

**METHOD AND SYSTEM FOR FACILITATING AUTHENTICATION OF A
PERSON FOR ACCESSING A GATED PROPERTY, AND METHOD AND
SYSTEM FOR CONTROLLING ACCESS OF A PERSON TO A GATED
PROPERTY**

5

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of priority of Singapore Patent Application No. 10202103239Q, filed on 30 March 2021, the content of which being hereby incorporated by reference in its entirety for all purposes.

10

TECHNICAL FIELD

[0002] The present invention generally relates to a method and a system for facilitating authentication of a person for accessing a gated property to perform a task therein, and a method and a system for controlling access of a person to a gated property to perform a task therein.

15

BACKGROUND

[0003] There are various situations or circumstances where it is required for a person to be authenticated in order for the person to be allowed to access a gated property to perform a task (e.g., provide a service) within the gated property, such as but not limited to, a delivery task, an electrical task, a plumbing task, and so on (in general, for any task that requires a person to access within the gated property to perform the task).

20

[0004] By way of an example only, with the proliferation of food delivery service and E-Commerce platform, consumers often order food and/or other goods which need to be delivered within a gated property, such as a condominium, a hotel, an office building, etc. Typically, once a delivery person arrives at such a gated property, a security guard needs to check the information of the delivery person (such as name, identity number, mobile phone number, etc.) and the details of the delivery package (such as delivery company, delivery destination, including resident's name, unit number, etc.). This presents a significant workload to the security guard, as well as safety risk due to human contact, for example, which may result in infection of disease(s), such as coronavirus and SARS virus, etc.

30

[0005] To provide security for a gated property (which may simply be referred to herein as property), two common approaches can be found in conventional techniques. A first approach is a pre-registration approach. Biometric data of a delivery person, such as a face image (or facial image), may be pre-registered and stored at a property access control system of the property. Once the delivery person arrives at the property, facial recognition using the pre-registered face image may be performed at an entrance gate of the property. For example, a face image of the delivery person may be captured at the property so as to match with the pre-registered face image of the delivery person stored at the property access control system. If the captured face image and the pre-registered face image match, then the delivery person may be allowed to enter the property. This approach, however, requires privacy data, i.e., requires a registered face image, of a delivery person to be stored at the property.

[0006] Alternatively, other information of the delivery person and/or delivery package may be pre-registered, and an access code may be generated and sent to the delivery person. Once the delivery person arrives the property, the delivery person can present the access code. If the access code presented and the pre-registered access code or information match, then the delivery person may be allowed to enter the gated property. This approach, however, may not be sufficiently secured as, for example, the access code may be passed to another person.

[0007] In addition, the pre-registration process may require an interface between the delivery company and the property. As a delivery company may need to provide delivery service to multiple properties, and a property may receive delivery services from multiple delivery companies, this approach may pose challenges for both the delivery company and the property to implement multiple interfaces and/or update the interfaces to meet new security requirements or regulations.

[0008] A second approach is to establish on-site intercom connection between the delivery person and the consumer, i.e., a resident at the property. When the delivery person arrives the property, the resident may attempt to verify or authenticate the delivery person via the intercom having video and/or audio capability and decide whether to allow the delivery person to enter the property. This approach, however, is not automated and not secure, as it may be difficult for the resident to verify or authenticate the delivery person.

[0009] A need therefore exists to provide a method and a system for facilitating authentication of a person for accessing a gated property, and a method and a system

for controlling access of a person to a gated property, that seek to overcome, or at least ameliorate, one or more of the above-mentioned deficiencies in the conventional methods and systems, and in particular, to improve the effectiveness and/or efficiency in authenticating a person and/or controlling access of the person to a gated property, such as enabling secured and automated contactless access to the gated property. It is against this background that the present invention has been developed.

SUMMARY

[0010] According to a first aspect of the present invention, there is provided a method of facilitating authentication of a person for accessing a gated property to perform a task therein, using at least one processor of an authentication facilitating system, the method comprising:

- generating a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task;
- obtaining first personal data associated with said person;
- sending first task information associated with the task to an access control system of the gated property, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of the first private-public key pair;
- receiving, in response to said sending the first task information to the access control system, a second public key of a second private-public key pair of the access control system of the gated property from the access control system, the second private-public key pair being associated with the task; and
- generating an authentication code associated with the task based on the second public key for said person to utilize for accessing the gated property to perform the task.

[0011] According to a second aspect of the present invention, there is provided an authentication facilitating system for facilitating authentication of a person for accessing a gated property to perform a task therein, the authentication facilitating system comprising:

- a memory; and
- at least one processor communicatively coupled to the memory and configured to perform the method of facilitating authentication of the person for accessing the gated property according to the above-mentioned first aspect of the present invention.

[0012] According to a third aspect of the present invention, there is provided a computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform the method of facilitating authentication of the person for accessing the gated property according to the above-mentioned first aspect of the present invention.

[0013] According to a fourth aspect of the present invention, there is provided a method of controlling access of a person to a gated property to perform a task therein, using at least one processor of an access control system of the gated property, the method comprising:

receiving first task information associated with the task from an authentication facilitating system, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of a first private-public key pair of the authentication facilitating system;

generating a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task;

sending, in response to said receiving the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system;

receiving an authentication code associated with the task upon being utilized by said person for accessing the gated property to perform the task, the authentication code being generated based on the second public key; and

determining whether to grant access to said person to access the gated property based on the authentication code received.

[0014] According to a fifth aspect of the present invention, there is provided an access control system for controlling access of a person to a gated property to perform a task therein, the access control system comprising:

a memory; and

at least one processor communicatively coupled to the memory and configured to perform the method of controlling access of the person to the gated property according to the above-mentioned fourth aspect of the present invention.

[0015] According to a sixth aspect of the present invention, there is provided a computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to

perform the method of controlling access of the person to the gated property according to the above-mentioned fourth aspect of the present invention.

