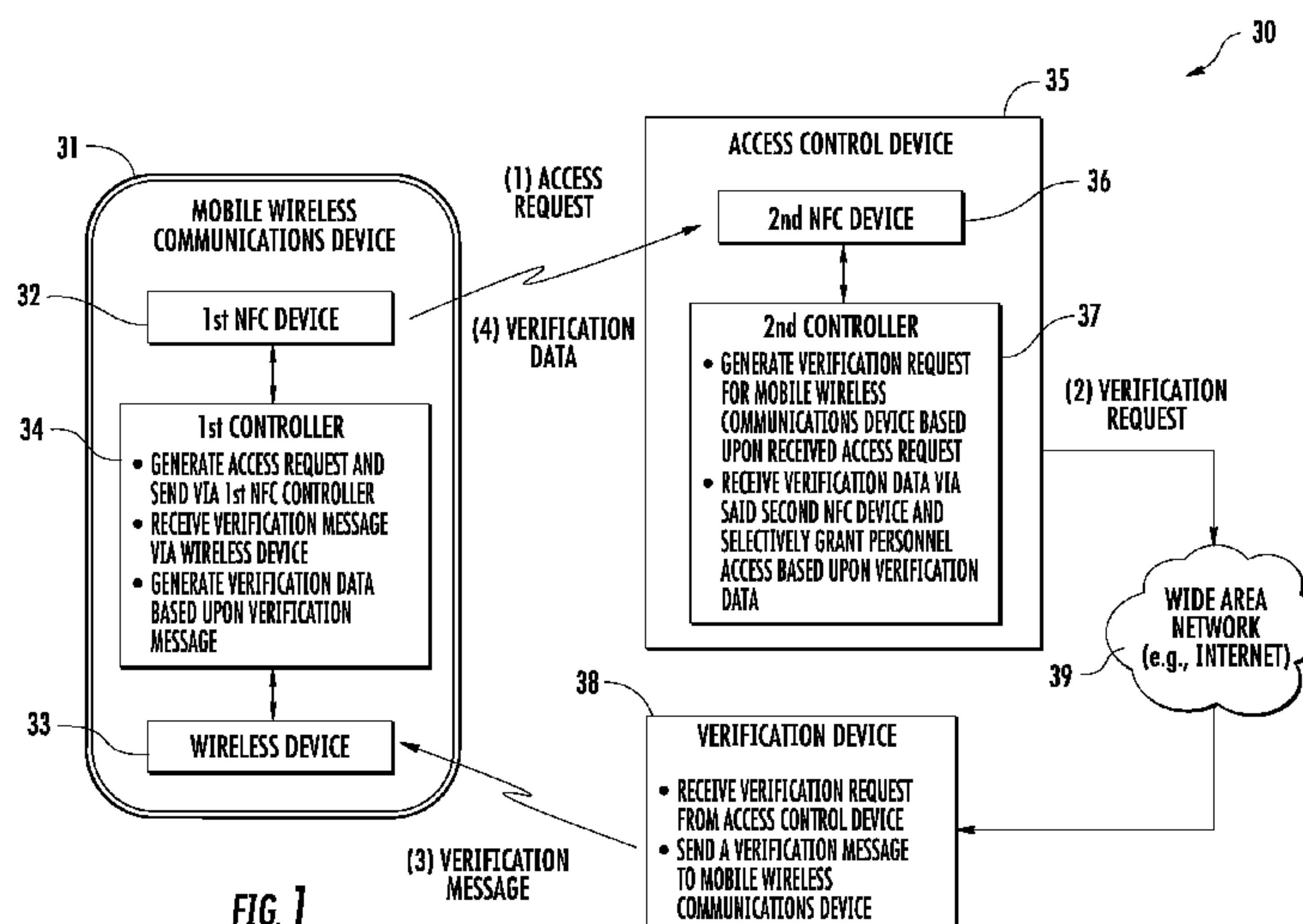


FIG. 1

(57) Abstract: A personnel access system may include a mobile device(s) comprising a first near field communication (NFC) device, a wireless device, and a first controller configured to generate an access request. An access control device may be associated with a personnel access position and include a second NFC device configured to receive the access request, and a second controller configured to generate a verification request for the mobile device(s) based upon the received access request. A verification device may be configured to receive the verification request from the access control device, and send a verification message to the mobile device(s). The first controller may be configured to receive the verification message via the wireless device, and generate verification data based thereon. The second controller may be configured to selectively grant personnel access based upon the verification data.

WO 2012/113080 A1

PERSONNEL ACCESS SYSTEM WITH VERIFICATION FEATURES UTILIZING
NEAR FIELD COMMUNICATION (NFC) AND RELATED METHODS

5 Cross-Reference to Related Application

[0001] This application claims the benefit of and
priority to European Patent Application Serial No.
11155796.3 filed February 24, 2011 under the title PERSONNEL
ACCESS SYSTEM WITH VERIFICATION FEATURES UTILIZING NEAR
10 FIELD COMMUNICATION (NFC) AND RELATED METHODS.

