



(51) International Patent Classification:

G06Q 10/00 (2012.01) H04W 4/14 (2009.01)
G07C 11/00 (2006.01) H04B 5/00 (2006.01)
H04W 4/00 (2009.01)

(21) International Application Number:

PCT/CA2016/051031

(22) International Filing Date:

31 August 2016 (31.08.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/270,322 21 December 2015 (21.12.2015) US

(71) Applicant: GENETEC INC. [CA/CA]; 2280 Alfred-Nobel, Suite 400, St-Laurent, Québec H4S 2A4 (CA).

(72) Inventor: RACZ, Pierre; 110 av. Willowdale, Montreal, Québec H3T1E9 (CA).

(74) Agents: ANGLEHART, James et al.; 1939 de Maison-neuve Ouest, Montreal, Québec H3H 1K3 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

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

— with amended claims (Art. 19(1))

(54) Title: METHOD AND SYSTEM FOR VIRAL IDENTIFICATION OF EVACUEES

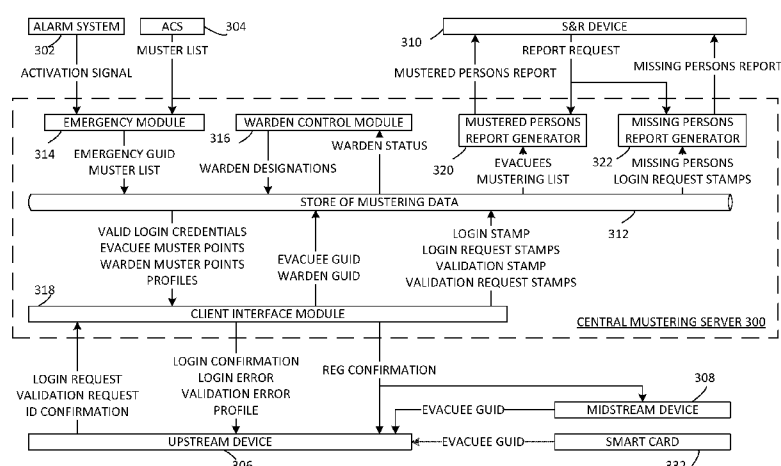


FIG. 3

(57) Abstract: A method and system for viral identification of evacuees are provided. The method is recursive and involves bringing an emergency warden and a midstream evacuee in close proximity with one another to enable a handheld computing device belonging to one of the two to read information from the other, enabling the handheld computing device to read the information, having the handheld computing device read the information to enable an identification of the midstream evacuee, providing the identifier of the midstream evacuee to a central mustering server, whereby the midstream evacuee is enabled to act as an emergency warden, and performing the method with the midstream evacuee acting as an emergency warden with respect to another evacuee before the central mustering server. The method provides the advantage of virally identifying evacuees within the confines of a muster point in an efficient and reliable manner.

METHOD AND SYSTEM FOR VIRAL IDENTIFICATION OF EVACUEES

Technical Field

[001] The present invention relates to emergency evacuation tools, and more specifically, to methods and systems for identifying evacuees.

5 Background

[002] When the alarm sounds and people must evacuate a building, the first priority is to make sure that everyone was able to get out as fast as possible. The usual fire drill procedure is to evacuate the people to a suitable muster point where a fire warden conducts a roll call and checks the name of the ones present against a list of the building occupants
10 expected to be seen at that muster point. The list should preferably be provided to the search and rescue services upon their arrival for assistance in their onsite operations.

[003] Pen and paper mustering solutions require that emergency wardens conduct roll calls before noisy crowds and manually produce attendance reports to be consulted by the fire and rescue services upon their arrival on site. Such solutions are impractical and lengthy,
15 especially in cases of larger evacuations, and as a result, the reports are rarely produced in a timely manner.

[004] Common electronic solutions involve a laptop that keeps an up-to-date list of all occupants, coupled with handheld card readers used to scan the badges of the evacuees. A peer-to-peer wireless network is established between the laptop and the card readers so that
20 as cards are being read, the laptop user is presented with seen/not-seen feedback. If no wireless network can be used, the handheld devices can collect the card reads, which can then be synchronized back to the laptop using a USB cable. Since this solution requires that every badge be scanned, and since handheld card readers can read seven to eight cards per minute, it can become impractical when the number of occupants increases.

25 [005] Electronic mustering solutions used within war zones can be adapted for use within the context of evacuations for expeditious mustering. Such solutions consist in mobile applications that enable survivors to report themselves before relevant authorities using Wi-Fi or SMS technologies. However, if the aforementioned mobile applications were adapted

for use within the context of evacuations, the reports that they would produce would be unreliable; not only would a building occupant be able to report from within the building, but also, someone can use a building occupant's device to issue a false report.

Summary

- 5 [006] It has been found that in a method of mustering evacuees, the steps of bringing an emergency warden and a midstream evacuee in close proximity with one another to enable a handheld computing device belonging to one of the two to read information from the other, enabling the handheld computing device to read the information, having the handheld computing device read the information to enable an identification of the midstream evacuee,
- 10 providing the identifier of the midstream evacuee to a central mustering server, whereby the midstream evacuee is enabled to act as an emergency warden, and performing the method in a recursive manner with the midstream evacuee acting as an emergency warden with respect to another evacuee provide the advantage of virally identifying evacuees within the confines of a muster point in an efficient and reliable manner.
- 15 [007] According to a first embodiment of the present invention there is provided a method of virally identifying evacuees at a muster point within the context of an emergency evacuation, the recursive method comprising: bringing an emergency warden and a midstream one of the evacuees in close proximity with one another to enable a handheld computing device of one of the emergency warden and midstream evacuee to read
- 20 information from another one of the emergency warden and midstream evacuee; enabling the handheld computing device to read the information; reading the information by the handheld computing device to enable an identification of the midstream evacuee before a central mustering server; providing an identifier of the midstream evacuee to the central mustering server, whereby the midstream evacuee is enabled to act as the emergency warden with
- 25 respect to another one of the evacuees; and performing the recursive method wherein the midstream evacuee acts as the emergency warden and the another evacuee acts as the midstream evacuee whereby the evacuees are virally identified within the confines of the muster point in an efficient and reliable manner.

[008] It has also been found that in a computer readable medium having stored thereon a mobile application to be executed within the context of an emergency evacuation at a muster point by evacuees on their handheld computing devices, the mobile application, when executed by a midstream one of the evacuees on a midstream one of the handheld computing devices, causing the device's processor to conduct a first transfer of information with an emergency warden to enable a first communication process by which the midstream evacuee is identified before a central mustering server, further requiring that the emergency warden and the midstream evacuee be brought in close proximity with one another to enable the first transfer of information, further causing the device's processor to conduct a second transfer of information with a downstream evacuee after the first transfer of information to enable a second communication process by which the downstream evacuee is identified before the central mustering server, the second exchange of information being enabled by bringing the midstream evacuee and the downstream evacuee in close proximity with one another; and further causing the processor to initiate at least one of the enabled first communication process and enabled second communication process provides the advantage of virally identifying evacuees within the confines of the muster point in an efficient and reliable manner.

[009] According to another aspect of the present invention, there is provided a computer readable medium having stored thereon a mobile application to be executed within the context of an emergency evacuation at a muster point by evacuees on their handheld computing devices, the mobile application, when executed by a midstream one of the evacuees on a midstream one of the handheld computing devices, causes the midstream handheld computing device's processor to: conduct a first transfer of information with an emergency warden to enable a first communication process by which the midstream evacuee is identified before a central mustering server, the first transfer of information being enabled by bringing the midstream evacuee and the emergency warden in close proximity with one another; conduct a second transfer of information with a downstream one of the evacuees after the first transfer of information to enable a second communication process by which the downstream evacuee is identified before the central mustering server, the second exchange of information being enabled by bringing the midstream evacuee and the downstream evacuee in close proximity with one another; and initiate at least one of the enabled first

communication process and the enabled second communication process, whereby the evacuees are virally identified within the confines of the muster point in an efficient and reliable manner.

5 [0010] According to yet another aspect of the present invention, there is provided a mustering system for use within the context of an emergency evacuation, the system comprising: a first computer readable medium having stored thereon a mobile application as characterized in the previous paragraph, and a second computer readable medium having stored thereon a software to be executed on a server, the software, when executed on the server, enables the server as a central mustering server and causes its server processor to
10 produce a list of missing persons for the search and rescue services by removing the midstream evacuee and downstream evacuee from a list of persons to be mustered as they are identified before the central mustering server.

Brief Description of the Drawings

15 [001] The invention will be better understood by way of the following detailed description of embodiments of the invention with reference to the appended drawings, in which:

[002] FIG. 1 is a top plan view of an evacuated building and an adjoining area in which evacuees are grouped around three distinct muster points;

20 [003] FIG. 2A is a top plan view of one of the groups of evacuees shown in FIG. 1, the group comprising a root emergency warden;

[004] FIG. 2B is a top plan view of the group of evacuees shown in FIG. 2A, the group comprising a root emergency warden and four deputy emergency wardens;

[005] FIG. 2C is a top plan view of the group of evacuees shown in FIG. 2A, the group comprising a root emergency warden and twenty deputy emergency wardens;

25 [006] FIG. 2D is a top plan view of the group of evacuees shown in FIG. 2A, the group comprising a root emergency warden and eighty-four deputy emergency wardens;

[007] FIG. 3 is a schematic block diagram illustrating a central mustering server;

[008] FIG. 4 is a schematic block diagram illustrating a client interface module of the central mustering server shown in FIG. 3;

[009] FIG. 5 is a flowchart illustrating the operation of the central mustering server shown in FIG. 3;

5 [0010] FIG. 6 is a flowchart illustrating the operation of a handheld computing device on which a mobile application is executed in identifying evacuees according to an embodiment of the invention;

[0011] FIG. 7 is a flowchart illustrating the operation of the handheld computing device on which the mobile application is executed in conducting a first transfer of information with
10 an emergency warden and initiating a first communication process over the course of which it provides to the central mustering an identifier of the evacuee to whom the handheld computing device belongs according to an embodiment of the invention;

[0012] FIG. 8 is a flowchart illustrating the operation of the handheld computing device on which the mobile application is executed in conducting a first transfer of
15 information with an emergency warden and initiating a first communication process over the course of which it provides to the root emergency warden an identifier of the evacuee to whom the handheld computing device belongs according to another embodiment of the invention;

[0013] FIG. 9 is a schematic block diagram illustrating the central mustering server, the
20 handheld computing device of an identified evacuee, and the handheld computing device of an evacuee in instance of identification communicating with one another according to flowchart shown in FIG. 7;

[0014] FIG. 10 is a schematic block diagram illustrating the central mustering server, the
25 handheld computing device of a root emergency warden, the handheld computing device of an identified evacuee, and the handheld computing device of an evacuee in instance of identification communicating with one another according to the flowchart shown in FIG. 8;

[0015] FIG. 11 is a schematic block diagram illustrating the devices shown in FIG. 10 communicating with one another to identify the evacuee in instance of identification before the central mustering server according to a hierarchical reporting scheme; and

[0016] FIG. 12 is a schematic block diagram of a server and a handheld computing device.

Detailed Description

[0017] The present invention relates to emergency evacuation tools, and more specifically, to methods and systems for identifying evacuees. Emergency procedures require that evacuees meet at a predetermined muster point located at a safe distance from the area to be evacuated. At the muster point, the evacuees are checked against a list of area occupants to identify and report the missing persons to the search and rescue services. The reporting of missing persons assists the search and rescue services in their onsite operations.

[0018] In the following, an occupant is a person physically located within a designated area and an evacuee is one that successfully evacuated the designated area. Referring to FIG. 1, there are shown a designated area in the form of a building 100, and three dense groups of evacuees assembled around three distinct muster points, each of which is located at a safe distance from the designated area: a group of evacuees 102, a group of evacuees 104, and a group of evacuees 106.

[0019] The method and system of the present invention provide for the identification of the members of the group of evacuees 102, the group of evacuees 104, and the group of evacuees 106 in a viral manner to accelerate the process by which the missing persons are identified and reported to the search and rescue services. As a result, emergency procedures are completed in a timely manner, which reduces costs and risks associated with real and simulated emergencies for all parties involved. The viral nature of the present invention is shown in FIG. 2A to FIG. 2D, each of which is a top plan view of the group of evacuees 102 taken at a different point in time.

[0020] FIG. 2A is a top plan view of the of the group of evacuees 102 taken right after one of its members, a predetermined emergency warden represented by a triangle, launches a

mobile application of the present invention on a handheld computing device, thereby initiating a process by which: (a) the predetermined emergency warden is identified before a central mustering server of the present invention; and (b) the handheld computing device is enabled as a mobile mustering station.

5 [0021] FIG. 2B is a top plan view of the of the group of evacuees 102 taken right after the predetermined emergency warden, now a root emergency warden, deputizes four evacuees represented by triangles, thereby establishing a first layer of deputy emergency wardens. In deputizing the four evacuees, the root emergency warden identifies them before the central mustering server and enables their handheld computing devices as mobile
10 mustering stations.

[0022] FIG. 2C is a top plan view of the of the group of evacuees 102 taken right after each member of the first layer deputizes four other evacuees represented by triangles, thereby establishing a second layer of deputy emergency wardens. In deputizing the sixteen evacuees, the first layer identifies them before the central mustering server and enables their
15 handheld computing devices as mobile mustering stations.

[0023] FIG. 2D is a top plan view of the of the group of evacuees 102 taken right after each member of the second layer deputizes four other evacuees represented by triangles, thereby establishing a third layer of deputy emergency wardens. In deputizing the sixty-four evacuees, the second layer identifies them before the central mustering server and enables
20 their handheld computing devices as mobile mustering stations.

[0024] FIG. 2A to FIG. 2D clearly illustrate the exponential growth attributable to the viral nature of the present invention as opposed to the linear growth achieved with prior art methods and systems. In FIG. 2A, there is shown no more than one identified evacuee, the predetermined emergency warden, whereas in FIG. 2D, there are shown no less than eighty-
25 five identified evacuees, namely the root emergency warden, the four deputy emergency wardens of the first layer, the sixteen deputy emergency wardens of the second layer, and the sixty-four deputy emergency wardens of the third layer.

[0025] According to an embodiment of the present invention, there is provided a mustering system comprising two computer readable media having stored thereon computer

programs to be executed on programmable processors. Each one of the computer-readable media can be any computer program product, apparatus, or device such as magnetic discs, optical disks, memory, and programmable logic devices used to provide machine instructions or data to a programmable processor. The computer programs can be any set of machine
5 instructions for a programmable processor and can be implemented in a high-level procedural language, in an objected-oriented language, in assembly or machine language, and in any combination thereof.

[0026] The first of the computer readable media has stored thereon a mobile application to be executed by evacuees on their handheld computing devices at a muster point located at
10 a safe distance from the evacuated area. The mobile application, when executed, enables the handheld computing devices to interact with one another, to interact with identification badges, and to capture biometric data such as fingerprints. A first example of an identification badge is a chip embedded in an object such as a smart card and on which is stored an identifier of the evacuee to whom it belongs. Another example of an identification
15 badge is an object on which is printed a code associated with an identifier of the evacuee to whom it belongs. In the latter example, the code can take the form of a QR code, a barcode, a Global Unique Identifier (GUID), or any other machine-readable code. As mentioned previously, the handheld computing device executing the mobile application is enabled to directly interact with evacuees for the purposes of viral identification. The mobile application
20 can be downloaded onto the handheld computing devices on demand from a service provider via an online marketplace such as the App StoreTM or Google PlayTM or from a server that specifically caters to the area's occupants via the Internet, a local area network, or a wide area network.