[0016] According to a seventh aspect of the present invention, there is provided an authentication system for authenticating a person for accessing a gated property to perform a task therein, the authentication system comprising:

the authentication facilitating system according to the above-mentioned second aspect of the present invention, and

the access control system according to the above-mentioned fifth aspect of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Embodiments of the present invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

FIG. 1A depicts a flow diagram of a method of facilitating authentication of a person for accessing a gated property to perform a task therein, according to various embodiments of the present invention;

FIG. 1B depicts a flow diagram of a method of controlling access of a person to a gated property to perform a task therein, according to various embodiments of the present invention;

FIG. 2A depicts a schematic block diagram of an authentication facilitating system for facilitating authentication of a person for accessing a gated property to perform a task therein, according to various embodiments of the present invention, such as corresponding to the method shown in FIG. 1A;

FIG. 2B depicts a schematic block diagram of an access control system for controlling access of a person to a gated property to perform a task therein, according to various embodiments of the present invention, such as corresponding to the method shown in FIG. 1B;

FIG. 2C depicts a schematic block diagram of an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various embodiments of the present invention;

FIG. 3 depicts a schematic block diagram of an exemplary computer system in which an authentication facilitating system for facilitating authentication of a person for accessing a gated property to perform a task therein or an access control system for

controlling access of a person to a gated property to perform a task therein, according to various embodiments of the present invention, may be realized or implemented;

FIG. 4 shows an exemplary schematic diagram of an overall system such as an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments;

FIG. 5 shows a block diagram illustrating the components in a security authentication platform, according to various example embodiments;

FIG. 6A shows an example of a flow diagram illustrating the exemplary steps of a delivery company registration program, according to various example embodiments;

FIG. 6B shows an example of a structure of a delivery company database, according to various example embodiments;

FIG. 7A shows an example of a flow diagram illustrating the exemplary steps of a property registration program, according to various example embodiments;

FIG. 7B shows an example of a structure of a property database, according to various example embodiments;

FIG. 7C shows an example of a structure of a third party data service database, according to various example embodiments of the present invention;

FIG. 8 shows an example of a flow diagram illustrating the exemplary steps of a delivery task registration program, according to various example embodiments of the present invention;

FIG. 9 shows an example of a flow diagram illustrating the exemplary steps of a face image retrieval program, according to various example embodiments of the present invention;

FIG. 10 shows an example of a structure of an encrypted face image database, according to various example embodiments of the present invention;

FIG. 11A shows an example of a structure of a delivery task table, according to various example embodiments of the present invention;

FIG. 11B shows an example of a structure of a key pair database, according to various example embodiments of the present invention;

FIG. 12A shows an example of a flow diagram illustrating the exemplary steps of a two-dimensional barcode generator, according to various example embodiments of the present invention;

FIG. 12B shows an example of a structure of a two-dimensional barcode database, according to various example embodiments of the present invention;

FIG. 13 shows a block diagram illustrating the components in an access control system at a property, according to various example embodiments of the present invention;

FIG. 14 shows an example of a flow diagram illustrating the exemplary steps of a delivery task registration program, according to various example embodiments of the present invention;

FIG. 15A shows an example of a structure of a delivery task table, according to various example embodiments of the present invention;

FIG. 15B shows an example of a structure of another key pair database, according to various example embodiments of the present invention;

FIG. 16A shows an example of a flow diagram illustrating the exemplary steps of an access control program, according to various example embodiments of the present invention;

FIG. 16B shows an example of a structure of a two-dimensional barcode database, according to various example embodiments of the present invention;

FIG. 17 shows an example of a flow diagram illustrating the exemplary steps of an authentication program at the security authentication platform, according to various example embodiments of the present invention;

FIG. 18 shows an example of a flow diagram illustrating the exemplary steps of a check-out management program, according to various example embodiments of the present invention;

FIG. 19 shows an example of a flow diagram illustrating the exemplary steps of a service quality report program, according to various example embodiments of the present invention;

FIG. 20 shows an example of a structure of a service quality database, according to various example embodiments of the present invention;

FIG. 21 shows a block diagram illustrating the components in an access control system at a property, according to various other example embodiments (or various second example embodiments);

FIG. 22 shows an example flow diagram illustrating the exemplary steps of a property registration program, according to various other example embodiments (or various second example embodiments);

FIG. 23 shows an example flow diagram illustrating exemplary steps of a two-dimensional barcode generator, according to various other example embodiments (or various second example embodiments);

FIG. 24 shows an example of flow diagram illustrating the exemplary steps of an access control program, according to various example embodiments (or various second example embodiments);

FIG. 25 shows a schematic diagram of an overall system, such as the authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various other example embodiments (or various third example embodiments);

FIG. 26A and FIG. 26B show schematic diagrams of an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments;

FIGS. 27A-27H illustrate exemplary scenarios for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments;

FIG. 28 illustrates a schematic diagram of an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various second example embodiments; and

FIGS. 29A-29B illustrates another exemplary scenario for authenticating a person for accessing a gated property to perform a task therein, according to various second example embodiments.

DETAILED DESCRIPTION

[0018] Various embodiments of the present invention provide a method and system for facilitating authentication of a person for accessing a gated property to perform a task therein, and a method and a system for controlling access of a person to a gated property to perform a task therein.

[0019] As described in the background, there are various situations or circumstances where it is required for a person to be authenticated in order for the person to be allowed to access a gated property to perform a task (e.g., provide a service) within the gated property, such as but not limited to, a delivery task, an electrical task, a plumbing task, and so on (in general, for any task that requires a person to access within the gated property to perform the task). Therefore, it will be appreciated

by a person skilled in the art that the present invention is not limited to any particular task, as long as the task requires a person to access within a gated property to perform the task.

[0020] FIG. 1A depicts a flow diagram of a method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein, using at least one processor of an authentication facilitating system. The method 100 comprises: generating (at 102) a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task; obtaining (at 104) first personal data associated with said person; sending (at 106) first task information associated with the task to an access control system of the gated property, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of the first private-public key pair; receiving (at 108), in response to said sending the first task information to the access control system, a second public key of a second private-public key pair of the access control system of the gated property from the access control system, the second private-public key pair being associated with the task; and generating (at 110) an authentication code associated with the task based on the second public key for said person to utilize for accessing the gated property to perform the task.