[0002] The content of the above patent application is
hereby expressly incorporated by reference into the detailed
description hereof.

15 Technical Field

[0003] This application relates to the field of
communications, and more particularly, to wireless
communications systems and related methods.

20 Background

[0004] 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
25 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
30 local area network (WLAN), for example.

[0005] Some mobile devices incorporate contactless card
technology and/or near field communication (NFC) chips. NFC
technology is commonly used for contactless short-range
communications based on radio frequency identification
35 (RFID) standards, using magnetic field induction to enable

communication between electronic devices, including mobile wireless communications devices. This short-range high frequency wireless communications technology exchanges data between devices over a short distance, such as only a few
5 centimeters.

Brief Description of the Drawings

- [0006] FIG. 1 is a schematic block diagram of a personnel access system in accordance with an example embodiment.
- 10 [0007] FIG. 2 is a flow diagram illustrating method aspects associated with the system of FIG. 1.
- [0008] FIG. 3 is a schematic block diagram of an example embodiment of the mobile wireless communications device of FIG. 1 shown in greater detail.
- 15 [0009] FIG. 4 is a schematic block diagram illustrating example components of a mobile wireless communications device that may be used with the devices of FIGS. 1 and 3.

Detailed Description

- 20 [0010] The present description is made with reference to the accompanying drawings, in which 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
25 provided so that this disclosure will be thorough and complete. Like numbers refer to like elements throughout.
- [0011] Generally speaking, a personnel access system is disclosed herein which may include at least one mobile wireless communications device comprising a first near field
30 communication (NFC) device, a wireless device, and a first controller coupled with the first NFC device and the wireless device and configured to generate an access request. The system may further include an access control device associated with a personnel access position and

comprising a second NFC device configured to receive the access request from the first NFC device based upon proximity therewith, and a second controller coupled with the second NFC device and configured to generate a

5 verification request for the at least one mobile wireless communications device based upon the received access request. The system may also include a verification device configured to receive the verification request from the access control device and, based thereon, send a

10 verification message to the at least one mobile wireless communications device. More particularly, the first controller may be further configured to receive the verification message via the wireless device and, based thereon, generate verification data. Also, the second

15 controller may be further configured to selectively grant personnel access based upon the verification data. Accordingly, the system may advantageously provide an enhanced level of security for providing personnel access based upon NFC.

20 **[0012]** The at least one mobile wireless communications device may have a unique identification (UID) associated therewith, and the verification device may be configured to send the verification message to the at least one mobile wireless communications device based upon the UID. The first

25 controller may be configured to send the verification data to the access control device via the first NFC device. By way of example, the verification message may comprise an electronic mail (email) message, a peer-to-peer message, or a short message service (SMS) message, etc.

30 **[0013]** Additionally, the at least one mobile wireless communications device may further comprise an input device coupled to the first controller, and the first controller may be further configured to generate the verification data based upon the input device and the message data. The first

controller may be further configured to receive a password via the input device and send the verification data to the access control device. By way of example, the input device may comprise a keypad, a biometric sensor, an optical
5 sensor, etc. Also by way of example, the wireless device may comprise a cellular receiver. Furthermore, the second controller may be configured to send the verification request to the verification device via a wide area network.

[0014] A related mobile wireless communications device,
10 and a related access control device, such as those described briefly above, are also provided. In addition, a related personnel access method may include generating an access request with at least one mobile wireless communications device, sending the access request from the at least one
15 mobile wireless communications device to an access control device via near field communication (NFC) based upon proximity therewith, and sending a verification request for the at least one mobile wireless communications device from the access control device to a verification device based
20 upon the received access request. The method may further include sending a verification message from the verification device to the at least one mobile wireless communications device based upon the verification request, generating verification data at the at least one mobile wireless
25 communications device based upon the verification message, and selectively granting personnel access with the access control device based upon the verification data.

[0015] A related computer-readable medium may have computer-executable instructions for causing a mobile
30 wireless communications device comprising an NFC device and a wireless device to perform steps comprising generating and communicating an access request to an access control device associated with a personnel access position via the NFC device, where the access control device is configured to

generate a verification request for the at least one mobile wireless communications device based upon the access request and communicate the verification request to a verification device. The steps may further include receiving a
5 verification message from the verification device via the wireless device, where the verification message is generated based upon the verification request, and generating verification data based upon the received verification message for causing the access control device to selectively
10 grant personnel access.

[0016] Referring initially to FIGS. 1 through 3, an example personnel access system **30** and related method aspects are first described. The system **30** illustratively includes one or more mobile wireless communications devices
15 **31**, which are also referred to as "mobile devices" herein. By way of example, mobile devices such as portable or personal media players (e.g., music or MP3 players, video players, etc.), portable gaming devices, portable or mobile telephones, smartphones, tablet computers, electronic
20 readers ("e-readers"), etc., may be used, although other suitable types of mobile devices may also be used in various embodiments.