[0027] The second of the computer readable media has stored thereon a server program
25 to be executed on a remote server located at a safe distance from the designated area. The remote server can be stationary or portable. It can be a ready-made device, such as a smartphone, or one that is specifically designed to execute the server program. The server program, when executed, enables the remote server as a central mustering server that consolidates information provided by the handheld computing devices to produce reports for
30 the search and rescue services.

[0028] Referring now to FIG. 3, there is provided a schematic block diagram of a central mustering server 300 according to an embodiment of the present invention. The central mustering server 300 is in communication: with an alarm system 302 to detect emergency evacuations in real-time; with an access control system 304 to identify the occupants of the designated area; with handheld computing devices exemplified by an upstream device 306 and a midstream device 308 to identify evacuees; as well as with a search and rescue device 310 to provide reports listing the evacuees and the missing persons.

[0029] The alarm system 302 can be a ready-made system or one that is specifically designed to interact with the central mustering server 300. It can be installed in a closed area such as a residential, commercial, or industrial building, or in an open area such as a theme park or a zoo. It can be triggered automatically by onsite sensors or manually by actuators. When triggered, it emits an audio signal instructing occupants to evacuate the designated area, it provides an activation signal to the central mustering server 300, and it provides an emergency notification to the search and rescue services. A timestamp of the emergency evacuation and the geographical location of the designated area are optionally encoded in the activation signal. In one embodiment, the central mustering server 300 is connected to sensors configured to reliably distinguish the audio signal from ambient noise, and the activation signal consists in the emitted audio signal. In another embodiment, the alarm system 302 provides the emergency notification to the central mustering server 300 as the activation signal. In yet another embodiment, the alarm system 302 provides a distinct, customized activation signal to the central mustering server 300.

[0030] The access control system 304 can be a ready-made system or one that is specifically designed to interact with the central mustering server 300. It can be installed in a closed area such as a residential, commercial, or industrial building, or in an open area such as a theme park or a zoo. It can comprise an access control panel in communication with readers positioned at opposite sides of an access point as well as with a barrier mounted at the access point to prevent any intrusions. The access control panel is an electronic system configured to receive identifiers from the readers and to check the received identifiers against an access list. If the identifier belongs to a person on the access list, the access control panel unlocks the barrier and edits the access list to indicate whether the person entered or left the

area. Otherwise, the access control panel keeps the barrier locked. The barrier is a physical obstacle such as a locked door preventing an intruder from passing through the access point. The readers are devices such as keypads, smart card readers, and biometric readers configured to read identifiers uniquely associated with persons permitted to access the area.

- 5 The access control system 304 provides the access list to the central mustering server 300 as a muster list.

[0031] The handheld computing devices exemplified by the upstream device 306 and the midstream device 308 can be ready-made devices such as smart phones, tablets, and laptops, or customized ones specifically designed to communicate with one another and with the
10 central mustering server 300. Their weight and dimensions make them easy to carry during emergency evacuations. They are equipped: with a processor capable of executing the mobile application of the present invention; any combination of hardware and software required to communicate with one another over ranges no greater than five meters; and any combination of hardware and software required to communicate with the central mustering server 300. As
15 a first example, the handheld computing devices are equipped with an infrared LED, a diode photo-detector, and an amplifier to communicate with one another using infrared wireless technology. As a second example, the handheld computing devices are equipped with Radio-Frequency Identification (RFID) or Near-Field Communication (NFC) tags and readers to communicate with one another using RFID or NFC technologies. The same technology can
20 be used for reading chips embedded in objects belonging to evacuees, such as smart cards. As a third example, the handheld computing devices are equipped with QR code generators, QR code readers, and cameras of sufficient resolution to capture QR codes to communicate with one another using QR codes. The same technology can be used to capture QR codes printed on an object belonging to an evacuee. The camera can also be used to capture
25 biometric data such as high-resolution images of irises for instance. Alternatively or in addition, the handheld computing device can capture another type of biometric data, fingerprints, through a fingerprint sensor. In order to communicate with the central mustering server 300, the handheld computing devices can be equipped with Wi-Fi modem circuitry. The handheld computing devices communicate with one another to initiate processes by
30 which they are enabled as mobile mustering stations and the evacuees to whom they belong are identified before the central mustering server 300 in a viral manner.

[0032] The search and rescue device 310 can be a ready-made device or one specifically designed to communicate with the central mustering server 300. It can be a stationary system installed in the precinct of the search and rescue services and capable of wired or wireless communication with the central mustering server 300. Alternatively, it can be a handheld
5 computing device that search and rescue agents carry with them on site and capable of wireless communication with the central mustering server 300 such as smart phones, tablets, and laptops. The search and rescue device 310 submits requests to the central mustering server 300, which in turn provides one or more reports listing evacuees and missing persons. The reports enable the search and rescue services to determine whether any person has
10 remained in the designated area and needs to be rescued.

[0033] The central mustering server 300 has: a store of mustering data 312 configured to consolidate data acquired prior to, during, and following a specific emergency evacuation; an emergency module 314 configured to retrieve or generate emergency-specific data; a warden control module 316 configured to designate substitute emergency wardens; a client
15 interfacing module 318 configured to interact with the handheld computing devices; a mustered persons report generator 320 configured to generate reports listing the identified evacuees; and a missing persons report generator 322 configured to generate reports listing missing persons, wherein both reports are intended to assist the search and rescue services in their onsite operations.

[0034] The store of mustering data 312 can be any combination of one or more computer programs and electronic circuits configured to store data. It can be a relational database, a non-relational database, or any other type of structured and persistent memory that enables computer programs to query and edit its content. For instance, it can be a Microsoft® SQL server database. The content of the store of mustering data 312 comprises data pertaining to
25 the designated area itself, to the persons with access to the covered area, to the persons to be mustered, or occupants, and to the evacuees. It comprises the geographical location of the designated area, the name of the area's operator, and the names of the predetermined emergency wardens. For each person having access to the covered area, the content includes the person's name, a headshot, login credentials, and a designated muster point. For each
30 person to be mustered, or occupant, the content includes the person's name and a time of

entry into the designated area in the form of a timestamp. For each evacuee, the content comprises the evacuee's name and coordinates, the name of the emergency warden by whom the evacuee was identified before the central mustering server 300, the time at which the evacuee was identified in the form of a timestamp, and the place where the evacuee was identified in the form of a location stamp. The content also includes a GUID assigned to at least some of the aforementioned data items. It is important to note that while the content of the store of mustering data 110 has been described as comprising GUIDs, it can alternatively comprise identifiers of a different type. For instance, if the covered area is a commercial building, employee numbers can be used as identifiers of area occupants.

5 [0035] A GUID is a unique reference number used as an identifier in computer software. The term GUID typically refers to various implementations of the universally unique identifier (UUID) standard. GUIDs are usually stored as 128-bit values, and are commonly displayed as 32 hexadecimal digits with groups separated by hyphens, such as {21EC2020-3AEA-4069-A2DD-08002B30309D}. GUIDs generated from random numbers sometimes
15 contain 6 fixed bits saying they are random and 122 random bits; the total number of unique such GUIDs is 2^{122} (approximately 5.3×10^{36}). This number is so large that the probability of the same number being generated randomly twice is negligible. However, other GUID versions have different uniqueness properties and probabilities, ranging from guaranteed uniqueness to likely non-uniqueness. Assuming uniform probability for simplicity, the
20 probability of one duplicate would be about 50% if every person on earth as of 2012 owned 600 million GUIDs each.

[0036] The emergency module 314 is a combination of one or more computer programs and electronic circuits configured to retrieve or generate emergency-specific data. It is in wired or wireless communication with the alarm system 302, the access control system 304,
25 and the store of mustering data 312. Upon receiving an activation signal from the alarm system 302, the emergency module 314 generates a GUID specific to the emergency evacuation, retrieves a muster list, also referred to as the list of occupants or the list of persons to be mustered, from the access control system 304, and stores the generated GUID and retrieved list in the store of mustering data 312.

[0037] The warden control module 316 is a combination of one or more computer programs and electronic circuits configured to designate substitute emergency wardens when necessary. It is in wired or wireless communication with the alarm system 302 and the store of mustering data 312. After receiving an activation signal from the alarm system 302, the warden control module 316 queries the store of mustering data 312 to determine whether any of the predetermined emergency wardens are absent from the designated area. For each absentee, it queries the store of mustering data 312 to identify an occupant sharing the same muster point and designates the identified occupant as a substitute emergency warden before the store of mustering data 312. Furthermore, after a predetermined amount of time elapses from the moment it receives the activation signal, the warden control module 316 queries the store of mustering data 312 to determine whether any of the occupants that are either predetermined emergency wardens or substitute emergency wardens have remained on the muster list. For each missing occupant, it queries the store of mustering data 312 to identify another occupant sharing the same muster point and having logged into the central mustering server 300. If the query returns a hit, the warden control module 316 designates the identified occupant as a substitute emergency warden before the store of mustering data 312. Otherwise, the query is repeated until it returns a hit.

[0038] The mustered persons report generator 320 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the search and rescue device 310 and the store of mustering data 312. It is configured to receive a report request from the search and rescue device 310 and, in response to the received request, to retrieve from the store of mustering data 312 the evacuees' names, the names of the emergency wardens that identified them before the central mustering server 300, as well as the corresponding time and location stamps. From the retrieved data, it produces a report in the form of a tree diagram wherein each node represents an evacuee, and its parent node represents the corresponding emergency warden. The mustered persons report generator 320 transmits the produced report to the search and rescue device 310. While the mustered persons report generator 320 has been described as generating reports in the form of a tree diagram, it can alternatively generate reports presenting the data in a different manner, such as in the form of a map or a chronological list.

[0039] The missing persons report generator 322 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the search and rescue device 310 and the store of mustering data 312. It is configured to receive a report request from the search and rescue device 310 and, in response to the received request, to generate a blank missing persons report, to retrieve from the store of mustering data 312 the names of the persons to be mustered as well as the names of the evacuees, to add the names of the persons to be mustered to the blank missing persons report, and to remove from the missing persons report the names of the evacuees. Subsequently, for each one of the remaining names, it retrieves from the store of mustering data 312 the corresponding profile as well as the person's login time and location stamps, if any, and incorporates the retrieved data into the report to produce a complete version. The missing persons report generator 322 provides the complete version to the search and rescue device 310 in order to assist the search and rescue services in their onsite operations.

[0040] The client interface module 318 is configured to interact with the handheld computing devices over the course of a communication process by which they are enabled as mobile mustering stations and the evacuees to whom they belong are identified before the central mustering server 300. Referring now to FIG. 4, there is provided a schematic block diagram of the client interface module 318, which has: a login module 424 configured to process requests to log into the central mustering server 300; a registration module 430 configured to process requests to identify an evacuee before the central mustering server 300 and to enable a handheld computing device of the evacuee as a mobile mustering station; a validation module 426 configured to determine whether a specific emergency warden is entitled to identify the evacuee before the central mustering server 300; and a profile module 428 configured to process requests for additional information regarding the evacuee.

[0041] The login module 424 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the handheld computing devices and the store of mustering data 312. It is configured to receive login requests from the handheld computing devices, which requests comprise login credentials, and in response to the received requests, to query the store of mustering data 312 for the login credentials. If the query returns a hit, the login module 424 generates and stores a login timestamp as

associated with the corresponding evacuee in the store of mustering data 312. It also provides to the handheld computing device from which the login request was issued a login confirmation. However, if the query fails to return a hit, the login module 424 provides to the handheld computing device from which the login request was issued a login error notification. If the login module 424 recognizes the corresponding evacuee as one of the predetermined emergency wardens or one of the substitute emergency wardens, it provides a registration request to the registration module 430. The login module 424 is preferably capable of handling a sufficiently large number of login requests per unit of time to minimize the likelihood of a system failure, which could slow down the mustering process significantly

[0042] The validation module 426 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the handheld computing devices and the store of mustering data 312 to process validation requests. It is configured to receive validation requests from the handheld computing devices, which requests comprise the GUIDs of the emergency wardens as well as the GUIDs of the evacuees in instance of identification, and in response to the received requests, to query the store of mustering data 312 for the received GUIDs in order to determine: whether the received GUIDs are associated to persons sharing a common muster point; whether one of the received GUIDs is associated with an entry on the muster list; and whether the location stamp matches the common muster point, in which case it submits a profile request to the profile module 428. Otherwise, it returns a validation error message to the handheld computing device from which the validation request was issued, the validation error message providing a justification as to the failed validation attempt. More specifically, the validation error message indicates that the validation had been issued either with respect to a person absent from the muster list, with respect to a person that fails to share a common muster point with the emergency warden, or from a location other than the common muster point. The validation error message can also indicate the geographic location of the muster point from which the validation request should have been issued. In some embodiments, the validation requests are stored in the store of mustering data 312 should the evacuees fail to have themselves subsequently identified before the central mustering server 300 in a proper manner.

[0043] The profile module 428 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the handheld computing devices and the store of mustering data 312 to process requests for additional information regarding evacuees in instance of identification. It is configured to receive profile requests from the handheld computing devices, which requests comprise the GUIDs of the evacuees in instance of identification, and in response to the received requests, to retrieve the evacuees' profiles from the store of mustering data 312, and to transfer the retrieved profiles to the handheld computing devices for visual confirmation by the emergency wardens. The profile can, for instance, include the evacuees' full names, the departments to which they belong, and headshots.

[0044] The registration module 430 is a combination of one or more computer programs and electronic circuits in wired or wireless communication with the handheld computing devices and the store of mustering data 312 to process the identification of evacuees before the central mustering server 300. It is configured to receive from the handheld computing devices of the emergency wardens confirmations that the GUIDs of the evacuees in instance of registration are indeed the emergency wardens' interlocutors. The confirmations comprise the GUIDs of the emergency wardens as well as the GUIDs of the evacuees in instance of identification. Responsive to the received confirmation, the registration module 430 stores the received GUIDs in the store of mustering data 312, thereby identifying the evacuees and their respective emergency wardens before the central mustering server 300. It also generates and stores registration timestamps within the store of mustering data 312 as associated with the identified evacuees. Furthermore, it provides the handheld computing devices of the evacuees and respective emergency wardens with registration confirmations, or reg confirmations, which confirm the end of the communication process by which the evacuees are identified before the central mustering server 300 and their handheld computing devices are enabled as mobile mustering stations. The registration module 430 is also configured to receive registration requests, or reg request, from the login module 424 with respect to predetermined emergency wardens and substitute emergency wardens that have successfully logged into the central mustering server 300, the registration requests comprising the GUIDs of the corresponding emergency wardens. Responsive to the received registration requests, the registration module 430 stores the received GUIDs in the store of mustering data 312,

thereby identifying the corresponding emergency wardens before the central mustering server 300. It is also configured to generate and store registration timestamps within the store of mustering data 312 as associated with the identified emergency wardens and to provide the handheld computing devices from which the login requests had been issued with registration confirmations, namely ones confirming identification before the central mustering server 300 and enablement of the handheld computing devices as mobile mustering stations.

[0045] As mentioned previously, according to an embodiment of the present invention, there is provided a mustering system comprising two computer readable media, the first of which has stored thereon a server program to be executed on a server. When the server program is executed, it enables the server as the central mustering server 300. The second computer readable medium has stored thereon a mobile application to be executed by the evacuees on their handheld computing devices. The mobile application, when executed, enables each one of the handheld computing devices to communicate with the central mustering server 300. The handheld computing devices are exemplified by the upstream device 306 and the midstream device 308. The operation of the central mustering server 300 in identifying the evacuees in a viral manner according to an embodiment of the present invention is described herein below with reference to FIG. 3, FIG. 4, and FIG. 5.

[0046] When the alarm system 302 is triggered, it generates an activation signal. In a step 500, the emergency module 314 is provided with the activation signal through a push or pull mechanism over wired or wireless communication. The activation signal can, for instance, be an audio signal instructing occupants to evacuate the covered area, an emergency notification submitted to the search and rescue services, or another signal designed specifically for the purposes of the central mustering server 300.