[0021] Accordingly, the method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein advantageously improve the effectiveness and efficiency in authenticating a person for accessing a gated property. For example, the authentication facilitating system (e.g., a central authentication facilitating system remote from the access control system of the gated property) and the access control system are each configured to generate its respective private-public key pair (e.g., corresponding to the above-mentioned “first private-public key pair” and the “second private-public key pair”) associated with the task which the person seeking access to the gated property is to perform. Moreover, the authentication facilitating system and the access control system are configured to exchange with each other their respective public key associated the task. Accordingly, for example, an authentication code associated with the task can be generated by the authentication facilitating system based on the public key (e.g., corresponding to the above-mentioned second public key of the second private-public key pair) of the access control system associated with the task for the person to utilize at the gated property (by presenting the authentication code

to the access control system thereat) to seek access to the gated property to perform the task. For example, encrypted data (e.g., corresponding to first encrypted data as will be described), including task related information, included in the authentication code associated with the task is able to be decrypted by the access control system since it has
5 been encrypted based on the public key of the access control system associated with the task. Furthermore, for example, since the access control system has the public key (e.g., corresponding to the above-mentioned first public key of the first private-public key pair) of the authentication facilitating system associated with the task, in various embodiments, the access control system is able to encrypt personal data of the person
10 captured in real-time at the gated property and securely send the encrypted personal data for authentication associated with the task seamlessly without requiring any pre-registration of personal data of the person at the gated property. Accordingly, the method 100 advantageously improves the effectiveness and efficiency in authenticating a person for accessing a gated property, such as enabling secured and automated
15 contactless access to the gated property. These advantages or technical effects, and/or other advantages or technical effects, will become more apparent to a person skilled in the art as the method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein, as well as the corresponding system, is described in more detail according to various embodiments and example embodiments of the present
20 invention.

[0022] In various embodiments, the above-mentioned generating the authentication code associated with the task based on the second public key comprises encrypting the task identification information associated with the task and the person identification information associated with said person based on the second public key to produce first
25 encrypted data associated with the task, and encoding the first encrypted data and the task identification information associated with the task to generate the authentication code associated with the task.

[0023] In various embodiments, the authentication code may be a graphical barcode.

30 **[0024]** In various embodiments, the authentication code may be a two-dimensional (2D) barcode.

[0025] In various embodiments, the method 100 further comprises receiving second task information associated with the task from a task management system for registering the task with the authentication facilitating system, the second task

information comprising the person identification information associated with said person and task location information associated with the task. In various embodiments, the above-mentioned generating the first private-public key pair associated with the task is in response to the second task information associated with the task received from the task management system.

[0026] In various embodiments, the first task information may be sent to the access control system based on the task location information associated with the task.

[0027] In various embodiments, the method 100 further comprises sending the authentication code associated with the task to the task management system for said person to utilize for accessing the gated property to perform the task.

[0028] In various embodiments, the method 100 further comprises sending a personal data request relating to said person to a third party personal data provider, the personal data request comprising the person identification information associated with said person, and the above-mentioned obtaining the first personal data associated with said person is obtained from the third party personal data provider in response to the personal data request sent to the third party personal data provider.

[0029] In various embodiments, the personal data request further comprises the first public key, and the first personal data is encrypted based on the first public key.

[0030] In various embodiments, the second task information received from the task management system further comprises the first personal data associated with said person, and the above-mentioned obtaining the first personal data associated with said person is obtained from the task management system.

[0031] In various embodiments, the method 100 further comprises extracting features from the first personal data associated with said person, and the above-mentioned encrypting the task identification information and the person identification information further comprises encrypting said features based on the second public key to produce the first encrypted data associated with the task.

[0032] In various embodiments, the method 100 further comprises receiving an authentication request from the access control system, the authentication request comprising the task identification information associated with the task and second personal data associated with said person, the second personal data being encrypted based on the first public key, decrypting the second personal data based on a first private key of the first private-public key pair associated with the task, determining whether the second personal data and the first personal data associated with the task satisfy one

or more predetermined authentication conditions, and sending an authentication response to the access control system, where the authentication response indicates authentication successful if the second personal data and the first personal data associated with the task satisfy the one or more predetermined authentication conditions, and indicates authentication unsuccessful if the second personal data and the first personal data associated with the task do not satisfy the one or more predetermined authentication conditions.

[0033] In various embodiments, the one or more predetermined authentication conditions comprises a predetermined matching condition that the second personal data and the first personal data are determined to match each other.

[0034] In various embodiments, the method 100 further comprises receiving task performance information in relation to the task performed at the gated property from the access control system, generating a service quality report based on the task performance information, and sending the service quality report to the task management system. Accordingly, various embodiments facilitate measurement and benchmarking of service quality, for example, for performing the task.

[0035] Various embodiments advantageously provide a single interface between a task management system to which the task is associated and the access control system of a gated property. Various embodiments also provide enhanced security using a two-factor authentication. For example, a first authentication may be performed to match the task identification information and a second authentication may be performed to match the first personal data and the second personal data.

[0036] In various embodiments, the task may be a delivery task, and the task management system may be associated with a company which provides a delivery service.

[0037] In various embodiments, the first personal data associated with said person comprises a face image of said person.

[0038] In various embodiments, the first personal data associated with said person further comprises a health-related status of said person.

[0039] FIG. 1B depicts a flow diagram of a method 150 of controlling access of a person to a gated property to perform a task therein, using at least one processor of an access control system of the gated property. The method 150 comprises: receiving (at 152) first task information associated with the task from an authentication facilitating system, the first task information comprising task identification information associated

with the task, person identification information associated with said person, and a first public key of a first private-public key pair of the authentication facilitating system; generating (at 154) a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task; 5 sending (at 156), in response to said receiving the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system; receiving (at 158) an authentication code associated with the task upon being utilized by said person for accessing the gated property to perform the task, the authentication code being generated based on the 10 second public key; and determining (at 160) whether to grant access to said person to access the gated property based on the authentication code received.

[0040] Accordingly, similarly or correspondingly as described above with respect to the method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein, the method 150 of controlling access of a person to 15 a gated property to perform a task therein advantageously improve the effectiveness and efficiency in authenticating a person and/or controlling access of the person to a gated property, such as enabling secured and automated contactless access to the gated property. These advantages or technical effects, and/or other advantages or technical effects, will become more apparent to a person skilled in the art as the method 150 of 20 controlling access of a person to a gated property to perform a task, as well as the corresponding system, is described in more detail according to various embodiments and example embodiments of the present invention.