[0017] The mobile device **31** illustratively includes a first near field communication (NFC) device **32**, a wireless
25 device **33**, and a first controller **34** coupled to the first NFC device **32** and the wireless device **33**. 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
30 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.

[0018] In the example of FIG. 3, the wireless device 33 is a cellular device (e.g., a cellular receiver or
5 transceiver). However, it will be appreciated that other wireless communications formats may also be used, such as Bluetooth, WiFi, WiMAX, etc., for example. The first controller 34 may be implemented using a combination of
10 hardware (e.g., processor, memory, etc.) and software (e.g., a computer-readable medium having computer-executable instructions), for example, to perform the various operations or functions described herein.

[0019] Now referring to FIG. 2, beginning at Block 50, the first controller 34 is configured to generate an access
15 request, at Block 51. More particularly, the first controller 34 may be configured to cooperate with the first NFC device 32 to communicate or send the access request to an access control device 35 via NFC, at Block 52. The access control device 35 is associated with a personnel access
20 position. By way of example, the personnel access position may correspond to a security door which is locked to prevent unauthorized access to a particular physical area. In other example embodiments, however, the personnel access position may correspond to a security gate or turnstile, or to a
25 secure object such as a safe, locker, or a vehicle, for example.

[0020] The access control device 35 illustratively includes a second NFC device 36 and a second controller 37 coupled to the second NFC device 36. It should be noted that
30 these components may be co-located or separately located in different embodiments. For example, the second NFC device 36 may be located at the personnel access position, and the second controller 37 may be co-located with the second NFC device 36 or remotely connected thereto, such as over a

local area network (LAN), wireless communications link, the Internet, etc. The second controller **37** may also be implemented using hardware and software components, for example.

5 **[0021]** The second NFC device **36** is configured to communicate with the first NFC device **32** based upon proximity therewith, as described above, to receive the access request. For example, when the mobile device **31** is swiped or bumped with the second NFC device **36**, NFC
10 communications are established between the first NFC device **32** and second NFC device **36**, and the access request is communicated or sent via NFC to the second NFC device **36**. By way of example, the mobile device **31** may have a unique identification (UID) associated therewith, and the access
15 request may include the UID to identify the given mobile device (and, therefore, a user associated with the mobile device) that is attempting to obtain access.

[0022] Rather than merely checking to see if the UID (or other identifier) of the mobile device **31** is on an approved
20 mobile device security list, for example, the access control device **35** advantageously initiates additional security measures to verify whether personnel access should be granted. For example, in some cases the mobile device **31** may be lost or stolen from its rightful owner, in which case
25 someone else may attempt to surreptitiously gain access via the access control device **35** using the mobile device. If the access control device **35** were to end its security check after determining that the mobile device **31** (which is associated with an authorized user) is on an approved mobile
30 device security list, then an unauthorized person would be granted access merely by possessing the mobile device of the authorized user.

[0023] However, the second controller **37** is advantageously configured to generate a verification request

for the mobile device **31** based upon the received access request, and send the verification request to a verification device **38**, at Block **53**. By way of example, the verification request may include the UID of the mobile device **31**, or
5 other data that identifies the given mobile device to the verification device **38**. For example, the verification device **38** may comprise a server that is remotely located from the access control device **35** and communicates with the access control device via a network, such as a wide area network **39**
10 (e.g., the Internet). However, in some embodiments the verification device **38** may be co-located with the access control device **35**, i.e., "on-site" adjacent the personnel access position, and they may communicate via a LAN, wireless link, etc. Moreover, other suitable verification
15 devices than a server may be used in some applications.

[0024] The verification device **38** is configured to receive the verification request from the access control device **35** and, based thereon, send a verification message to the mobile device **31**, at Block **54**. By way of example, the
20 verification message may comprise an electronic mail (email) message, short message service (SMS) message, peer-to-peer message, etc. That is, the message is directed to a unique address (e.g., the UID) associated with the mobile device
31, which in the case of an email the UID comprises an email
25 address, and in the case of an SMS message the UID comprises a telephone number. However, other UIDs may also be used, such as an IMEI number, a PIN number, etc.

[0025] The first controller **34** is further configured to receive the verification message via the wireless device **33**
30 and, based thereon, send verification data to the access control device **35**, such as via the first NFC device **32** (although this may also be done via the wireless device **33** and the verification device **38** in some example embodiments) at Block **55**. In accordance with one example, the

verification data may be included in the verification message. That is, an alphanumeric verification sequence, etc., may be included in the message to pass along to the access control device **35**. By way of example, the

5 verification data may comprise a pseudorandom data, may be single or one-time use data, a rolling PIN code, expire after a certain duration, etc.