[0047] In a step 502, the emergency module 314 is provided with a muster list from the access control system 304 through a push or pull mechanism, over wired or wireless communication, and stores the provided muster list in the store of mustering data 312. In some embodiments, the emergency module 314 pulls the muster list from the access control system 304 in response to the activation signal. In other embodiments, the access control system 304 pushes the muster list to the emergency module 314 upon being notified that the

alarm system 302 has been triggered. The muster list comprises the occupants' names, GUIDs, and times of entry. The muster list can be provided in the form of a Microsoft ExcelTM file, a Microsoft AccessTM file, or in any other machine-readable format. The emergency module 314 can store the muster list as provided in the store of mustering data 312, or alternatively, it can adapt the muster list according to the requirements of the store of mustering data 312 beforehand.

[0048] In a step 504, the emergency module 314, responsive to the activation signal, generates and stores a GUID specific to the emergency evacuation in the store of mustering data 312. The generated GUID serves the purpose of distinguishing within the store of mustering data 312 any content pertaining to the emergency evacuation from the remaining content. The remaining content of the store of mustering data 312 can, for instance, pertain to previous emergency evacuations. Keeping historical records of emergency evacuations can be useful for the purposes of measuring improvements or identifying weaknesses in implementing emergency procedures.

[0049] While the central mustering server 300 is performing the steps 500, 502, and 504, the occupants evacuate the designated area and meet as evacuees at one or more predetermined muster points. If the designated area is of modest capacity, its occupants may be directed to a same muster point. However, designated areas of larger capacity may call for a plurality of muster points, in which case evacuees would be directed to a specific one of the muster points as a function of one or more criterion. For instance, occupants of a residential building may be directed to different muster points as a function of their floor whereas those of a commercial building may be directed to different muster point depending on their employer. In some embodiments, a routing device is installed at the muster point to enable communication between the handheld computing devices and the central mustering server 300 over a Wi-Fi network. The routing device can be enabled by default, or alternatively, enabled only when the alarm system 302 is triggered. As soon as the occupants reach their muster point, they are required to launch the mobile application on their handheld computing devices and submit a login request to the login module 424.

[0050] In a step 506, the login module 424 receives a login request issued by the upstream device 306 and transmitted over wired or wireless communication. As mentioned

previously, the login request comprises the login credentials as well as the corresponding time and location stamps. The login credentials, which had been previously stored in the store of mustering data 312 as associated with the evacuee, can be in the form of a username and password generated by the evacuee or on behalf of the evacuee. For instance, in cases
5 where the designated area is a commercial building, the credentials may be the same as those used to log into workstations. Alternatively, the login credential may be in the form of biometric data such as fingerprints or iris patterns.

[0051] In a step 508, responsive to the login request, the login module 424 validates the login credentials by accessing the store of mustering data 312, in which are stored the login
10 credentials of all persons with access to the designated area. In some embodiments, the login module 424 validates the login credentials by submitting a query, and in others, it sequentially retrieves login credentials from the store of mustering data 312 and checks them against the evacuee's login credentials. If the login request comprises additional details regarding the evacuee such as a residence floor, the login module 424 can use the additional
15 details to narrow down its search within the store of mustering data 312. The login module 424 also determines whether the received login credentials are those of a predetermined or substitute emergency warden.

[0052] In a step 510, if the login module 424 determined that the received login credentials are invalid, it returns a login error message for display on the screen of the
20 upstream device 306. In some embodiments, the login error message is generic, and in others, it provides a justification. For instance, the login error message can indicate that the username has been recognized and provide instructions to retrieve the forgotten password. Alternatively, the login error message can indicate that the username has not been recognized and provide instructions to retrieve the username.

[0053] In a step 512, if the login module 424 determined that the received login credentials are valid, it generates and stores a login timestamp in the store of mustering data 312 as associated with the evacuee to whom the upstream device 306 belongs, namely the
25 upstream evacuee. In embodiments wherein the login request comprises corresponding time and location stamps generated by the upstream device 306, the login module 424 stores the
30 received stamps in the store of mustering data 312 as associated with the upstream evacuee.

The time and location stamps are particularly useful in cases where the upstream evacuee, for one reason or another, fails to subsequently register before the central mustering server 300 as they provide the search and rescue services with additional information as to the upstream evacuee's whereabouts.

5 [0054] In a step 514, and after storing a login timestamp in the store of mustering data 312 as associated with the upstream evacuee, the login module 424 provides a login confirmation for display on the screen of the upstream device 306. The login confirmation informs the upstream evacuee that the login request has been successfully processed and can, in some embodiments, comprise the login timestamp generated by the login module 424. The
10 login process provides for a more reliable mustering process as it decreases the likelihood that handheld computing devices such as the upstream device 306 are in the hands of anyone other than their rightful operators.

[0055] In a step 516, if the login module 424 previously determined that the received login credentials are those of a predetermined emergency warden or substitute emergency
15 warden, the upstream evacuee is identified before the central mustering server 300 and provided with a registration confirmation on the upstream device 306. More specifically, the login module 424 submits a registration request, or reg. request, to the registration module 430 on behalf of the upstream evacuee, the registration request comprising the GUID of the upstream evacuee. In response to the registration request, the registration module 430
20 generates and stores a registration timestamp as associated with the upstream evacuee in the store of mustering data 312, whereby the upstream evacuee is identified before the central mustering server 300. The registration confirmation is provided for display on the upstream device 306 as a notification: that the upstream evacuee has been identified before the central mustering server 300; that the upstream device 306 is enabled as a mobile mustering station;
25 and that as an emergency warden, the upstream evacuee may now identify others before the central mustering server 300.

[0056] Following the step 516, the upstream evacuee is entitled to act as an emergency warden with respect to other evacuees within the confines of the muster point by using the upstream device 306 as a mobile mustering station. One such evacuee is referred to herein
30 below as the midstream evacuee, whose handheld computing device is the midstream device

308. The upstream evacuee and the midstream evacuee select a same communication technology to be used by their respective devices for the purposes of transferring information. Thereafter, they bring their respective devices in proximity with one another to enable the information transfer, which can only take place within ranges no greater than five
5 meters. Once the information transfer is enabled and completed, a communication process is initiated to identify the midstream evacuee before the central mustering server 300 and enable the midstream device 308 as a mobile mustering station.

[0057] In the embodiment shown in FIG. 3 and FIG. 4, the information transfer consists in the transfer of the midstream evacuee's GUID from the midstream device 308 to the
10 upstream device 306. This information transfer initiates a communication process over the course of which the upstream device 306 submits a validation request to the central mustering server 300.

[0058] Referring back to FIG. 5, in a step 518, the validation module 426 is provided with a validation request over wired or wireless communication from the upstream device
15 306. The validation request comprises the GUID of the upstream evacuee, the GUID of the midstream evacuee, as well as a location stamp generated by the upstream device 306 for the purpose of identifying the geographical location in which the information transfer took place. The validation request serves the purpose of instructing the validation module 426 to determine whether the upstream evacuee is entitled to have the midstream evacuee identified
20 before the store of mustering data 312 at the geographical location in which the information transfer took place. This is because emergency wardens can only operate within the confines of their muster points; and with respect to evacuees in instance of identification before the central mustering server 300 that were assigned the same muster points.

[0059] In a step 520, the validation module 426, responsive to the provided validation
25 request, queries the store of mustering data 312 using the GUID of the upstream evacuee and the GUID of the midstream evacuee to determine: whether the upstream evacuee and midstream evacuee share a common muster point; whether the received location stamp matches the common muster point; and whether the midstream evacuee is on the muster list. If all three criteria are met, the validation module 426 determines that the upstream evacuee,
30 acting as an emergency warden, is indeed entitled to have the midstream evacuee identified

before the central mustering server 300 at the geographical location from which the validation request was issued. Otherwise, the validation module 426 determines that the upstream evacuee is not entitled to do so.

[0060] In a step 522, if the validation module 426 previously determined that the upstream evacuee is entitled to have the midstream evacuee registered before the store of mustering data 312 at the geographical location in which the information transfer took place, it submits a profile request to the profile module 428. The profile request comprises the GUID of the midstream evacuee and serves the purpose of instructing the central mustering server 300 to provide the upstream evacuee with additional information that may prove useful in confirming that the midstream evacuee is indeed the person holding the midstream device 308. This is particularly useful in situations where emergency wardens are not expected to know all persons assigned to their muster points.

[0061] In a step 524, the profile module 428, responsive to the profile request received from the validation module 426, queries the store of mustering data 312 using the GUID of the midstream evacuee to retrieve a corresponding profile, and provides the retrieved profile for display on the screen of the upstream device 306. The profile can, for instance, include the person's full name, the department to which the person belongs, headshots, and any other information that may assist the upstream evacuee in confirming that the midstream evacuee is indeed the person operating the midstream device 308.

[0062] After consulting the retrieved profile, if the upstream evacuee is unable to confirm that the midstream evacuee is indeed the person holding the midstream device 308, the upstream evacuee submits a request to cancel the communication process and moves on to another evacuee in instance of registration before the central mustering server 300. Otherwise, the upstream evacuee requests that an ID confirmation be issued. The upstream evacuee can submit any of the two aforementioned requests through the upstream device 306.

[0063] In a step 526, if the upstream evacuee previously submitted a request to issue an ID confirmation, the registration module 430 receives the ID confirmation from the upstream device 306. The ID confirmation comprises the GUID of the upstream evacuee as well as the

GUID of the midstream evacuee. Responsive to the received ID confirmation, the registration module 430 generates and stores a registration timestamp within the store of mustering data 312 as associated with the midstream evacuee, whereby the midstream evacuee is identified before the central mustering server 300.

5 [0064] In a step 516, the registration module 430 provides a registration confirmation for display on the upstream device 306. The registration confirmation confirms to the upstream evacuee: that the midstream evacuee has been identified before the central mustering server 300; that the midstream device 308 is enabled as a mobile mustering station; and that as an emergency warden, the midstream evacuee may now identify others before the central
10 mustering server 300. In some embodiments, the registration confirmation comprises the registration timestamp generated in the step 526.

[0065] In a step 530, if the validation module 426 previously determined that the upstream evacuee is not entitled to identify the midstream evacuee before the central mustering server 312 at the geographical location in which the information transfer took
15 place, it returns a validation error message to the upstream device 306, which validation error message comprises a justification as to the failed validation attempt. More specifically, the validation error message indicates that: the midstream evacuee is absent from the muster list; the midstream evacuee fails to share a common muster point with the upstream evacuee; or the information transfer took place outside the boundaries of the common muster point, in
20 which case it can provide an indication as to the geographical location of the boundaries.

[0066] An exemplary operation of the upstream device 306 and midstream device 308 in virally identifying evacuees is described herein below with reference to FIG. 3, FIG. 4, and FIG. 6, the latter presenting a flowchart of the operation. In a step 600, the upstream device 306 receives a request to launch the mobile application from the upstream evacuee. In some
25 embodiments, the upstream evacuee submits the request by clicking or tapping an icon displayed on the screen of the upstream device 306. In other embodiments, the evacuee submits the request by issuing a voice command. In yet another embodiment, the evacuee submits the request by bringing the upstream device 306 in proximity with an RFID or NFC chip programmed specifically for this purpose and accessible at the muster point.

[0067] In a step 602, once the mobile application is launched, it requests and receives the login credentials of the upstream evacuee. The login credentials can, for instance, be requested and received through a touch screen of the upstream device 306. In another embodiment, the login credentials can be received through a physical keyboard of the upstream device 306. In yet another embodiment, the login credentials are received in the form of fingerprints by a fingerprint sensor of the upstream device 306 or in the form of ocular patterns captured by a camera of the upstream device 306.

[0068] In a step 604, the upstream device 306 provides a login request to the login module 424 over wired or wireless communication. The login request comprises the login credentials of the evacuee and the corresponding time and location stamps, both of which are generated by the upstream device 306. In one embodiment of the present invention, the upstream device 306 generates the location stamp using its Global Positioning System (GPS). In another embodiment, it generates the location stamp by signal triangulation.

[0069] In a step 606, if the login module 424 determined that the received login credentials are invalid, the upstream device 306 receives a login error message for display on its screen. In some embodiments, the login error message is generic, and in others, it provides a justification as to the failed login attempt. As a first example, the login error message can indicate that the username has been recognized and provide instructions to retrieve the forgotten password. As a second example, the error message can indicate that the username has not been recognized and provide instructions to retrieve the username. As a third example, the error message can indicate that the provided biometric data fail to meet predetermined standards.

[0070] In a step 608, if the login module 424 previously determined that the received login credentials are valid, the upstream device 306 receives from the login module 424 a login confirmation for display on its screen. The login confirmation informs the upstream evacuee that the login request has been successfully processed. In some embodiments, the login confirmation comprises a login timestamp generated by the login module 424. The login process provides for a more reliable mustering process as it decreases the likelihood that handheld computing devices such as the upstream device 306 are in the hands of anyone other than their rightful operators.

[0071] In a step 610, if the login module 424 determined that the login credentials are valid and belonged to a root emergency warden, the upstream device 306 is provided with a registration confirmation for display on its screen. The registration confirmation indicates that: the upstream evacuee has been identified before the central mustering server 300; the upstream device 306 has been enabled as a mobile mustering station; and the upstream evacuee can act as an emergency warden with respect to other evacuees. For the purposes of the description herein below, the upstream evacuee will act as an emergency warden with respect to the midstream evacuee.

[0072] In a step 612, the upstream device 306 receives from the upstream evacuee a selection of a communication technology to be used in transferring information to or from the midstream device 308. The selected communication technology is restricted to ranges no greater than five meters. According to one embodiment, the selected communication technology is restricted to ranges no greater than two meters. According to another embodiment, the selected communication technology is restricted to ranges no greater than one meter.

[0073] In a step 614, the upstream device 306 is brought within proximity of the midstream device 308 to enable the transfer of information over the selected communication technology. For instance, if the selected communication technology provides for information transfers over ranges no greater than one meter, the upstream device 306 is to be brought within a distance no greater than one meter from the midstream device 308. The information transfer consists in receiving the GUID of the midstream evacuee from the midstream device 308.

[0074] In a step 616, the previous information transfer initiates a communication process over the course of which the upstream device 306 submits a validation request to the validation module 426, which in turn determines whether the upstream evacuee is entitled to identify the midstream evacuee before the central mustering server 300 at the geographical location of the information transfer. If the validation module 426 determines that the upstream evacuee is not entitled to do so, it provides a validation error message to the upstream device 306 for display on its screen. Otherwise, the validation module 426 submits a profile request to the profile module 428, which in turn retrieves the midstream evacuee's

profile and provides it to the upstream device 306 for display. After consulting the provided profile and recognizing that the midstream evacuee is indeed the person holding the midstream device 308, the upstream evacuee instructs the upstream device 306 to provide an ID confirmation to the registration module 430, which in turn generates and stores a registration timestamp within the store of mustering data 312 as associated with the midstream evacuee, whereby the midstream evacuee is identified before the central mustering server 300 and the midstream device 308 is enabled as a mobile mustering station.

[0075] In a step 618, the upstream device 306 receives a registration confirmation from the registration module 430 for display on its screen. The registration confirmation is provided for display on the upstream device 306 as a notification: that the midstream evacuee has been identified before the central mustering server 300; that the specific device 306 is enabled as a mobile mustering station; and that as an emergency warden, the midstream evacuee may now identify other evacuees before the central mustering server 300. In some embodiments, the registration confirmation comprises a registration timestamp generated by the registration module 430 over the course of the communication process.