[0041] In various embodiments, the authentication code associated with the task has encoded therein first encrypted data and the task identification information 25 associated with the task. The first encrypted data associated with the task comprises the task identification information associated with the task and the person identification information associated with said person encrypted based on the second public key.

[0042] In various embodiments, the authentication code may be a graphical barcode.

30 **[0043]** In various embodiments, the authentication code may be a 2D barcode.

[0044] In various embodiments, the method 150 further comprises decoding the authentication code to obtain the first encrypted data and the task identification information associated with the task, and decrypting the first encrypted data based on a second private key of the second private-public key pair associated with the task to

obtain the task identification information associated with the task and the person identification information associated with said person.

5 [0045] In various embodiments, the method 150 further comprises obtaining second personal data from said person captured in real-time using a real-time personal data capturing device.

[0046] In various embodiments, the method 150 further comprises encrypting the second personal data based on the first public key; sending an authentication request to the authentication facilitating system, the authentication request comprising the task identification information associated with the task and the second personal data
10 associated with said person encrypted based on the first public key; and receiving, in response to the authentication request sent to the authentication facilitating system, an authentication response from the authentication facilitating system, where the above-mentioned determining whether to grant access to said person is further based on the authentication response received.

15 [0047] In various embodiments, the first encrypted data associated with the task further comprises features extracted from first personal data associated with said person encrypted based on the second public key. The method 150 further comprises decrypting the first personal data based on the second private key of the second private-public key pair associated with the task; determining whether the second personal data
20 and the first personal data associated with the task satisfy one or more predetermined authentication conditions; and generating an authentication response based on said determining whether the second personal data and the first personal data associated with the task satisfy one or more predetermined authentication conditions. The authentication response indicates authentication successful if the second personal data
25 and the first personal data associated with the task satisfy the one or more predetermined authentication conditions, and indicates authentication unsuccessful if the second personal data and the first personal data associated with the task do not satisfy the one or more predetermined authentication conditions, and the above-mentioned determining whether to grant access to said person is further based on the
30 authentication response generated.

[0048] In various embodiments, the one or more predetermined authentication conditions comprise a predetermined matching condition that the second personal data and the first personal data are determined to match each other.

[0049] In various embodiments, the method 150 further comprises sending task performance information in relation to the task performed at the gated property to the authentication facilitating system.

[0050] In various embodiments, the task may be a delivery task.

5 [0051] In various embodiments, the first personal data associated with said person comprises a face image of said person.

[0052] In various embodiments, the first personal data associated with said person further comprises a health-related status of said person.

[0053] FIG. 2A depicts a schematic block diagram of an authentication facilitating
10 system 200 for facilitating authentication of a person for accessing a gated property to perform a task therein, according to various embodiments of the present invention, such as corresponding to the method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein as described hereinbefore according to various embodiments of the present invention. The authentication facilitating system
15 200 comprises a memory 202, and at least one processor 204 communicatively coupled to the memory 202 and configured to perform the method of facilitating authentication of the person for accessing the gated property, including: generating a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task; obtaining first personal data associated with said person;
20 sending first task information associated with the task to an access control system of the gated property, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of the first private-public key pair; receiving, in response to said sending the first task information to the access control system, a second public key of
25 a second private-public key pair of the access control system of the gated property from the access control system, the second private-public key pair being associated with the task; and generating an authentication code associated with the task based on the second public key for said person to utilize for accessing the gated property to perform the task.

[0054] It will be appreciated by a person skilled in the art that the at least one
30 processor 204 may be configured to perform the required functions or operations through set(s) of instructions (e.g., software modules) executable by the at least one processor 204 to perform the required functions or operations. Accordingly, as shown in FIG. 2A, the authentication facilitating system 200 may comprise a first private-public key pair generating module (or a first private-public key pair generating circuit)

206 configured to generate a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task; a first personal data obtaining module (or a first personal data obtaining circuit) 208 configured to obtain first personal data associated with said person; a task information sending module (or a task information sending circuit) 210 configured to send first task information associated with the task to an access control system of the gated property; a second public key receiving module (or a second public key receiving circuit) 212 configured to receive, in response to said sending the first task information to the access control system, a second public key of a second private-public key pair of the access control system of the gated property from the access control system; and an authentication code generating module (or an authentication code generating circuit) 214 configured to generate an authentication code associated with the task based on the second public key for said person to utilize for accessing the gated property to perform the task.

[0055] It will be appreciated by a person skilled in the art that the above-mentioned modules are not necessarily separate modules, and one or more modules may be realized by or implemented as one functional module (e.g., a circuit or a software program) as desired or as appropriate without deviating from the scope of the present invention. For example, two or more of the first private-public key pair generating module 206, the first personal data obtaining module 208, the task information sending module 210, the second public key receiving module 212 and the authentication code generating module 214 may be realized (e.g., compiled together) as one executable software program (e.g., software application or simply referred to as an “app”), which for example may be stored in the memory 202 and executable by the at least one processor 204 to perform the functions/operations as described herein according to various embodiments.

[0056] In various embodiments, the system 200 corresponds to the method 100 as described hereinbefore with reference to FIG. 1A, therefore, various functions or operations configured to be performed by the least one processor 204 may correspond to various steps of the method 100 described hereinbefore according to various embodiments, and thus need not be repeated with respect to the system 200 for clarity and conciseness. In other words, various embodiments described herein in context of the methods are analogously valid for the respective systems, and vice versa.

[0057] For example, in various embodiments, the memory 202 may have stored therein the first private-public key pair generating module 206, the first personal data obtaining module 208, the task information sending module 210, the second public key receiving module 212 and/or the authentication code generating module 214, which respectively correspond to various steps of the method 100 as described hereinbefore according to various embodiments, which are executable by the at least one processor 204 to perform the corresponding functions/operations as described herein.

[0058] FIG. 2B depicts a schematic block diagram of an access control system 250 for controlling access of a person to a gated property to perform a task therein, according to various embodiments of the present invention, such as corresponding to the method 150 of controlling access of a person to a gated property to perform a task therein as described hereinbefore according to various embodiments of the present invention. The access control system 250 comprises a memory 202, and at least one processor 204 communicatively coupled to the memory 202 and configured to perform the method of controlling access of a person to the gated property, including: receiving first task information associated with the task from an authentication facilitating system, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of a first private-public key pair of the authentication facilitating system; generating a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task; sending, in response to said receiving the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system; receiving an authentication code associated with the task upon being utilized by said person for accessing the gated property to perform the task, the authentication code being generated based on the second public key; and determining whether to grant access to said person to access the gated property based on the authentication code received.