[0026] The verification data may be made available to provide to the access control device **35** upon opening of the
10 verification message on the mobile device **31**, for example. Because access to messages received on the mobile device **31** may be restricted (e.g., through password protection, etc.), this may advantageously be used to verify that the proper user of the mobile device **31** does indeed have it in his
15 possession. That is, simply having possession of the mobile device **31** would not be sufficient to gain access to the physical location controlled by the access control device **35**. Rather, one would also have to have access to the email, SMS message, etc., that will be addressed and sent directly
20 to the address, phone number, etc., known to be associated with the intended recipient and user of the mobile device **31**. For example, a password or other factor of authentication may need to be entered via the input device **40** to switch the mobile device **31** from a locked state into
25 an unlocked state in which the verification message may be viewed or used. In one example use case, a user may enter a device password to obtain access to an access code that the verification device 38 sends to the mobile device **31**.

[0027] In accordance with another example, the mobile
30 device **31** may further include one or more input devices **40** (FIG. 3), and the verification data may be generated also based upon input from the input device **40**. In one example, input device **40** comprises a keypad. To generate proper verification data, the verification message may prompt a

user to enter an alphanumeric verification sequence (e.g., a pseudorandom key, etc.) included in the message, for example. In another example, input device **40** comprises an audio input device (e.g., microphone), and the verification message may prompt a user to record a particular speech pattern, etc., to generate proper verification data. In yet another example, input device **40** comprises a biometric sensor (e.g., a fingerprint sensor), and the verification message may prompt the user for appropriate biometric input to generate the verification data. In still another example, input device **40** comprises an optical sensor (e.g., a digital camera), and the user may be prompted by the verification message to capture an image of something at the personnel access position for verification purposes (e.g., a bar code or QR code, etc.).

[0028] The second controller **37** may be further configured to receive the verification data generated or provided by the mobile device **31** via the second NFC device **36** (although in some embodiments verification data (e.g., PIN, etc.) may be provided at the access control device (e.g., via a keypad, etc.)), and selectively grant personnel access based thereon, at Block **56**, which illustratively concludes the method of FIG. 2 (Block **57**). That is, in addition to initially determining that the mobile device **31** is authorized for personnel access, which may be done prior to sending the verification request to the verification device **38**, the access control device **35** also verifies that the correct verification data is provided by the mobile device **31**, responsive to a verification message uniquely addressed to the mobile device **31**, before providing personnel access. This advantageously helps ensure that the operator or user that has possession of the mobile device **31** is in fact the user assigned to or associated with the mobile device, and therefore authorized for gaining personnel access. The

second controller **37** may verify the received verification data based upon previously stored information (e.g., by comparison to a reference fingerprint or voice print), or via communication with the verification device **38** (e.g., to
5 retrieve the pseudorandom password sent to the mobile device **31** for comparison, etc.). In some example embodiments, the verification device **38** may perform the requisite verification or comparison operations (e.g., fingerprint comparison, voice print comparison, etc.).

10 **[0029]** Accordingly, the system **30** advantageously provides an additional layer of security for physical access control situations. For example, it may allow companies, governmental institutions, educational institutions, financial institutions, and other owners or tenants of real
15 property, etc., to control after hours access to buildings and rooms with high value or sensitive equipment or information. In this regard, the additional verification performed by sending the verification to the verification device **38** may be selectively enabled, such as during
20 particular times of the day (e.g., after-hours) when a personnel access position is not otherwise attended by a receptionist or security guard, for example. Such access control features may be set by a system administrator with access to the access control device **35** or the verification
25 device **38**, for example.

[0030] In accordance with one example implementation using the BlackBerry communications infrastructure from the present assignee Research in Motion Limited, the verification device **38** may be implemented using the
30 BlackBerry Enterprise Server (BES). In this regard, a BlackBerry PIN message may be used as the verification message, for example. However, it will be noted that other suitable verification devices and verification message types may be used in difference embodiments.

[0031] Example components of a mobile wireless communications device **1000** that may be used in accordance with the above-described embodiments are further described below with reference to FIG. 4. The device **1000**
5 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**
10 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**.

15 [0032] The housing **1200** may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keypad may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

20 [0033] In addition to the processing device **1800**, other parts of the mobile device **1000** are shown schematically in FIG. 4. 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
25 **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
30 the capability to communicate with other computer systems via the Internet.

[0034] 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**.

[0035] 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.

[0036] 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
5 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,
10 3GPP, UMTS, 4G, etc.

[0037] 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
15 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.

20 [0038] 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
25 to the receiver **1500**, which provides for signal amplification, frequency down conversion, filtering, channel 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
30 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**.

[0039] 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**.

10 [0040] 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**.

[0041] 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.

[0042] 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
5 subsystem may include an infrared device and associated circuits and components, a Bluetooth™ communications module to provide for communication with similarly-enabled systems and devices, or a near field communications (NFC) sensor for communicating with a NFC device or NFC tag via NFC
10 communications.

[0043] 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
15 various modifications and embodiments are intended to be included within the scope of the appended claims.