[0076] It should be noted that while the steps 612 to 618 have been described as involving two handheld computing devices, one of which has been previously enabled as a mobile mustering station, they can alternatively involve a handheld computing device belonging to either one of an identified evacuee and an unidentified evacuee, and an identification badge bearing an identifier of the other, which identifier is readable by the handheld computing device, such as a smart card. This would prove practical for evacuees having none of their handheld computing devices. Identified evacuees can use their identification badges to identify other evacuees before the central mustering server 300. As a result, the viral identification of evacuees can be propagated not only by those of the evacuees having their handheld computing devices, but also by those having their identification badges.

[0077] It should be noted that while the steps 612 to 618 have been described as involving two handheld computing devices, one of which has been previously enabled as a mobile mustering station, they can alternatively involve no more than a handheld computing device belonging to either one of an identified evacuee and an unidentified evacuee, which

would read information from the other in the form of biometric identifiers such as fingerprints or iris patterns. This would prove practical for evacuees having none of their handheld computing devices or identification badges. Identified evacuees can act as emergency wardens by submitting their biometric data through the handheld computing devices of unidentified evacuees, which would trigger a communication process by which the unidentified evacuees are identified before the central mustering server 300 and the handheld computing devices are enabled as mobile mustering stations. As a result, the viral identification of evacuees can also be propagated by those that have neither one of their handheld computing devices and identification badges.

[0078] It is also important to note that should an evacuee have no handheld computing devices or identification badges such as the smart card 332, the mobile application presents a manual entry feature that enables the emergency warden to request for an electronic form to be displayed on the screen of the mobile mustering station, which form can be filled out by either one of the emergency warden and the evacuee in instance of registration. In some embodiments, the manual entry of the identifier of the evacuee in instance of registration within the electronic form serves as the transfer of information that initiates a communication process by which the evacuee is to be identified before the store of mustering data 312.

[0079] If the login module 424 determined that the login credentials are not those of an emergency warden, the upstream evacuee can, for instance, interact with a mobile mustering station through the upstream device 306 in order to be identified before the central mustering server 300. In a step 620, the upstream device 306 receives from the upstream evacuee a selection of a communication technology to be used in transferring information to or from the mobile mustering station. In a step 622, the upstream device 306 is brought into proximity with the mobile mustering station for a transfer of information to take place using the selected communication technology. The information transfer consists in the transfer of the GUID of the upstream evacuee from the upstream device 308 to the mobile mustering station. The exchange of information initiates the communication process in the step 616, which leads to the identification of the upstream evacuee before the central mustering server 300 and the enablement of the upstream device 306 as a mobile mustering station. In the step 618, the upstream device 306 receives a registration confirmation for display on its screen.

[0080] The steps 612 to 618 can be performed recursively as other handheld computing devices become enabled as mobile mustering stations, which leads to a proliferation of mobile mustering stations across highly dense crowds. This provides for expeditious mustering in comparison with prior art solutions, which typically require that the dense
5 crowds be organized into line-ups behind predetermined mustering stations. Also, use of short-range (e.g. RFID, NFC) rather than longer range (e.g. Wi-Fi, SMS) communication technologies for information transfers enable evacuees to establish a tighter human chain, which provides for greater reliability as it reduces the likelihood that occupants report themselves from the designated area and provides emergency wardens with the opportunity
10 to visually recognize other evacuees before having them identified.

[0081] While in some embodiments, a same handheld computing device or identification badge can be used to identify an unlimited number of evacuees before the central mustering server 300, in other embodiments, it can be used to identify no more than a predetermined number of evacuees, thereby minimizing the likelihood that identified evacuees forget one or
15 more of the unidentified evacuees for whom they acted as emergency wardens.

[0082] While the transfer of information between the upstream device 306 and the midstream device 308 has been described as consisting in the transfer of the GUID of the midstream evacuee from the latter device to the former, it can alternatively consist in transfers of other types of information, or transfers directed from the former device to the
20 latter. For instance, according to one embodiment, the transfer of information consists in the transfer of the emergency GUID from the upstream device 306 to the midstream device 308.

[0083] While the communication process initiated by the information transfer has been described as the series of communications between the upstream device 306, the store of mustering data 312, the validation module 426, the profile module 428, and the registration
25 module 430, it can alternatively consist in a different series of communications. For instance, the communication process can consist in a transfer of a GUID of the midstream evacuee from the midstream device 308 to the registration module 430.

[0084] The communication process has been described as providing measures to reduce the likelihood of false reports such as the requirement that the emergency warden be logged

into the central mustering server 300 as well as the requirement that the emergency warden confirm the identity of the evacuee prior to identifying the evacuee before the central mustering server 300. However, in other embodiments, the communication process is streamlined by dispensing with such measures.

5 [0085] While the central mustering server 300 has been described as retrieving the muster list from the access control system 304, it can alternatively, be generated from one or more data sources comprising: presence registers kept by the covered area's operator; ad-hoc sweeps of the covered area prior to the emergency via communication technologies such as Bluetooth™ or RFID; access control systems; and devices interfacing with access control
10 systems.

[0086] While the method of virally identifying evacuees at a muster point has been described as initiated by predetermined emergency wardens, it can alternatively be initiated by ad-hoc emergency wardens, in which case the central mustering server 300 would not comprise the warden control module 316 and the content of the store of mustering data 312
15 would not include the names of predetermined emergency wardens. For instance, in some embodiments, each one of the muster points is equipped with a stationary mustering station, which can be in the form of a visible and accessible RFID chip mounted on a stationary structure. In the absence of emergency wardens at the muster point, an evacuee can identify himself before the central mustering server 300 using the stationary mustering station, at
20 which point he becomes deputized as an emergency warden, and initiate the method of virally identifying evacuees at the muster point.

[0087] The invention has been described within the context of an evacuation to a plurality of muster points. The scattering of evacuees across multiple locations is in some cases required, if only to comply with jurisdictional regulations, and in others, desirable,
25 especially if no single location within the immediate surroundings of the designated area is of sufficient capacity to accommodate the area's occupants. Nevertheless, the invention can be applied within the context of an evacuation that calls for no more than one muster point, in which case all evacuees would meet at a same, predetermined location. In the latter context, the validation module 426 would not have to be configured to verify whether the received
30 GUIDs are associated with persons sharing a common muster point.

[0088] In the described embodiments, the midstream device 308 provides the GUID of the midstream evacuee, who is in instance of registration, to the upstream device 306, which had been previously enabled as a mobile mustering station, and the upstream device 306 provides the received GUID to the central mustering server 300. However, the GUID of the midstream evacuee can be transferred from the midstream device 308 to the central mustering server 300 through different paths. For instance, in one embodiment, the midstream device 308 transfers the GUID directly to the central mustering server 300 over the Internet or a local area network. Referring now to FIG. 9, there are shown the upstream device 306, the midstream device 308, and the central mustering server 300, wherein the midstream device 308 transfers the GUID of the midstream evacuee directly to the central mustering server 300. This particular communication path is reflected in the flowchart presented in FIG. 7, which illustrates the transfers of information between the upstream device 306, enabled as a mobile mustering station, the midstream device 308 of the midstream evacuee in instance of registration, and the central mustering server 300. In a step 700, the midstream device 308 receives an initiation signal from the upstream device 306 such as, for instance, the emergency GUID, in response to which in a step 702, the midstream device 308 provides the GUID of the midstream evacuee to the central mustering server 300. In return, in a step 804, the midstream device 308 receives from the central mustering server 300 a registration confirmation for display on its screen, which confirmation notifies the midstream evacuee that: the midstream evacuee is identified before the central mustering server 300; and the midstream device 308 is enabled as a mobile mustering station.

[0089] In another embodiment, the midstream device 308 transfers the GUID of the midstream evacuee directly to the root mobile mustering station, namely the mobile mustering station that initiated the viral identification of evacuees at the mustering point. In turn, the root mobile mustering station provides the received GUID to the central mustering server 300. In the latter embodiment, the midstream device 308 can, for instance, transfer the GUID of the midstream evacuee to the root mobile mustering station over SMS technology. Referring now to FIG 10, there are shown the upstream device 306, the midstream device 308, a root mobile mustering station 1000, and the central mustering server 300, wherein the midstream device 308 transfers the midstream evacuee's GUID directly to the root mobile

mustering station 1000. This particular communication path is reflected in the flowchart presented in FIG. 8, which illustrates the exchange of information between the upstream device 306, enabled as a mobile mustering station, the midstream device 308, and the root mobile mustering station 1000. In a step 800, the midstream device 308 receives an initiation signal from the upstream device 306 such as, for instance, the emergency GUID, in response to which in a step 802, the midstream device 308 provides the GUID of the midstream evacuee to the root mobile mustering station 1000 through, for instance SMS messaging. In return, in a step 804, the midstream device 308 receives from the root emergency warden 900 a registration confirmation for display on its screen, which confirmation notifies the midstream evacuee that: the midstream evacuee is identified before the central mustering server 300; and the midstream device 308 is enabled as a mobile mustering station.

[0090] In yet another embodiment, the midstream device 308 does not transfer the GUID of the midstream evacuee directly to the root mobile mustering station 1000, but rather by a sequence of upstream transfers that reaches the root mobile mustering station 1000, which in turn transfers the received GUID to the central mustering server 300. In the latter embodiment, the upstream transfers can, for instance, take place over an ad-hoc BluetoothTM network created over the course of the viral proliferation of mobile mustering stations. Referring now to FIG 11, there are shown the upstream device 306, the midstream device 308, a root mobile mustering station 1000, and the central mustering server 300, wherein the midstream device 308 transfers the GUID of the midstream evacuee to the upstream device 306, which in turn transfers the same to the root mobile mustering station 1000.

[0091] While the ID confirmation has been described as comprising the GUID of the upstream evacuee as well as the GUID of the midstream evacuee, it can also comprise other data such as a photograph and health status of the midstream evacuee as provided by the upstream evacuee. The health status can, for instance, be in the form of a numerical value on a scale from 1 to 5, where 1 can mean healthy, 5 can mean unconscious or dead, and mid-values indicate various degrees of injuries according to a pre-established definition customized to each site's characteristics and requirements. The registration module 430 stores the photograph and health status as associated with the midstream evacuee within the

store of mustering data 312. The mustered persons report generator 320 produces reports incorporating the stored photograph and health status.

[0092] While data transfers between the central mustering server 300 and the handheld computing devices have been described as taking place over networks based on longer-range technologies such as Wi-Fi, they can alternatively take place over technologies such as BluetoothTM and NFC. In some embodiments, the server program is executed on the handheld computing device of the root emergency warden for enablement as the central mustering server 300. At the muster point, the handheld computing device of the root emergency warden communicates with the handheld computing devices of the other evacuees as the central mustering server 300. It does so over an ad-hoc network created over the course of the viral proliferation of mobile mustering stations and based on technologies such as BluetoothTM and NFC. The root emergency warden provides a copy of the compiled information to the search and rescue services upon their arrival. This is particularly useful in environments less suited for longer-range technologies such as oil facilities in war zones, where a minimum network infrastructure (antennas, routing devices, etc.) cannot be easily installed and maintained operational on site.

[0093] FIG. 12 shows an example of a server 1200 and a handheld computing device 1250, which may be used to implement the processes described herein. The server 1200 is intended to represent various forms of servers. The handheld computing device 1250 is intended to represent various forms of devices such as personal digital assistants, cellular telephones, smartphones, and other similar computing devices. The components shown here, their connections, their relationships, and their functions, are meant to be exemplary only, and are not meant to limit implementations of the present invention. For the purposes of clarity, the server program can, for instance, be executed on either one of the server 1200 and the handheld computing device 1250 to enable the corresponding device as the central mustering server 300.

[0094] The server 1200 has a processor 1202, memory 1204, a storage device 1206, a high-speed interface 1208, high-speed expansion ports 1210, a low speed interface 1212, and a low speed bus 1214 interconnected using various busses and mounted on a common motherboard. The processor 1202 can process instructions for execution within the server

1200, including instructions stored in the memory 1204 or on the storage device 1206 to display graphical information for a GUI on an external input/output device, such as a display coupled to the high-speed interface 1208. In other implementations, multiple processors and multiple busses may be used as appropriate, along with multiple memories of different types.

5 Also, the server 1200 may comprise multiple servers connected with one another and dedicated to a subset of the operations. In some embodiments, the server 1200 is located in a cloud platform such as Microsoft AzureTM.

[0095] The memory 1204 can be volatile or non-volatile. The storage device 1206 is capable of providing mass storage for the server 1200. In one implementation, the storage
10 device 1206 may be or contain a computer-readable medium, such as a floppy disk device, a hard disk device, an optical disk device, or a tape device, a flash memory or other similar solid state memory device, or an array of devices, including devices in a storage area network. A computer program can be tangibly embodied in an information carrier and contain instructions which, when executed, perform one or more methods, such as those
15 described above. The information carrier may be a non-transitory computer-readable or machine-readable storage medium, such as the memory 1204, the storage device 1206, or memory in the processor 1202.

[0096] The high-speed controller 1208 manages bandwidth-intensive operations for the server 1200, while the low-speed controller 1212 manages lower bandwidth-intensive
20 operations. In one implementation, the high-speed controller 1208 is coupled to the memory 1204, to the display through, for instance, a graphics processor or accelerator, and to the high-speed expansion ports 1210, which may accept various expansion cards. The low-speed controller 1212 is coupled to the storage device 1206 and low-speed expansion port 1210. The low-speed expansion port 1212, which may include various communication ports such
25 as ones configured for USB, BluetoothTM, Ethernet, and wireless Ethernet communications, may be coupled to one or more input/output devices, such as a keyboard, a pointing device, a scanner, and a networking device such as a switch or router through a network adapter.

[0097] The handheld computing device 1250 includes a processor 1252, memory 1254, a display 1256, a communication interface 1258, a transceiver 1260 among other components,
30 interconnected using various busses and mounted on a common motherboard. The handheld

computing device 1250 can also have a storage device, such as a micro-drive or other device, to provide additional storage.

[0098] The processor 1252 is configured to execute instructions stored in the memory 1254. It can be implemented as a single chip, or alternatively, as a chipset that includes
5 separate and multiple analog and digital processors. The processor 1252 may provide, for example, for coordination of the other components of the handheld computing device 1250, such as control of user interfaces, applications run by the handheld computing device 1250 and wireless communication by the handheld computing device 1250.

[0099] The processor 1252 may communicate with a user through a control interface
10 1262 and a display interface 1264 coupled to the display 1256. The display 1256 may be a TFT LCD (Thin-Film-Transistor Liquid Crystal Display), an OLED (Organic Light Emitting Diode) display, or any other appropriate display technology. The display interface 1264 may comprise appropriate circuitry for driving the display 1256 to present graphical information to a user. The control interface 1262 may receive commands from a user and convert them
15 for submission to the processor 1252. In addition, an external interface 1266 may be provided in communication with the processor 1252, so as to enable near field communication of the handheld computing device 1250 with other devices. The external interface 1266 may provide, for example, for wired communication in some implementations, or for wireless communication in other implementations, and multiple
20 interfaces may also be used.

[00100] The memory 1254 stores information within the handheld computing device 1250. It can be implemented as one or more of a computer-readable medium or media, a volatile memory unit or units, or a non-volatile memory unit or units. Expansion memory 1268 may also be provided and connected to the handheld computing device 1250 through an
25 expansion interface 1270, which may include, for example, a SIMM (Single In Line Memory Module) card interface. The expansion memory 1268 may provide extra storage space for the handheld computing device 1250, or may also store applications or other information for the handheld computing device 1250. Specifically, the expansion memory 1268 may include instructions to carry out or supplement the processes described above, and may include
30 secure information also. Thus, for example, the expansion memory 1268 may be provided as

a security module for the handheld computing device 1250 and may be programmed with instructions that permit secure use of the handheld computing device 1250. In addition, secure applications may be provided via the SIMM cards, along with additional information, such as placing identifying information on the SIMM card in a secure manner.