[0059] It will be appreciated by a person skilled in the art that the at least one processor 204 may be configured to perform the required functions or operations through set(s) of instructions (e.g., software modules) executable by the at least one processor 204 to perform the required functions or operations. Accordingly, as shown in FIG. 2B, the access control system 250 may comprise a task information receiving module (or a task information receiving circuit) 256 configured to receive first task

information associated with the task from an authentication facilitating system; a second private-public key pair generating module (or a second private-public key pair generating circuit) 258 configured to generate a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task; a second public key sending module (or a second public key sending circuit) 260 configured to send, in response to said receive the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system; an authentication code receiving module (or an authentication code receiving circuit) 262 configured to receive an authentication code associated with the task upon being utilized by said person for accessing the gated property to perform the task, the authentication code being generated based on the second public key; and an access granting determining module (or an access granting determining circuit) 264 configured to determine whether to grant access to said person to access the gated property based on the authentication code received.

[0060] It will be appreciated by a person skilled in the art that the above-mentioned modules are not necessarily separate modules, and one or more modules may be realized by or implemented as one functional module (e.g., a circuit or a software program) as desired or as appropriate without deviating from the scope of the present invention. For example, two or more of the task information receiving module 256, the second private-public key pair generating module 258, the second public key sending module 260, the authentication code receiving module 262 and the access granting determining module 264 may be realized (e.g., compiled together) as one executable software program (e.g., software application or simply referred to as an “app”), which for example may be stored in the memory 202 and executable by the at least one processor 204 to perform the functions/operations as described herein according to various embodiments.

[0061] In various embodiments, the system 250 corresponds to the method 150 as described hereinbefore with reference to FIG. 1B, therefore, various functions or operations configured to be performed by the least one processor 204 may correspond to various steps of the method 150 described hereinbefore according to various embodiments, and thus need not be repeated with respect to the system 250 for clarity and conciseness. In other words, various embodiments described herein in context of the methods are analogously valid for the respective systems, and vice versa.

[0062] For example, in various embodiments, the memory 202 may have stored therein the task information receiving module 256, the second private-public key pair generating module 258, the second public key sending module 260, the authentication code receiving module 262 and/or the access granting determining module 264, which respectively correspond to various steps of the method 150 as described hereinbefore according to various embodiments, which are executable by the at least one processor 204 to perform the corresponding functions/operations as described herein.

[0063] A computing system, a controller, a microcontroller or any other system providing a processing capability may be provided according to various embodiments in the present disclosure. Such a system may be taken to include one or more processors and one or more computer-readable storage mediums. For example, the authentication facilitating system 200/access control system 250 described hereinbefore may include a processor (or controller) 204 and a computer-readable storage medium (or memory) 202 which are for example used in various processing carried out therein as described herein. A memory or computer-readable storage medium used in various embodiments may be a volatile memory, for example a DRAM (Dynamic Random Access Memory) or a non-volatile memory, for example a PROM (Programmable Read Only Memory), an EPROM (Erasable PROM), EEPROM (Electrically Erasable PROM), or a flash memory, e.g., a floating gate memory, a charge trapping memory, an MRAM (Magnetoresistive Random Access Memory) or a PCRAM (Phase Change Random Access Memory).

[0064] In various embodiments, a “circuit” may be understood as any kind of a logic implementing entity, which may be special purpose circuitry or a processor executing software stored in a memory, firmware, or any combination thereof. Thus, in an embodiment, a “circuit” may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g., a microprocessor (e.g., a Complex Instruction Set Computer (CISC) processor or a Reduced Instruction Set Computer (RISC) processor). A “circuit” may also be a processor executing software, e.g., any kind of computer program, e.g., a computer program using a virtual machine code, e.g., Java. Any other kind of implementation of the respective functions which will be described in more detail below may also be understood as a “circuit” in accordance with various alternative embodiments. Similarly, a “module” may be a portion of a system according to various embodiments in the present invention and may encompass

a “circuit” as above, or may be understood to be any kind of a logic-implementing entity therefrom.

[0065] Some portions of the present disclosure are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0066] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “obtaining”, “generating”, “sending”, “receiving”, “determining”, or the like, refer to the actions and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0067] The present specification also discloses a system (e.g., which may also be embodied as a device or an apparatus), such as the authentication facilitating system 200, and/or the access control system 250, for performing the operations/functions of the methods described herein. Such a system may be specially constructed for the required purposes, or may comprise a general purpose computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose machines may be used with computer programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate.

[0068] In addition, the present specification also at least implicitly discloses a computer program or software/functional module, in that it would be apparent to the person skilled in the art that the individual steps of the methods described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used

to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention. It will be appreciated by a person skilled in the art that various modules described herein (e.g., the first private-public key pair generating module 206, the first personal data obtaining module 208, the task information sending module 210, the second public key receiving module 212, the authentication code generating module 214, the task information receiving module 256, the second private-public key pair generating module 258, the second public key sending module 260, the authentication code receiving module 262 and/or the access granting determining module 264) may be software module(s) realized by computer program(s) or set(s) of instructions executable by a computer processor to perform the required functions, or may be hardware module(s) being functional hardware unit(s) designed to perform the required functions. It will also be appreciated that a combination of hardware and software modules may be implemented.

[0069] Furthermore, one or more of the steps of a computer program/module or method described herein may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a general purpose computer. The computer program when loaded and executed on such a general-purpose computer effectively results in an apparatus that implements the steps of the methods described herein.

[0070] In various embodiments, there is provided a computer program product, embodied in one or more computer-readable storage mediums (non-transitory computer-readable storage medium), comprising instructions (e.g., the first private-public key pair generating module 206, the first personal data obtaining module 208, the task information sending module 210, the second public key receiving module 212 and/or the authentication code generating module 214) executable by one or more computer processors to perform a method 100 of facilitating authentication of a person for accessing a gated property to perform a task therein as described hereinbefore with reference to FIG. 1A. Accordingly, various computer programs or modules described herein may be stored in a computer program product receivable by a system therein,

such as the system 200 as shown in FIG. 2A, for execution by at least one processor 204 of the system 200 to perform the required or desired functions.