THAT WHICH IS CLAIMED IS:

1. A personnel access system comprising:
at least one mobile wireless communications device
5 comprising
a first near field communication (NFC)
device,
a wireless device, and
a first controller coupled with said first
10 NFC device and said wireless device, the first
controller being configured to generate an access
request;
an access control device associated with a
personnel access position, the access control device
15 comprising
a second NFC device configured to receive the
access request from said first NFC device based
upon proximity therewith, and
a second controller coupled with said second
20 NFC device, the second controller being configured
to generate a verification request for the at
least one mobile wireless communications device
based upon the received access request; and
a verification device configured to receive the
25 verification request from said access control device and,
based thereon, send a verification message to said at least
one mobile wireless communications device;
said first controller being further configured to
receive the verification message via said wireless device
30 and, based thereon, generate verification data;
said second controller being further configured to
selectively grant personnel access based upon the
verification data.

2. The personnel access system of Claim 1 wherein said at least one mobile wireless communications device has a unique identification (UID) associated therewith; and wherein said verification device is
5 configured to send the verification message to said at least one mobile wireless communications device based upon the UID.

3. The personnel access system of Claim 1
10 wherein said first controller is further configured to send the verification data to said access control device via said first NFC device.

4. The personnel access system of Claim 1
15 wherein the verification message comprises at least one of an electronic mail (email) message, a peer-to-peer message, or a short message service (SMS) message.

5. The personnel access system of Claim 1
20 wherein said at least one mobile wireless communications device further comprises an input device coupled to said first controller; and wherein said first controller is further configured to generate the verification data based upon said input device.

25 6. A mobile wireless communications device comprising:
a near field communication (NFC) device,
a wireless device, and
30 a controller coupled with said first NFC device and said wireless device, the controller being configured to generate and communicate an access request to an access control device associated with a personnel access position via said NFC device,

receive a verification message from a
verification device via said wireless device, and
generate verification data based upon the
received verification message for causing the
5 access control device to selectively grant
personnel access.

7. The mobile wireless communications device of
Claim 6 wherein said controller is further configured to
10 send the verification data to the access control device via
said NFC device.

8. The mobile wireless communications device of
Claim 6 further comprising an input device coupled to said
15 controller; and wherein said controller is further
configured to generate the verification data based upon said
input device.

20 9. A personnel access method comprising:
generating an access request with at least one
mobile wireless communications device;
sending the access request from the at least one
mobile wireless communications device to an access control
25 device via near field communication (NFC) based upon
proximity therewith;
sending a verification request for the at least
one mobile wireless communications device from the access
control device to a verification device based upon the
30 received access request;
sending a verification message from the
verification device to the at least one mobile wireless
communications device based upon the verification request;

generating verification data at the at least one mobile wireless communications device based upon the verification message; and

selectively granting personnel access with the
5 access control device based upon the verification data.

10. The method of Claim 9 wherein the at least one mobile wireless communications device has a unique identification (UID) associated therewith; and wherein
10 sending the verification message comprises sending the verification message to the at least one mobile wireless communications device based upon the UID.

11. The method of Claim 9 further comprising
15 sending the verification data from the at least one mobile wireless communications device to the access control device via NFC.

12. The method of Claim 9 wherein the
20 verification message comprises at least one of an electronic mail (email) message, a peer-to-peer message, or a short message service (SMS) message.

13. The method of Claim 9 wherein the at least
25 one mobile wireless communications device further comprises an input device coupled with the first controller; and further comprising generating the verification data based upon the input device.