5 [00101] The memory may include, for example, flash memory and/or NVRAM memory, as discussed below. In one implementation, a computer program product is tangibly embodied in an information carrier. The computer program product contains instructions that, when executed, perform one or more methods, such as those described herein below. The information carrier is a computer-readable medium or machine-readable medium, such
10 as the memory 1254, the expansion memory 1268, memory embedded in the processor 1252, or a propagated signal that may be received, for example, over the transceiver 1260 or the external interface 1266.

[00102] The handheld computing device 1250 may communicate wirelessly through the communication interface 1258, which may include digital signal processing circuitry where
15 necessary. The communication interface 1258 may provide for communications under various modes or protocols, such as GSM voice calls, SMS, EMS, or MMS messaging, CDMA, TDMA, PDC, WCDMA, CDMA2000, or GPRS, among others. Such communication may occur, for example, through the transceiver 1260. Also, communication may occur through a BluetoothTM transceiver 1272, a Wi-Fi transceiver 1274, an NFC
20 transceiver 1276, or other such transceivers. In addition, a GPS (Global Positioning System) receiver module 1278 may provide additional navigation-related and location-related wireless data to the handheld computing device 1250, which may be used as appropriate by mobile applications running on the handheld computing device 1250.

[00103] The handheld computing device 1250 may also communicate audibly using an
25 audio codec 1280, which may receive spoken information from a user and convert it to usable digital information. The audio codec 1280 may likewise generate audible sounds for a user through, for instance, a speaker of the handheld computing device 1250. Such sounds may include sounds generated during telephone calls, recorded sounds (e.g. voice messages and music files), as well as sounds generated by mobile applications running on the handheld
30 computing device 1250.

What is claimed is:

1. A recursive method of virally identifying evacuees at a muster point within the context of an emergency evacuation, said recursive method comprising:

bringing an emergency warden and a midstream one of said evacuees in close proximity with one another to enable a handheld computing device of one of said emergency warden and said midstream evacuee to read information from another one of said emergency warden and said midstream evacuee;

enabling said handheld computing device to read said information;

reading said information by said handheld computing device to enable an identification of said midstream evacuee before a central mustering server;

providing an identifier of said midstream evacuee to said central mustering server, whereby said midstream evacuee is enabled to act as said emergency warden with respect to another one of said evacuees; and

performing said recursive method wherein said midstream evacuee acts as said emergency warden and said another evacuee acts as said midstream evacuee,

whereby said evacuees are virally identified within the confines of said muster point in an efficient and reliable manner.

2. The method of claim 1 further comprising displaying a confirmation of said providing said identifier to at least one of said emergency warden and said midstream evacuee.

3. The method of any one of claims 1-2 wherein said enabling said handheld computing device comprises establishing a Near-Field Communication (NFC) connection between said handheld computing device and an NFC chip on which said information is stored.

4. The method of any one of claims 1-3 wherein said providing said identifier to said central mustering server is performed by at least one of said emergency warden and said midstream evacuee.

5. The method of claim 4 wherein said providing said identifier to said central mustering server is performed by said midstream evacuee.

6. The method of any one of claims 1-5 further comprising displaying a profile of said midstream evacuee to said emergency warden and receiving a confirmation from said
5 emergency warden that said profile matches said midstream evacuee before said providing said identifier to said central mustering server.

7. The method of any one of claims 1-6 wherein said information is said identifier, and said handheld computing device belongs to said emergency warden.

8. The method of any one of claims 1-7 wherein said identifier is provided to said central
10 mustering server over a local area network.

9. The method of any one of claims 1-3 further comprising providing said identifier of said midstream evacuee to the root emergency warden, wherein said root emergency warden is the person having initiated the viral identification of said evacuees, and said providing said identifier of said midstream evacuee to said emergency warden is performed by said root
15 emergency warden.

10. The method of claim 9 wherein said providing said identifier of said midstream evacuee is performed over Short Message Service (SMS) communication.

11. The method of any one of claims 1-10 wherein said enabling said handheld computing device to read said information comprises receiving login credentials from at least one of
20 said emergency warden and said midstream evacuee, and validating said login credentials.

12. The method of any one of claims 1-11 wherein said enabling said handheld computing device to read said information comprises receiving from at least one of said emergency warden and said midstream evacuee a selection of a communication technology, wherein said reading said information is performed over said communication technology.

25 13. The method of any one of claims 1-12 further comprising:

receiving instructions from said emergency warden to display an electronic form on said handheld computing device for manual entry of an identifier of one of said evacuees;

displaying said electronic form on said handheld computing device;
receiving said manual entry through said electronic form; and
providing said manually entered identifier to said central mustering server.

5 14. The method of any one of claims 1-13 further comprising providing an identifier of said emergency warden to said central mustering server as the person by whom said midstream evacuee was identified.

10 15. The method of any one of claims 1-14 further comprising determining a geographical location where said reading said information took place and providing said geographical location to said central mustering server as the location where said reading said information took place.

16. The method of claim 15 wherein said determining said geographical location is performed using a Global Positioning System (GPS).

15 17. The method of any one of claims 1-16 wherein said emergency warden is prevented from identifying more than a predetermined number of said evacuees before said central mustering server.

20 18. A computer readable medium having stored thereon a mobile application to be executed within the context of an emergency evacuation at a muster point by evacuees on their handheld computing devices, said mobile application, when executed by a midstream one of said evacuees on a midstream one of said handheld computing devices, causes said midstream handheld computing device's processor to:

conduct a first transfer of information with an emergency warden to enable a first communication process by which said midstream evacuee is identified before a central mustering server, said first transfer of information being enabled by bringing said midstream evacuee and said emergency warden in close proximity with one another;

25 conduct a second transfer of information with a downstream one of said evacuees after said midstream evacuee is identified before said central mustering server to enable a second communication process by which said downstream evacuee is identified before said central

mustering server, said second exchange of information being enabled by bringing said midstream evacuee and said downstream evacuee in close proximity with one another; and initiate at least one of said enabled first communication process and said enabled second communication process,

- 5 whereby said evacuees are virally identified within the confines of said muster point in an efficient and reliable manner.

19. The computer readable medium of claim 18 wherein said processor is further caused to display on said specific handheld computing device at least one of: a confirmation that said midstream evacuee is identified before said central mustering server; and a confirmation that
10 said downstream evacuee is identified before said central mustering server.

20. The computer readable medium of any one of claims 18-19 wherein said processor is caused to establish an NFC connection with an NFC chip, and one of said first transfer of information and said second transfer of information is performed over said NFC connection.

21. The computer readable medium of any one of claims 18-20 wherein said processor is
15 caused to receive an identifier of said downstream evacuee, and over the course of said second communication process, provide said received identifier to said central mustering server.

22. The computer readable medium of claim 21 wherein said processor is caused to provide said received identifier to said central mustering server over a local area network.

20 23. The computer readable medium of any one of claims 18-20 wherein said processor is caused to receive an identifier of said downstream evacuee, and over the course of said second communication process, said processor is caused to:

display said identifier on said midstream handheld computing device; and

receive a confirmation from said midstream evacuee that said identifier matches said
25 downstream evacuee to enable an identification of said downstream evacuee before said central mustering server.

24. The computer readable medium of any one of claims 18-23 wherein said processor is caused to perform at least one of: providing an identifier of said midstream evacuee to said emergency warden over the course of said first transfer of information; and receiving an identity of said downstream evacuee from said downstream evacuee over the course of said second transfer of information.

25. The computer readable medium of any one of claims 18-20 wherein said processor is caused to provide an identifier of at least one of said midstream evacuee and said downstream evacuee over the course of at least one of said first communication process and said second communication process to the root emergency warden, said root emergency warden being the person having initiated the viral identification of said evacuees.

26. The computer readable medium of claim 25 wherein said processor is caused to provide said identifier to said root emergency warden over Short Message Service (SMS) communication.

27. The computer readable medium of any one of claims 18-26 wherein said processor is further caused to receive login credentials of said midstream evacuee and initiate a validation of said credentials before said first transfer of information.

28. The computer readable medium of any one of claims 18-27, wherein said processor is further caused to receive a selection of a communication technology from said midstream evacuee, and at least one of said first transfer of information and said second transfer of information is performed over said communication technology.

29. The computer readable medium of any one of claims 18-28, wherein said processor is further caused to:

receive instructions from said midstream evacuee to display an electronic form for manual entry of an identifier of one of said evacuees;

display said electronic form on said midstream handheld computing device;

receive said manual entry through said electronic form; and

initiate a communication process by which said manually entered identifier is provided to said central mustering server.

30. The computer readable medium of any one of claims 18-29 wherein said second communication process is one by which an identifier of said midstream evacuee is provided to said central mustering server as the person by whom said downstream evacuee was identified.

31. The computer readable medium of any one of claims 19-30 wherein said processor is caused to determine a geographical location where at least one of said first transfer of information and said second transfer of information took place, and a corresponding one of said first communication process and said second communication process comprises providing said geographical location to said central mustering server.

32. The computer readable medium of claim 31 wherein said processor is caused to determine said geographical location using a GPS of said specific midstream handheld computing device.

33. The computer readable medium of any one of claims 18-32 wherein said processor is further caused to have no more than a predetermined number of said downstream evacuee identified before said central mustering server.

34. A mustering system for use within the context of an emergency evacuation, the system comprising:

the computer readable medium of claim 18; and

a computer readable medium having stored thereon a software to be executed on a server, said software, when executed on said server, enables said server as a central mustering server and causes its server processor to produce a list of missing persons for the search and rescue services by removing said midstream evacuee and said downstream evacuee from a list of persons to be mustered as they are identified before said central mustering server.

35. The mustering system of claim 34 wherein said server processor is further caused to retrieve said list of persons to be mustered from an Access Control System of the area being evacuated.

5 36. The mustering system of any one of claims 34-35 wherein said server processor is caused to receive an activation signal from an alarm system covering said area when said alarm system is triggered, and retrieve said list of persons to be mustered in response to said activation signal.

10 37. The mustering system of any one of claims 34-36 wherein said server processor is caused to produce a list of evacuees for the search and rescue services from said midstream evacuee and said downstream evacuee after they are identified before said central mustering server.

38. The mustering system of claim 37 wherein:

said computer readable medium of claim 18 is the computer readable medium of claim 30; and

15 said server processor is caused to record on said list of evacuees said midstream evacuee as the person by whom said downstream evacuee was identified before said central mustering server.

20 39. The mustering system of claim 38 wherein said server processor is caused to produce said list of evacuees in the form of a tree diagram illustrating said viral identification of said evacuees, said midstream evacuee being represented by a node, and said downstream evacuee being represented by a corresponding child node.

40. The mustering system of any one of claims 34-39 wherein said server processor is caused to validate that said midstream evacuee can be identified before said central mustering server at the geographical location of said first transfer of information by said emergency warden prior to removing said midstream evacuee from said list of persons to be mustered.

25 41. The mustering system of claim 40 wherein if said midstream evacuee cannot be identified before said central mustering server at said geographical location by said

emergency warden, said server processor is caused to provide said midstream handheld computing device with an error message.

42. The mustering system of any one of claims 34-41 wherein:

5 said computer readable medium of claim 18 is the computer readable medium of claim 27;
and

said server processor is caused to validate said login credentials, provide said midstream handheld computing device with a login confirmation if said login credentials are valid, and provide said midstream handheld computing device with a login error if said login credentials are invalid.

10 43. The mustering system of claim 42, wherein said server processor is caused to generate a timestamp for said login confirmation and record said timestamp as associated with said midstream evacuee.

15 44. The mustering system of any one of claims 42-43, wherein said server processor is caused to determine whether said login credentials belong to a predetermined emergency warden or a substitute emergency warden, in which case said server processor is caused to remove the person to whom said login credentials belong from said list of persons to be mustered.

20 45. The mustering system of any one of claims 34-44 wherein said server processor is caused to determine that a predetermined emergency warden is absent and designate another one of said evacuees as a substitute emergency warden.

46. The mustering system of any one of claims 34-45 wherein said server processor is caused to receive a status request from a device operated by said search and rescue services and provide the most recent version of said list of missing persons in response to said status request.

AMENDED CLAIMS

received by the International Bureau on 21 April 2017 (21.04.17)

What is claimed is:

1. A recursive method of virally identifying evacuees at a muster point within the context of an emergency evacuation, said recursive method comprising:

bringing an emergency warden and a midstream one of said evacuees in close proximity with one another to enable a handheld computing device of one of said emergency warden and said midstream evacuee to read information from the other one of said emergency warden and said midstream evacuee;

enabling said handheld computing device to read said information;

reading said information by said handheld computing device to enable an identification of said midstream evacuee before a central mustering server;

providing an identifier of said midstream evacuee to said central mustering server, whereby said midstream evacuee is enabled to act as said emergency warden with respect to another one of said evacuees; and

performing said recursive method wherein said midstream evacuee acts as said emergency warden and said another evacuee acts as said midstream evacuee,

whereby said evacuees are virally identified within the confines of said muster point in an efficient and reliable manner.

2. The method of claim 1 further comprising displaying to at least one of said emergency warden and said midstream evacuee a confirmation of said providing said identifier.

3. The method of any one of claims 1-2, wherein said enabling said handheld computing device comprises establishing a Near-Field Communication (NFC) connection between said handheld computing device and an NFC chip on which said information is stored.

4. The method of any one of claims 1-3, wherein said providing said identifier to said central mustering server is performed by at least one of said emergency warden and said midstream evacuee.

5. The method of claim 4, wherein said providing said identifier to said central mustering server is performed by said midstream evacuee.
6. The method of any one of claims 1-5, further comprising displaying a profile of said midstream evacuee to said emergency warden and receiving a confirmation from said
5 emergency warden that said profile matches said midstream evacuee before said providing said identifier to said central mustering server.
7. The method of any one of claims 1-6, wherein said information is said identifier, and said handheld computing device belongs to said emergency warden.
8. The method of any one of claims 1-7, wherein said identifier is provided to said central
10 mustering server over a local area network.
9. The method of any one of claims 1-3, further comprising providing said identifier of said midstream evacuee to the root emergency warden, wherein said root emergency warden is the person having initiated the viral identification of said evacuees, and said providing said identifier of said midstream evacuee to said emergency warden is performed by said root
15 emergency warden.
10. The method of claim 9, wherein said providing said identifier of said midstream evacuee is performed over Short Message Service (SMS) communication.
11. The method of any one of claims 1-10, wherein said enabling said handheld computing device to read said information comprises receiving login credentials from at least one of
20 said emergency warden and said midstream evacuee, and validating said login credentials.
12. The method of any one of claims 1-11, wherein said enabling said handheld computing device to read said information comprises receiving from at least one of said emergency warden and said midstream evacuee a selection of a communication technology, wherein said reading said information is performed over said communication technology.
- 25 13. The method of any one of claims 1-12, further comprising:

receiving instructions from said emergency warden to display an electronic form on said handheld computing device for manual entry of an identifier of one of said evacuees;

displaying said electronic form on said handheld computing device;

receiving said manual entry through said electronic form; and

providing said manually entered identifier to said central mustering server.

14. The method of any one of claims 1-13, further comprising providing an identifier of said
5 emergency warden to said central mustering server as the person by whom said midstream
evacuee was identified.

15. The method of any one of claims 1-14, further comprising determining a geographical
location where said reading said information took place and providing said geographical
location to said central mustering server as the location where said reading said information
10 took place.

16. The method of claim 15, wherein said determining said geographical location is
performed using a Global Positioning System (GPS).

17. The method of any one of claims 1-16, wherein said emergency warden is prevented
from identifying more than a predetermined number of said evacuees before said central
15 mustering server.