[0071] In various other embodiments, there is provided a computer program product, embodied in one or more computer-readable storage mediums (non-transitory computer-readable storage medium), comprising instructions (e.g., the task information receiving module 256, the second private-public key pair generating module 258, the second public key sending module 260, the authentication code receiving module 262 and/or the access granting determining module 264) executable by one or more computer processors to perform a method 150 of controlling access of a person to a gated property to perform a task therein as described hereinbefore with reference to FIG. 1B. Accordingly, various computer programs or modules described herein may be stored in a computer program product receivable by a system therein, such as the system 250 as shown in FIG. 2B, for execution by at least one processor 204 of the system 200 to perform the required or desired functions.

[0072] The software or functional modules described herein may also be implemented as hardware modules. More particularly, in the hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC). Numerous other possibilities exist. Those skilled in the art will appreciate that the software or functional module(s) described herein can also be implemented as a combination of hardware and software modules.

[0073] In various embodiments, an authentication system 280 for authenticating a person for accessing a gated property to perform a task therein may be provided, as illustrated in FIG. 2C. The authentication system 280 may comprise the authentication facilitating system 200 and the access control system 250.

[0074] In various embodiments, the authentication facilitating system 200 and the access control system 250 may each be realized by any computer system (e.g., desktop or portable computer system) including at least one processor and a memory, such as a computer system 300 as schematically shown in FIG. 3 as an example only and without limitation. Various methods/steps or functional modules (e.g., the first private-public key pair generating module 206, the first personal data obtaining module 208, the task information sending module 210, the second public key receiving module 212, the authentication code generating module 214, the task information receiving module 256,

the second private-public key pair generating module 258, the second public key sending module 260, the authentication code receiving module 262 and/or the access granting determining module 264) may be implemented as software, such as a computer program being executed within the computer system 300, and instructing the computer system 300 (in particular, one or more processors therein) to conduct the methods/functions of various embodiments described herein.

[0075] The computer system 300 may comprise a computer module 302, input modules, such as a keyboard 304 and a mouse 306, and a plurality of output devices such as a display 308, and a printer 310. The computer module 302 may be connected to a computer network 312 via a suitable transceiver device 314, to enable access to e.g., the Internet or other network systems such as Local Area Network (LAN) or Wide Area Network (WAN). The computer module 302 in the example may include a processor 318 for executing various instructions, a Random Access Memory (RAM) 320 and a Read Only Memory (ROM) 322. The computer module 302 may also include a number of Input/Output (I/O) interfaces, for example I/O interface 324 to the display 308, and I/O interface 326 to the keyboard 304. The components of the computer module 302 typically communicate via an interconnected bus 328 and in a manner known to the person skilled in the relevant art.

[0076] It will be appreciated by a person skilled in the art that the terminology used herein is for the purpose of describing various embodiments only and is not intended to be limiting of the present invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0077] In order that the present invention may be readily understood and put into practical effect, various example embodiments of the present invention will be described hereinafter by way of examples only and not limitations. It will be appreciated by a person skilled in the art that the present invention may, however, be embodied in various different forms or configurations and should not be construed as limited to the example embodiments set forth hereinafter. Rather, these example

embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the present invention to those skilled in the art.

- [0078] In particular, for better understanding of the present invention and without limitation or loss of generality, and unless stated otherwise, various example
- 5 embodiments of the present invention will now be described with respect to the task to be performed by a person being a delivery task, or more specifically, a contactless delivery task. However, it will be appreciated by a person skilled in the art that the present invention is not limited to a delivery task and may be applied to any other type of task (or service) as desired or as appropriate, as long as the task requires a person to
- 10 access within a gated property to perform the task, such as but not limited to, a plumbing task, electrical task, home tuition task in various non-limiting examples. It will also be appreciated by a person skilled in the art that a task may refer to a single task or a combination of tasks (e.g., of the same or different types), without going beyond the scope of the present invention.
- 15 [0079] Various example embodiments provide an intermediate security authentication platform that enables a secured and automated contactless delivery service. The system provides security authentication using two-factor authentication with asymmetric encryption. According to various example embodiments, the two-factor authentication may be realized by (i) a first factor authentication by matching
- 20 asymmetric encrypted data in a two-dimensional barcode, and (ii) a second factor authentication by matching asymmetric encrypted face images and/or facial features. The service may further generate service quality and benchmarking report. According to various example embodiments, the service may generate service quality and benchmarking report by measuring service quality based on arriving time and dwell
- 25 time of a delivery person, and/or benchmarking service quality across delivery companies. Various embodiments of the invention advantageously protect the privacy data of a delivery person (e.g., corresponding to the personal data associated with said person such as first personal data, second personal data, as described hereinbefore according to various embodiments), without pre-registration of privacy data, such as
- 30 face image, of the delivery person at a property. Various embodiments of the invention enable a standard and single interface for a delivery company and a property. Various embodiments of the invention also enable a property to customize additional third party data services for the security authentication.

[0080] FIG. 4 shows a schematic diagram of an overall system 400 such as an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments. The system includes a security authentication platform 410, a plurality of delivery companies 420, a plurality of properties 430, and a plurality of third party data services 440, and a communication network 450. A delivery company of the plurality of delivery companies 420 may further comprise a delivery management system (e.g., corresponding to the “task management system” as described hereinbefore according to various embodiments) 421, and a plurality of delivery persons 422. Each delivery person may have a personal device 423, such as a mobile phone. A property of the plurality of properties 430 may further comprise a plurality of units 431 and an access control system 434. Each unit 431 may have one or more residents (or recipients or occupants) 432 with a personal device 433, such as mobile phone. An example of a third party data service 440 is a national digital identity system which has each citizen’s national identity number and face image. Another example of a third party data service 440 is a national digital health system which has each citizen’s health certificate, such as a digital coronavirus vaccination certification. The communication network 450 may support various connectivity, such as Internet, Ethernet, Wi-Fi, BLE (Bluetooth Low Energy), Zigbee, and various protocols, such as HTTP, RTSP, MQTT (Message Queueing Telemetry Transport), TCP/UDP, in a non-limiting example.