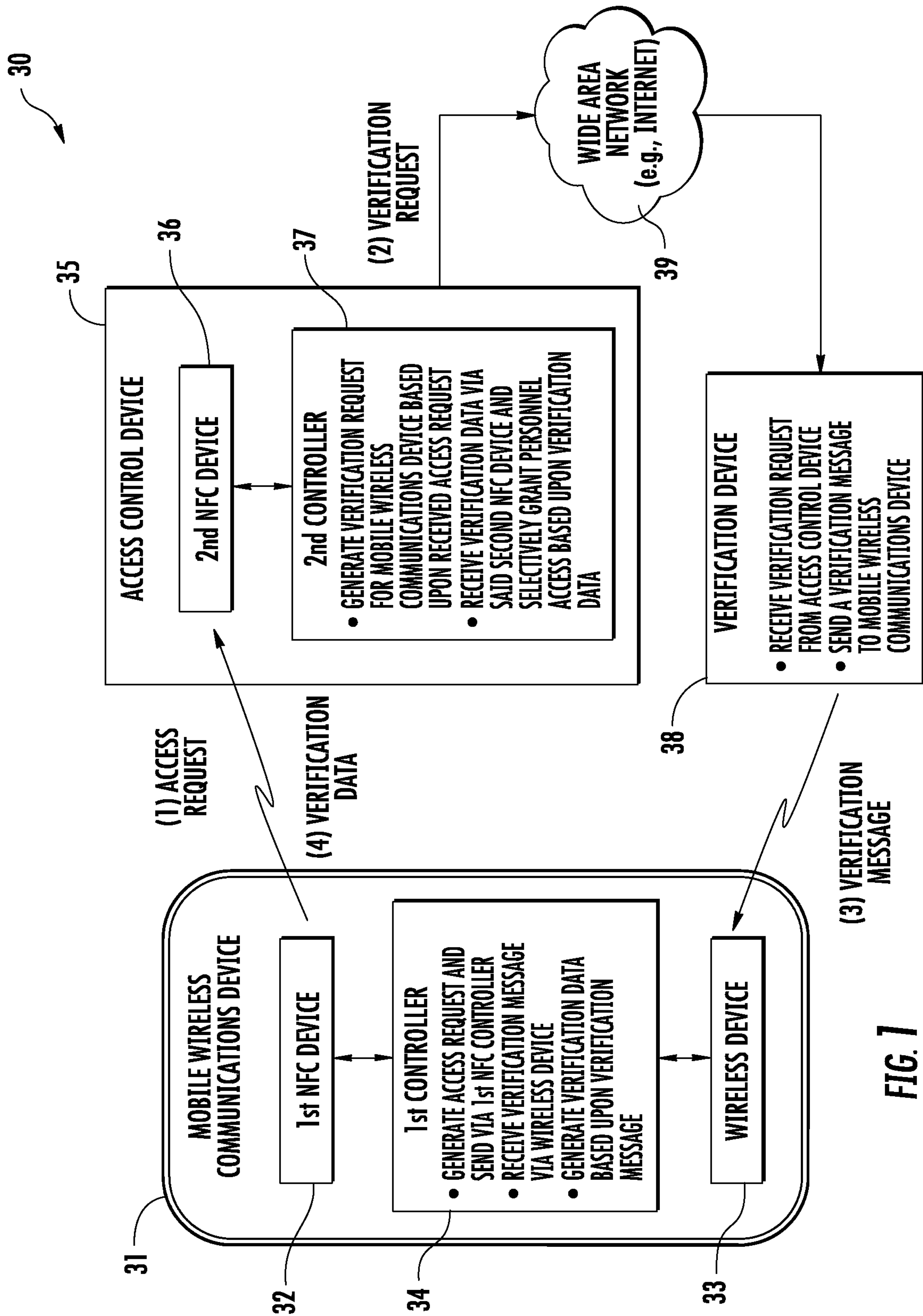
30 14. The method of Claim 9, wherein the at least one mobile wireless communications device further comprises an input device, the method further comprising receiving a password via the input device and sending the verification data to the