18. A computer readable medium having stored thereon a mobile application to be executed
within the context of an emergency evacuation at a muster point by evacuees on their
handheld computing devices, said mobile application, when executed by a midstream one of
said evacuees on a midstream one of said handheld computing devices, causes said
20 midstream handheld computing device's processor to:

conduct a first transfer of information with an emergency warden to enable a first
communication process by which said midstream evacuee is identified before a central
mustering server, said first transfer of information being enabled by bringing said midstream
evacuee and said emergency warden in close proximity with one another;

25 conduct a second transfer of information with a downstream one of said evacuees after said
midstream evacuee is identified before said central mustering server to enable a second
communication process by which said downstream evacuee is identified before said central

mustering server, said second exchange of information being enabled by bringing said midstream evacuee and said downstream evacuee in close proximity with one another; and initiate at least one of said enabled first communication process and said enabled second communication process,

- 5 whereby said evacuees are virally identified within the confines of said muster point in an efficient and reliable manner.

19. The computer readable medium of claim 18, wherein said processor is further caused to display on said specific handheld computing device at least one of: a confirmation that said midstream evacuee is identified before said central mustering server; and a confirmation that
10 said downstream evacuee is identified before said central mustering server.

20. The computer readable medium of any one of claims 18-19, wherein said processor is caused to establish an NFC connection with an NFC chip, and one of said first transfer of information and said second transfer of information is performed over said NFC connection.

21. The computer readable medium of any one of claims 18-20, wherein said processor is
15 caused to receive an identifier of said downstream evacuee, and over the course of said second communication process, provide said received identifier to said central mustering server.

22. The computer readable medium of claim 21, wherein said processor is caused to provide said received identifier to said central mustering server over a local area network.

20 23. The computer readable medium of any one of claims 18-20, wherein said processor is caused to receive an identifier of said downstream evacuee, and over the course of said second communication process, said processor is caused to:

display said identifier on said midstream handheld computing device; and

25 receive a confirmation from said midstream evacuee that said identifier matches said downstream evacuee to enable an identification of said downstream evacuee before said central mustering server.

24. The computer readable medium of any one of claims 18-23, wherein said processor is caused to perform at least one of: providing an identifier of said midstream evacuee to said emergency warden over the course of said first transfer of information; and receiving an identity of said downstream evacuee from said downstream evacuee over the course of said
5 second transfer of information.

25. The computer readable medium of any one of claims 18-20, wherein said processor is caused to provide an identifier of at least one of said midstream evacuee and said downstream evacuee over the course of at least one of said first communication process and said second communication process to the root emergency warden, said root emergency
10 warden being the person having initiated the viral identification of said evacuees.

26. The computer readable medium of claim 25, wherein said processor is caused to provide said identifier to said root emergency warden over Short Message Service (SMS) communication.

27. The computer readable medium of any one of claims 18-26, wherein said processor is
15 further caused to receive login credentials of said midstream evacuee and initiate a validation of said credentials before said first transfer of information.

28. The computer readable medium of any one of claims 18-27, wherein said processor is further caused to receive a selection of a communication technology from said midstream evacuee, and at least one of said first transfer of information and said second transfer of
20 information is performed over said communication technology.

29. The computer readable medium of any one of claims 18-28, wherein said processor is further caused to:

receive instructions from said midstream evacuee to display an electronic form for manual entry of an identifier of one of said evacuees;

25 display said electronic form on said midstream handheld computing device;

receive said manual entry through said electronic form; and

initiate a communication process by which said manually entered identifier is provided to said central mustering server.

30. The computer readable medium of any one of claims 18-29, wherein said second communication process is one by which an identifier of said midstream evacuee is provided to said central mustering server as the person by whom said downstream evacuee was identified.

31. The computer readable medium of any one of claims 19-30, wherein said processor is caused to determine a geographical location where at least one of said first transfer of information and said second transfer of information took place, and a corresponding one of said first communication process and said second communication process comprises providing said geographical location to said central mustering server.

32. The computer readable medium of claim 31, wherein said processor is caused to determine said geographical location using a GPS of said specific midstream handheld computing device.

33. The computer readable medium of any one of claims 18-32, wherein said processor is further caused to have no more than a predetermined number of said downstream evacuee identified before said central mustering server.

34. A mustering system for use within the context of an emergency evacuation, the system comprising:

the computer readable medium of claim 18; and

a computer readable medium having stored thereon a software to be executed on a server, said software, when executed on said server, enables said server as a central mustering server and causes its server processor to produce a list of missing persons for the search and rescue services by removing said midstream evacuee and said downstream evacuee from a list of persons to be mustered as they are identified before said central mustering server.

35. The mustering system of claim 34, wherein said server processor is further caused to retrieve said list of persons to be mustered from an Access Control System of the area being evacuated.

5 36. The mustering system of any one of claims 34-35, wherein said server processor is caused to receive an activation signal from an alarm system covering said area when said alarm system is triggered, and retrieve said list of persons to be mustered in response to said activation signal.

10 37. The mustering system of any one of claims 34-36, wherein said server processor is caused to produce a list of evacuees for the search and rescue services from said midstream evacuee and said downstream evacuee after they are identified before said central mustering server.

38. The mustering system of claim 37, wherein:

said computer readable medium of claim 18 is the computer readable medium of claim 30;
and

15 said server processor is caused to record on said list of evacuees said midstream evacuee as the person by whom said downstream evacuee was identified before said central mustering server.

20 39. The mustering system of claim 38, wherein said server processor is caused to produce said list of evacuees in the form of a tree diagram illustrating said viral identification of said evacuees, said midstream evacuee being represented by a node, and said downstream evacuee being represented by a corresponding child node.

25 40. The mustering system of any one of claims 34-39, wherein said server processor is caused to validate that said midstream evacuee can be identified before said central mustering server at the geographical location of said first transfer of information by said emergency warden prior to removing said midstream evacuee from said list of persons to be mustered.

41. The mustering system of claim 40, wherein if said midstream evacuee cannot be identified before said central mustering server at said geographical location by said emergency warden, said server processor is caused to provide said midstream handheld computing device with an error message.

5 42. The mustering system of any one of claims 34-41, wherein:

said computer readable medium of claim 18 is the computer readable medium of claim 27;
and

said server processor is caused to validate said login credentials, provide said midstream handheld computing device with a login confirmation if said login credentials are valid, and
10 provide said midstream handheld computing device with a login error if said login credentials are invalid.

43. The mustering system of claim 42, wherein said server processor is caused to generate a timestamp for said login confirmation and record said timestamp as associated with said midstream evacuee.

15 44. The mustering system of any one of claims 42-43, wherein said server processor is caused to determine whether said login credentials belong to a predetermined emergency warden or a substitute emergency warden, in which case said server processor is caused to remove the person to whom said login credentials belong from said list of persons to be mustered.

20 45. The mustering system of any one of claims 34-44, wherein said server processor is caused to determine that a predetermined emergency warden is absent and designate another one of said evacuees as a substitute emergency warden.

46. The mustering system of any one of claims 34-45, wherein said server processor is caused to receive a status request from a device operated by said search and rescue services
25 and provide the most recent version of said list of missing persons in response to said status request.