[0081] FIG. 5 shows a block diagram illustrating the components in a security authentication platform 410, according to various example embodiments. According to various example embodiments, the security authentication platform 410 may include, but is not limited to, a delivery company registration program 501, a property registration program 502, a delivery task registration program 503, a key pair generator 504, an encryption program 505, a decryption program 506, a two-dimensional barcode generator 507, a facial recognition program 508, an authentication program 509, a service quality report program 510, a plurality of third party data retrieval programs 530 (e.g., including face image retrieval program 531 and/or other third party data retrieval programs 532), and a database 520. The database 520 may include, but is not limited to, delivery company 521, property 522, third party data service 523, delivery task 524, key pair 525, encrypted face image 526, two-dimensional (2D) barcode 527, and service quality 528.

[0082] FIG. 6A shows an example of a flow diagram illustrating the exemplary steps of the delivery company registration program 501. At 610, the system receives registration information from a delivery company, such as company name, address, in a non-limiting example. At 620, the system allows the registering delivery company to
5 configure data communication interfaces, such as URL/IP address for HTTP interface. At 630, the system stores the delivery company information into the delivery company database 521.

[0083] FIG. 6B shows an example of the structure of the delivery company database 521, which may include, but is not limited to, a delivery company identifier (ID) 651,
10 a delivery company name 653, a delivery company address 655, information in relation to an interface from delivery company 657, and information in relation to an interface to delivery company 659.

[0084] FIG. 7A shows an example of a flow diagram illustrating the exemplary steps of the property registration program 502. At 710, the system receives registration
15 information from a property, such as property name, address, in a non-limiting example. The registration information may also include a threshold body temperature, above which the delivery person from a delivery company is not allowed to enter the property. At 720, the system allows the registering property to configure data communication interfaces, such as URL/IP address for HTTP interface. At 730, the system further
20 allows the registering property to configure third party data services (e.g., face image authentication, digital health certification, etc.) such as, for example, via an interface with a checklist menu from which third party data services may be selected as needed. At 740, the system stores the property information into the property database 522.

[0085] FIG. 7B shows an example of the structure of the property database 522,
25 which may include, but is not limited to, a property ID 751, a property name 753, a property address 755, information in relation to an interface from property 757, information in relation to an interface to property 759, a threshold of body temperature 761, and third party data services 763.

[0086] FIG. 7C shows an example of the structure of the third party data service database 523, which includes a mapping for each third party data service 771 and its
30 corresponding data retrieval program 773.

[0087] In various example embodiments, an occupant (or recipient) 432 in a property (of the plurality of properties 430) may request a delivery service, including delivery details and delivery address, to a delivery company (of the plurality of delivery

companies 420), via a personal device 433. The delivery company may first register a delivery task to the security authentication platform 410 in response to the requested delivery service.

[0088] FIG. 8 shows an example of a flow diagram illustrating the exemplary steps of a delivery task registration program 503. At 0801, the system receives a delivery task information in relation to a delivery task (e.g., corresponding to the “receiving second task information associated with the task” as described hereinbefore according to various embodiments) from a delivery company, such as delivery company, task location information associated with the task such as delivery address (e.g., property address, unit number, etc.), delivery person ID, expected arriving time. At 0802, the system generates a public and private key pair (Pub_key1, Pri_key1) (e.g., corresponding to the “generating a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task” as described hereinbefore according to various embodiments), by executing the key pair generator 504. At 0803, the system obtains face image of the delivery person (e.g., corresponding to the “obtaining first personal data associated with said person” as described hereinbefore according to various embodiments) using the face image retrieval program 531. At 0804, the system checks if the face image is obtained. If no, at 0810, the system returns “Registration Failed” to the delivery company. If yes, at 0805, the system further checks if additional data service is required by the property (registered during the property registration described with respect to FIG. 7A). If no, at 0808, the system generates a two-dimensional barcode. If yes, at 0806, the system obtains additional data by executing the corresponding data retrieval program, by looking up the third party data service database 523 (refer to FIG. 7C). At 0807, the system determines if the additional data service check is successful. If no, at 0810, the system returns “Registration Failed” to the delivery company. If yes, at 0808, the system generates a two-dimensional barcode, by executing the two-dimensional barcode generator 507. At 0809, the system returns “Registration Success” and sends the two-dimensional barcode to the delivery company (e.g., corresponding to the “sending the authentication code associated with the task to the task management system” as described hereinbefore according to various embodiments). It should be noted that if a delivery task registration is successful, the system will generate a unique delivery task ID (e.g., corresponding to the “task identification information associated with the task” as described hereinbefore according to various embodiments) and store

a delivery task to a delivery task table 524 with the unique delivery task ID. In other words, the delivery task ID is generated by the delivery task registration program 503. In addition, the system will store the unique delivery task ID and the key pair generated at 0802 to the key pair database 525.

5 **[0089]** Once received the “Registration Success” from the security authentication platform, the delivery company may send a notification to the occupant on the estimated arriving time, delivery person name, etc. In addition, the delivery company may send the two-dimensional barcode to the personal device 423 of the assigned delivery person 422.

10 **[0090]** FIG. 9 shows an example of a flow diagram illustrating the exemplary steps of a face image retrieval program 531. At 0910, the system sends the delivery person ID and the public key (Pub_key1) (e.g., corresponding to the first public key of the first private-public key pair) generated at 0802, to a third party data service (e.g., corresponding to the “sending a personal data request relating to said person to a third
15 party personal data provider, the personal data request comprising the person identification information associated with said person” as described hereinbefore according to various embodiments). At 0920, the system checks if an encrypted face image is received from the third party data service (e.g., corresponding to the “obtaining the first personal data associated with said person is obtained from the third party
20 personal data provider in response to the personal data request sent to the third party personal data provider” as described hereinbefore according to various embodiments). If yes, the system stores the encrypted face image to the encrypted face image database 526 and returns face image retrieval success. If no at 0920, at 0940, the system returns face image retrieval failed. In other words, the face image received from the third party
25 data service is encrypted using the public key (Pub_key1) from the security authentication platform, i.e., the first public key of the first private-public key pair.

30 **[0091]** FIG. 10 shows an example of the structure of the encrypted face image database 526, which may include, but is not limited to, a delivery person ID 1010, an encrypted face image from a third party data service 1020, and an encrypted face image from property access control system 1030 (refer to FIGS. 16A-16B).