access control device based upon the password.

35

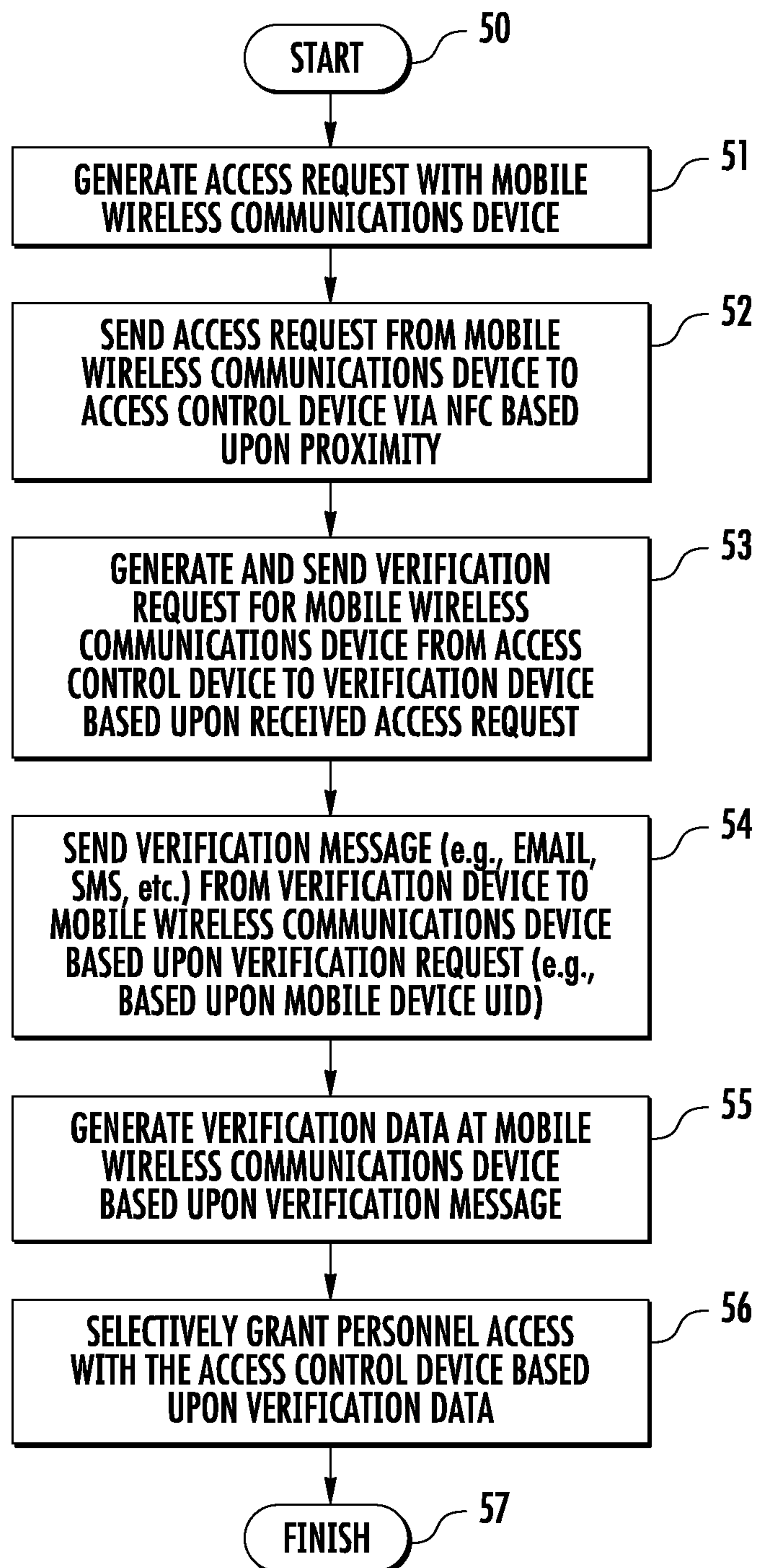
15. The method of Claim 9 wherein sending the verification request comprises sending the verification request from the access control device to the verification device via a wide area network.