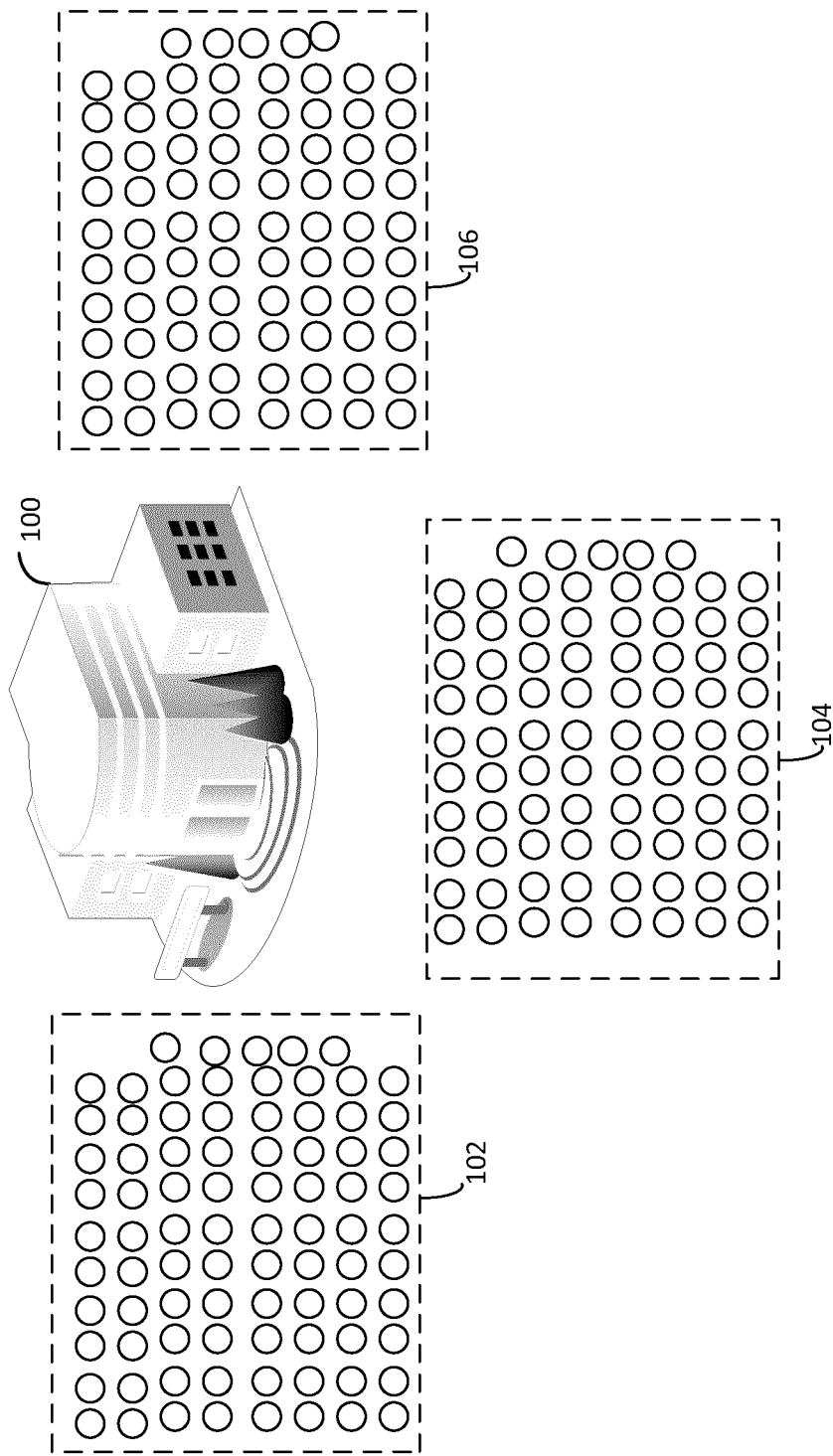


FIG. 1

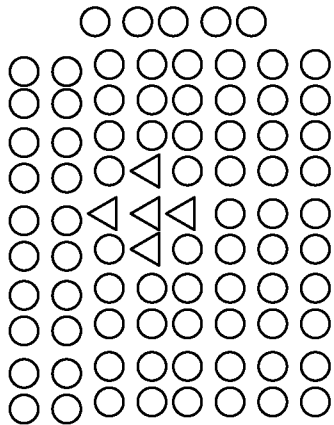


FIG. 2A

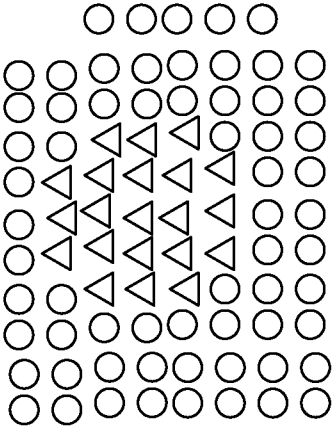


FIG. 2B

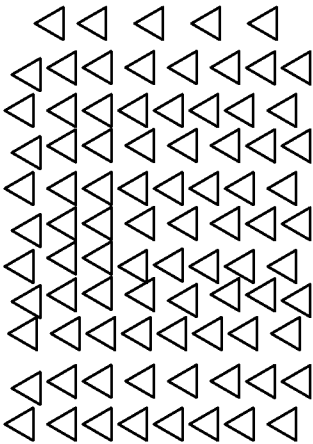


FIG. 2C

FIG. 2D

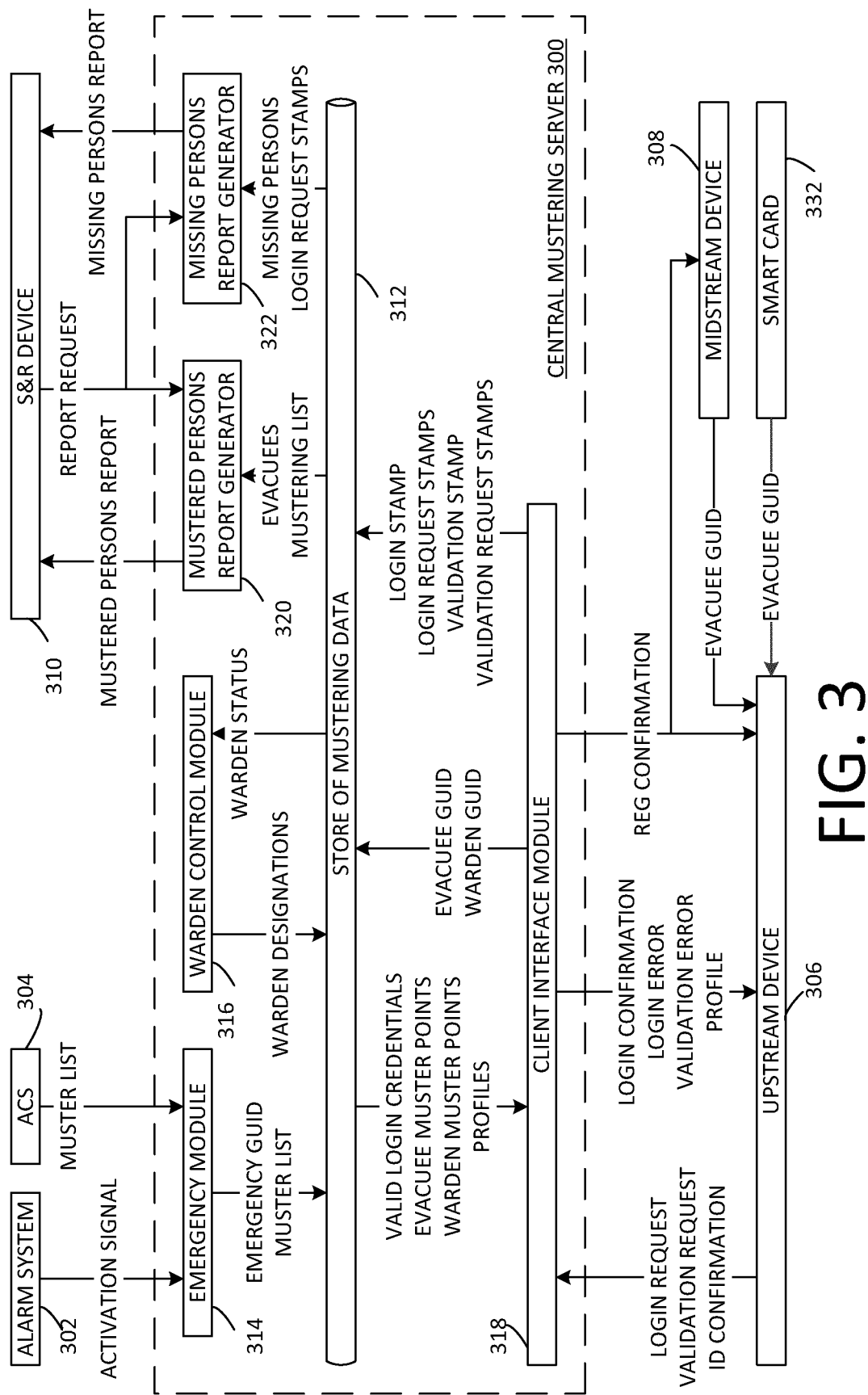


FIG. 3

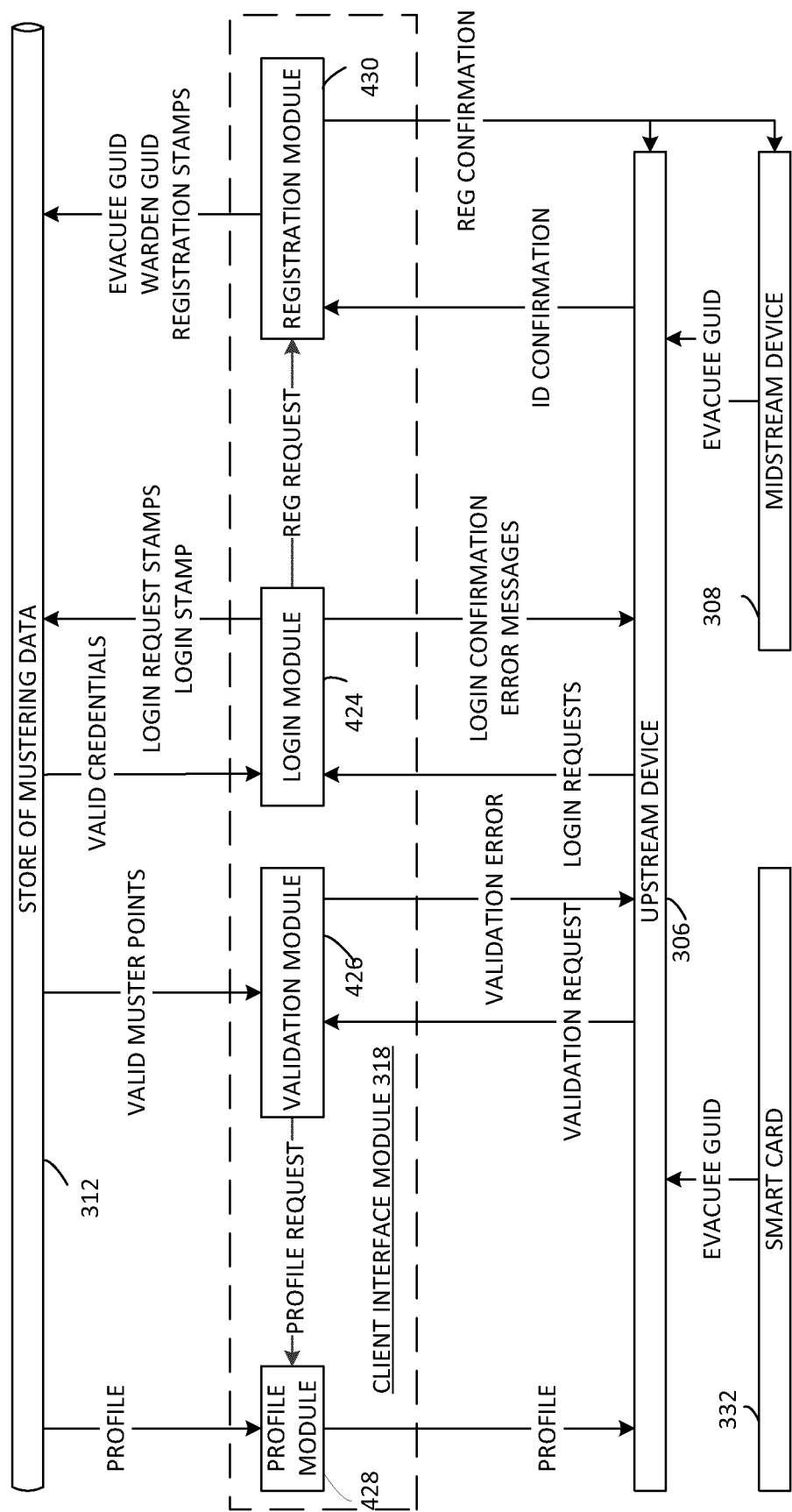


FIG. 4

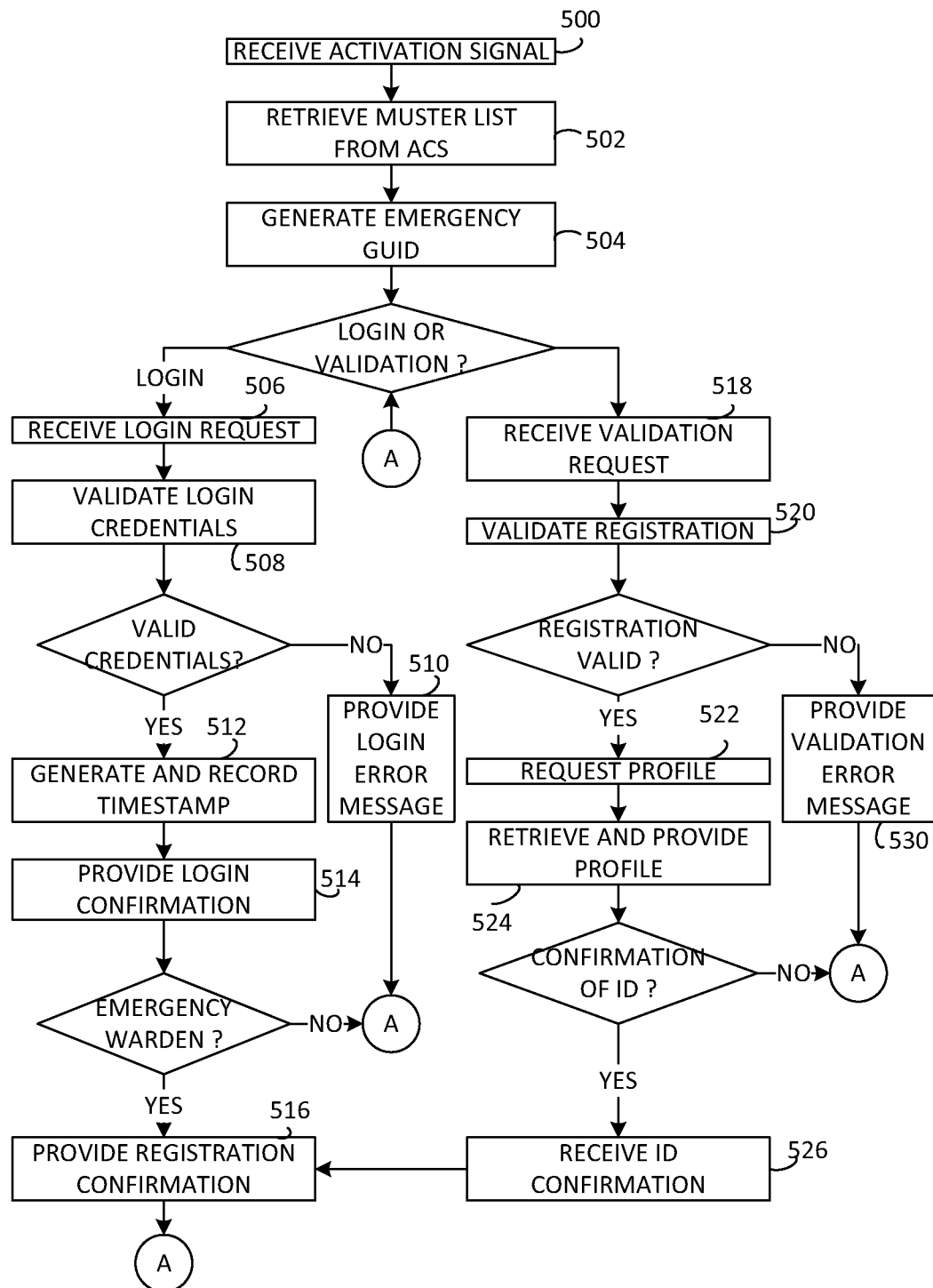


FIG. 5

6/11

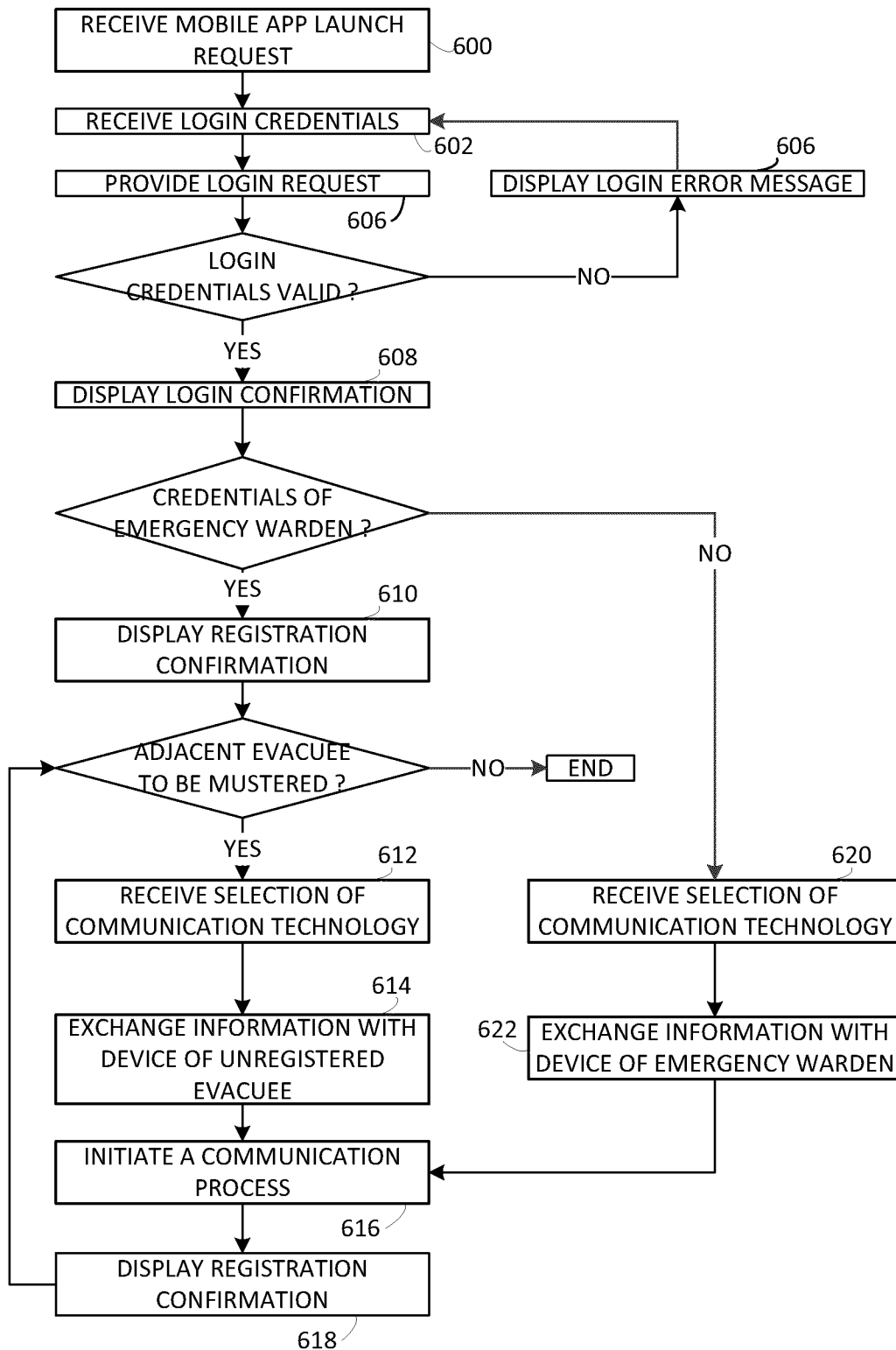


FIG. 6

7/11

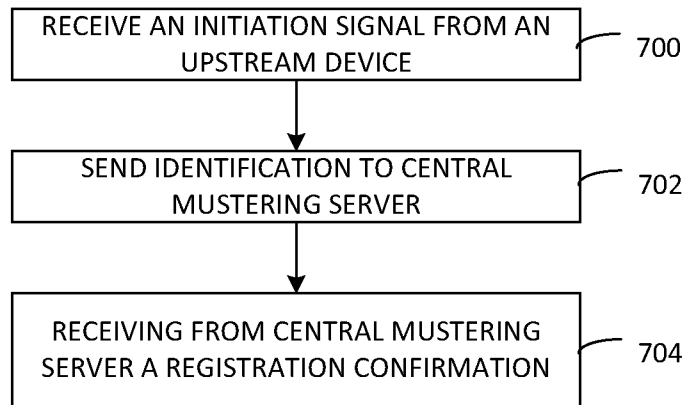


FIG. 7

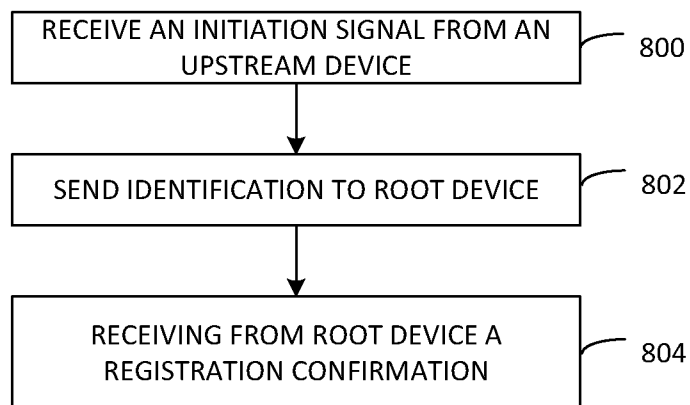


FIG. 8

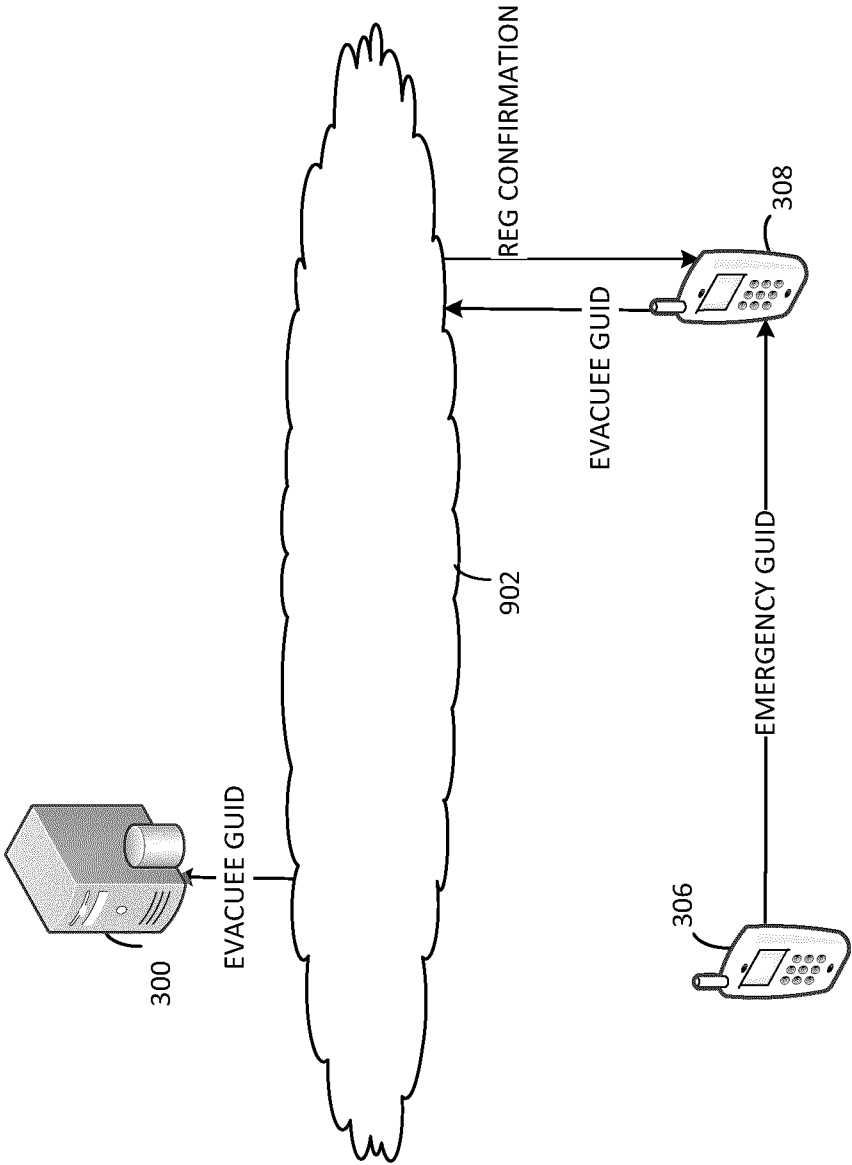


FIG. 9

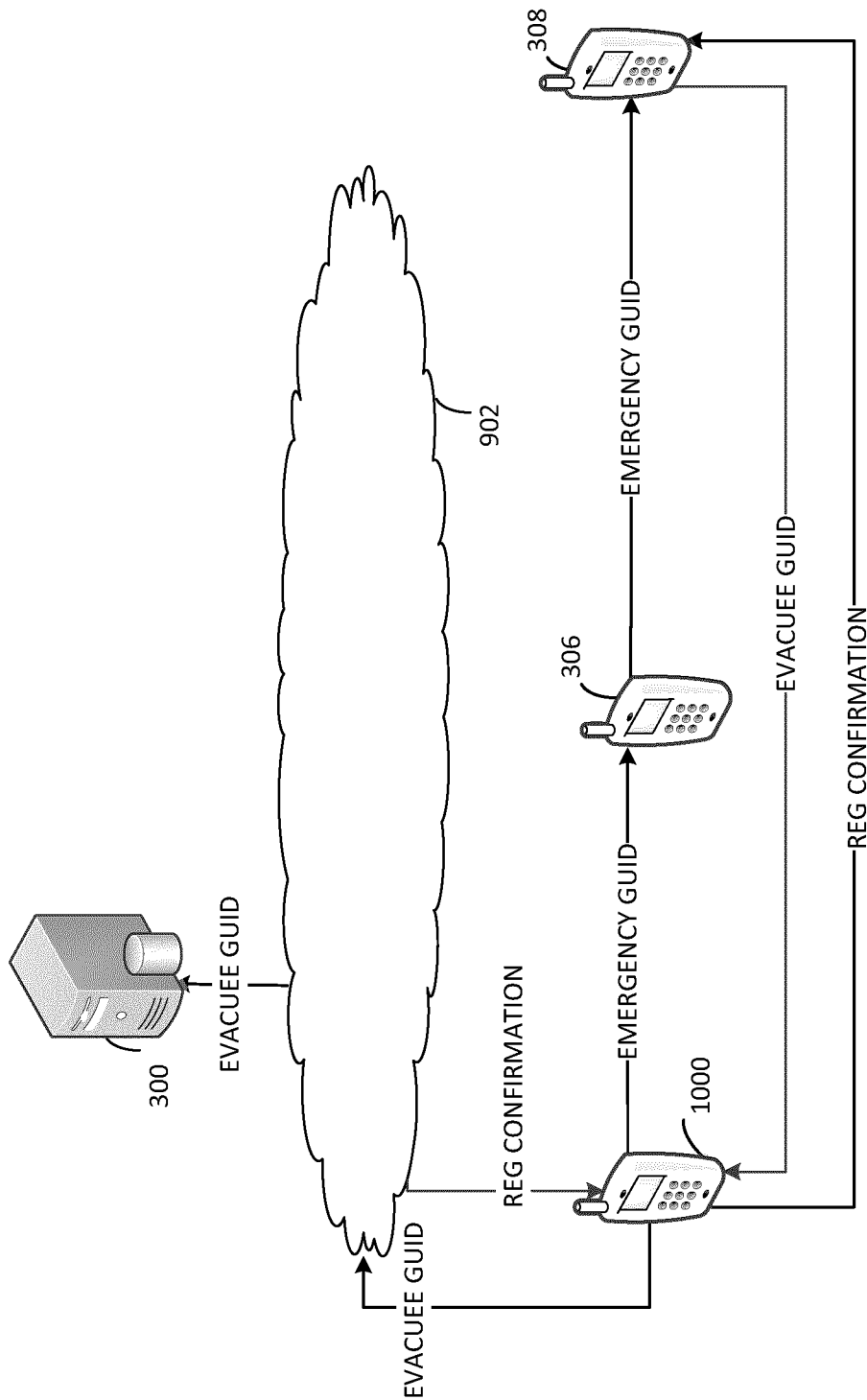


FIG. 10

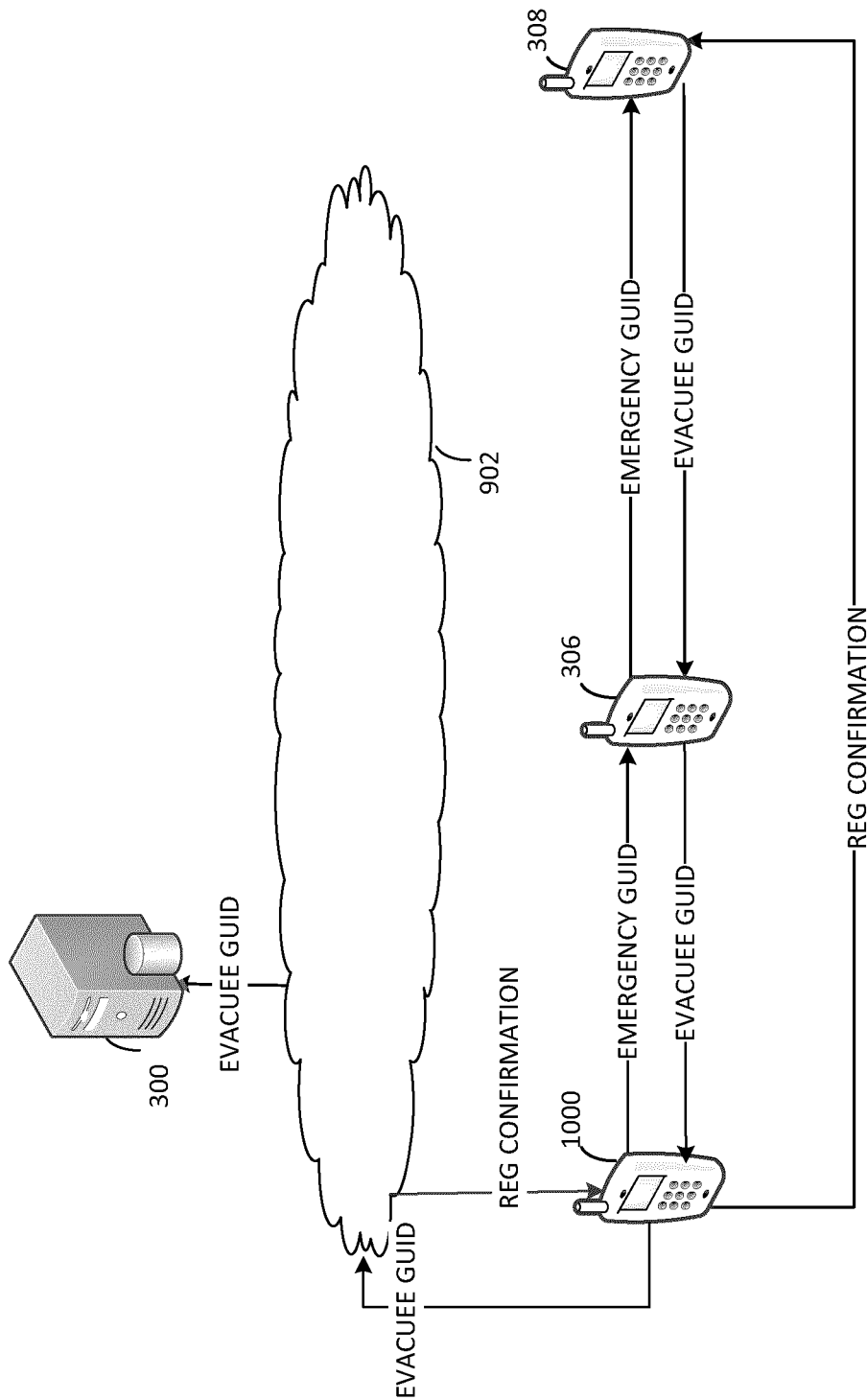


FIG. 11

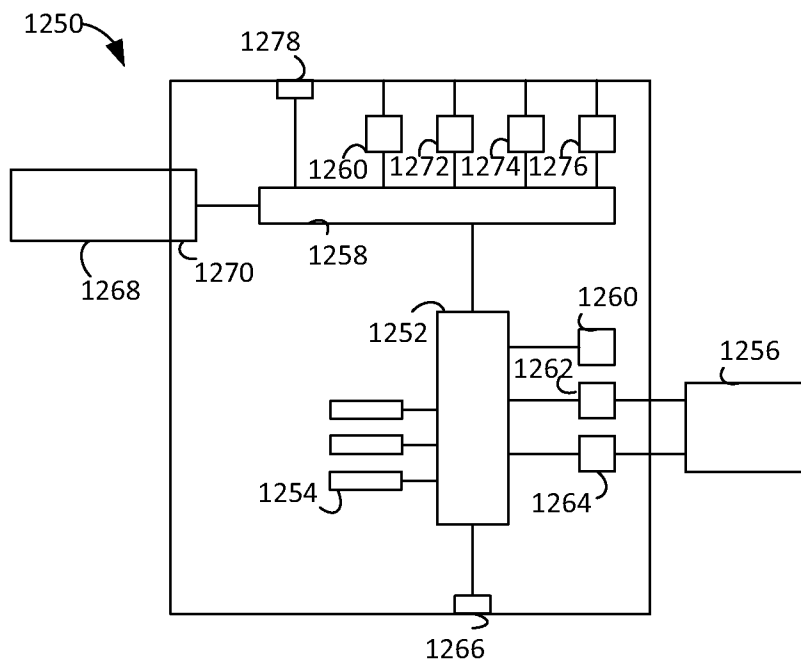
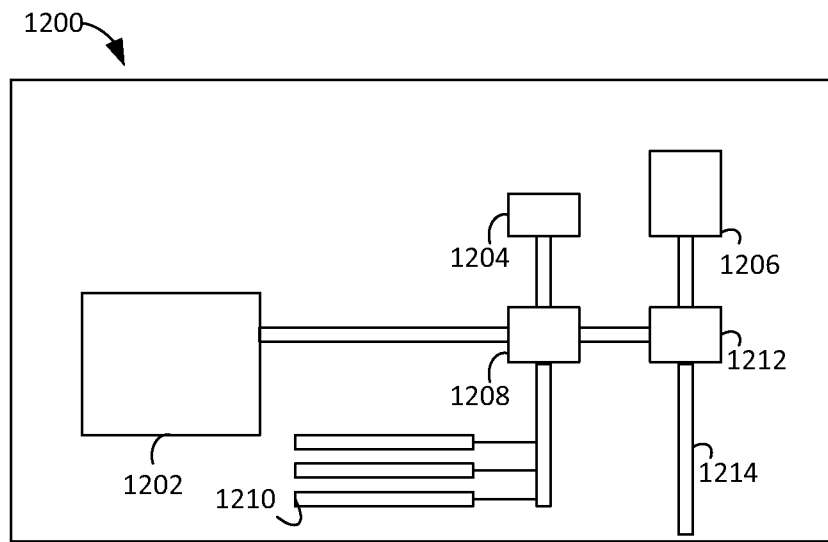


FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/051031

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **G06Q 10/00** (2012.01), **G07C 11/00** (2006.01), **H04W 4/00** (2009.01), **H04W 4/14** (2009.01),
H04B 5/00 (2006.01)

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)
 Keywords across all IPC.

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)

Canadian patent database; Questel Orbit (FAMPAT); Google Patents; CIPOL Library Discovery Tool: genetec, evacu*, muster*, handheld, emergenc*, racz, incident, disaster, identi*, mobile, telephone, smart, device, employee, user, worker, person*, portable, viral, mesh, peer, ad hoc, roll, headcount, attendance, regist*, log, logs, log*, warden, assembl*, gather*, account, phone.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages				Relevant to claim No.
A	US 2006/0 118 636	MILES et al.	8 June 2006	(08-06-2006)	1 to 46
A	US 2006/0 193 262	MCSHEFFREY et al.	31 August 2006	(31-08-2006)	1 to 46
A	US 2008/0 129 467	GENNARD	5 June 2008	(05-06-2008)	1 to 46
A	US 2010/0 282 839	ZURA et al.	11 November 2011	(11-11-2010)	1 to 46
A	US 2015/0 228 183	ROTHKOPF et al.	13 August 2015	(13-08-2015)	1 to 46
A	WO 2011/106 529	DAIGLE et al.	1 September 2011	(01-09-2011)	1 to 46