5

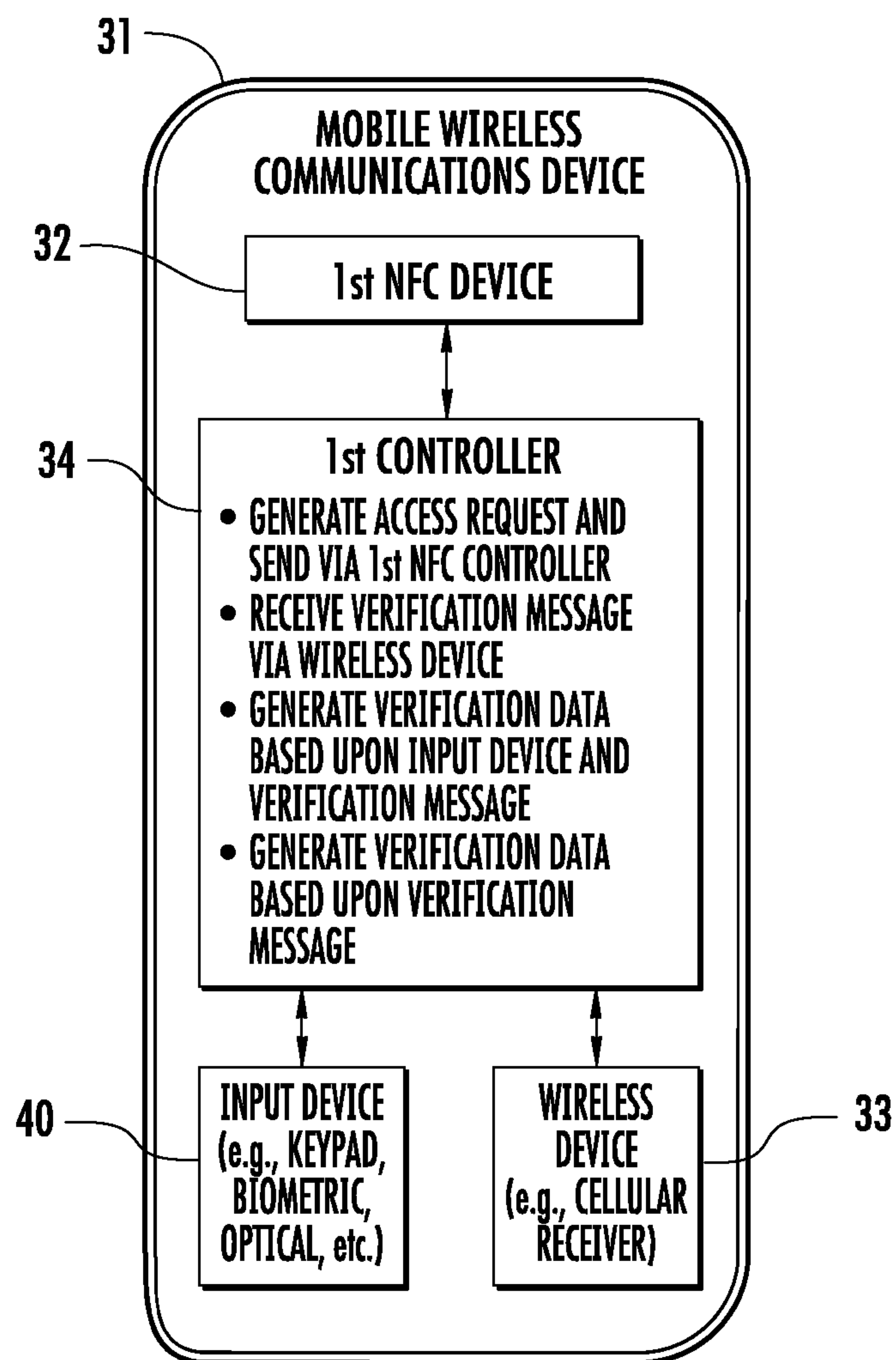
1/4



2/4

**FIG. 2**

3/4

**FIG. 3**

4/4

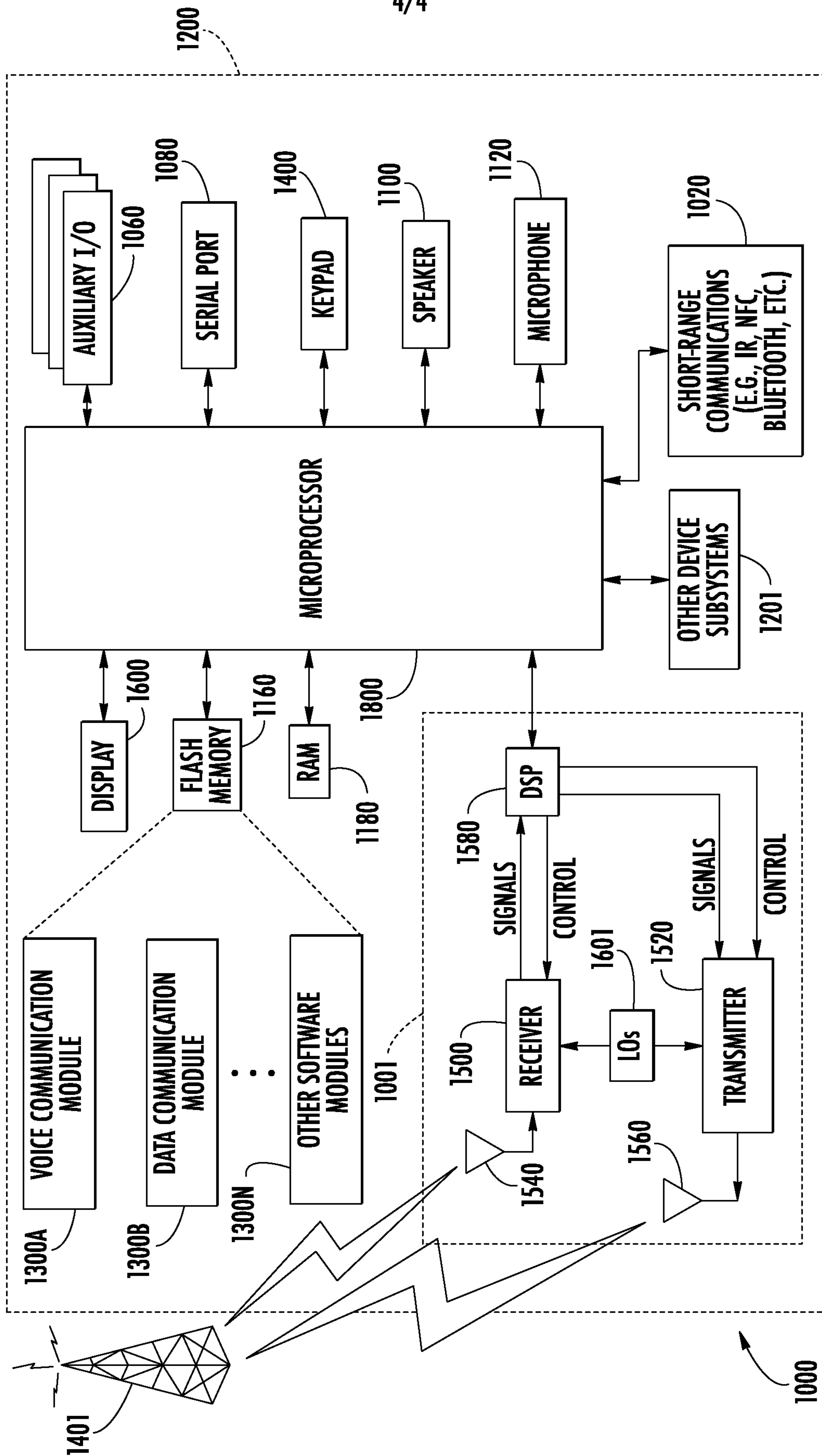


FIG. 4