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* "A" "E" "L" "O" "P"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance earlier application or patent but published on or after the international filing date 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) document referring to an oral disclosure, use, exhibition or other means document published prior to the international filing date but later than the priority date claimed	"T" "X" "Y" "&"	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 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 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
 20 October 2016 (20-10-2016)

Date of mailing of the international search report
 26 October 2016 (26-10-2016)

Name and mailing address of the ISA/CA
 Canadian Intellectual Property Office
 Place du Portage I, C114 - 1st Floor, Box PCT
 50 Victoria Street
 Gatineau, Quebec K1A 0C9
 Facsimile No.: 819-953-2476

Authorized officer

Leigh Matheson (819) 639-8209

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CA2016/051031

Patent Document Cited in Search Report	Patent Family Member(s)	Publication Date
US2006118636A1	None	08 June 2006 (08-06-2006)
US2006193262A1	None	31 August 2006 (31-08-2006)
US2008129467A1	US7916024B2 AT439660T CN101160610A CN101160610B CY1109588T1 DE602006008431D1 DK1854084T3 EP1854084A1 EP1854084B1 ES2330966T3 GB0502527D0 GB2422937A RU2007133545A RU2409866C2 WO2006085056A1	05 June 2008 (05-06-2008) 29 March 2011 (29-03-2011) 15 August 2009 (15-08-2009) 09 April 2008 (09-04-2008) 16 February 2011 (16-02-2011) 13 August 2014 (13-08-2014) 24 September 2009 (24-09-2009) 23 November 2009 (23-11-2009) 14 November 2007 (14-11-2007) 12 August 2009 (12-08-2009) 17 December 2009 (17-12-2009) 16 March 2005 (16-03-2005) 09 August 2006 (09-08-2006) 20 March 2009 (20-03-2009) 20 January 2011 (20-01-2011) 17 August 2006 (17-08-2006)
US2010282839A1	None	11 November 2010 (11-11-2010)
US2015228183A1	EP2893525A1 GB201215760D0 GB2505517A WO2014037711A1	13 August 2015 (13-08-2015) 15 July 2015 (15-07-2015) 17 October 2012 (17-10-2012) 05 March 2014 (05-03-2014) 13 March 2014 (13-03-2014)
WO2011106529A2	WO2011106529A3 US2011244798A1	01 September 2011 (01-09-2011) 22 December 2011 (22-12-2011) 06 October 2011 (06-10-2011)