[0092] FIG. 11A shows an example of the structure of the delivery task table 524, which may include, but is not limited to, a delivery task ID 1101, a delivery company 1102, a delivery person ID 1103, a delivery address 1104, a delivery person body

temperature 1105, a check-in time at a property 1106, and a check-out time at the property 1107.

[0093] FIG. 11B shows an example of the structure of the key pair database 525, which may include, but is not limited to, a delivery task ID 1101, a public key (e.g., corresponding to the first public key of the first private-public key pair) 1108, a private key (e.g., corresponding to the first private key of the first private-public key pair) 1109, and a public key from a property (e.g., corresponding to the second public key of the second private-public key pair) 1110.

[0094] FIG. 12A shows an example of a flow diagram illustrating the exemplary steps of a two-dimensional barcode generator 507. At 1201, the system sends delivery task information (e.g., corresponding to the “first task information” as described hereinbefore according to various embodiments), such as delivery task ID, delivery company, delivery address (e.g, property address, unit number, etc.), delivery person ID, and a public key (Pub_key1) to the property access control system 434. At 1202, the system receives a delivery task ID and a public key (Pub_key2) from the property (e.g., corresponding to the “second public key of a second private-public key pair of the access control system” as described hereinbefore according to various embodiments), and stores the public key, i.e., second public key, in the key pair database 525. It should be noted the delivery task ID received at 1202 is the same as the delivery task ID sent to the property at 1201. At 1203, the system creates one-time passcode by encrypting the delivery task ID, and the delivery person ID 1103, using the public key (Pub_key2) (e.g., corresponding to the “encrypting the task identification information associated with the task and the person identification information associated with said person based on the second public key to produce first encrypted data associated with the task” as described hereinbefore according to various embodiments). The encryption may be executed using the encryption program 505, such as an asymmetric encryption algorithm RSA. At 1204, the system generates a two-dimensional (2D) barcode (e.g., using a two-dimensional barcode generator) by encoding the delivery task ID and the one-time passcode (e.g., corresponding to the “encoding the first encrypted data and the task identification information associated with the task to generate the authentication code associated with the task” as described hereinbefore according to various embodiments), and stores it in a two-dimensional barcode database 527. For example, the two-dimensional barcode generator is a data

encoder to encode information into a two-dimensional image, in which data are present in both horizontal and vertical components of the image.

[0095] FIG. 12B shows an example of the structure of the two-dimensional barcode database 527, which may include, but is not limited to, a delivery task ID 1210, and a two-dimensional barcode 1220.

[0096] FIG. 13 shows a block diagram illustrating the components in an access control system 434 at a property. An access control system may include, but is not limited to, a delivery task registration program 1301, an access control program 1302, a check-out management program 1303, a key pair generator 1304, an encryption program 1305, a decryption program 1306, a two-dimensional barcode reading module 1307, a face image capturing module 1308, a body temperature measuring module 1309, and a database 1320. The database 1320 may further include, but is not limited to, delivery task database 1321, key pair database 1322, and two-dimensional barcode database 1323.

[0097] FIG. 14 shows an example of a flow diagram illustrating the exemplary steps of a delivery task registration program 1301. At 1401, the access control system receives a delivery task information from the security authentication platform 410 (e.g., corresponding to the “receiving first task information associated with the task from an authentication facilitating system” as described hereinbefore according to various embodiments), such as delivery task ID, delivery company, delivery address (property address, unit number, etc.), delivery person ID, and a public key (Pub_key1). The delivery task information and the public key (Pub_key1) will then be stored in a delivery task table (or database) 1321 and a key pair database 1322, respectively. At 1402, the system generates a public and private key pair (Pub_key2, Pri_key2) (e.g., corresponding to the “generating a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task” as described hereinbefore according to various embodiments), by executing the key pair generator 1304, and stores the key pair to the key pair database 1322. At 1403, the system returns the delivery task ID and a public key (Pub_key2) to the security authentication platform (e.g., corresponding to the “sending, in response to said receiving the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system” as described hereinbefore according to various embodiments).

[0098] FIG. 15A shows an example of the structure of a delivery task table 1321, which may include, but is not limited to, a delivery task ID 1501, a delivery company 1502, a delivery person ID 1503, a delivery address 1504, a delivery person body temperature 1505, a check-in time 1506, and a check-out time 1507.

5 [0099] FIG. 15B shows an example of the structure of the key pair database 1322, which may include, but is not limited to, a delivery task ID 1501, a public key (e.g., corresponding to the “second public key of the second private-public key pair”) 1508, a private key (e.g., corresponding to the “second private key of the second private-public key pair”) 1509, and a public key from the security authentication platform (e.g.,
10 corresponding to the “first public key of the first private-public key pair”) 1510.

[00100] When a delivery person 422 arrives at the property, the delivery person may first present the two-dimensional barcode, received from the delivery company, to the access control system 434, using a personal device 423 of the delivery person.

[00101] FIG. 16A shows an example of a flow diagram illustrating the exemplary steps of the access control program 1302. For example, the access control program may determine whether to grant access to a person to access the gated property based on the authentication code received. At 1601, the access control system may read a two-dimensional barcode presented by a delivery person (e.g., corresponding to the “receiving an authentication code associated with the task upon being utilized by said
20 person for accessing the gated property to perform the task” as described hereinbefore according to various embodiments). At 1602, the system decrypts the one-time passcode in the two-dimensional barcode using a private key (Pri_key2) (e.g., corresponding to the “decrypting the first encrypted data based on a second private key of the second private-public key pair associated with the task” as described hereinbefore according to various embodiments), by looking up the key pair database 1322 for the
25 corresponding delivery task ID. The decrypted one-time passcode comprises the delivery task ID, and the delivery person ID (e.g., refer to step 1203 in FIG. 12A). At 1603, the system checks if the delivery task is registered, by matching the delivery task ID and delivery person ID obtained in step 1602. If no, at 1609, the system will decline
30 the gate access. If yes at 1603, then at 1604, the system obtains face image and body temperature of the delivery person, using the face image capturing module 1308 and the body temperature measuring module 1309 (e.g., corresponding to the “obtaining second personal data from said person captured in real-time using a real-time personal data capturing device” as described hereinbefore according to various embodiments).

For example, with the latest facial recognition technology in the arts, a delivery person may even wear a mask during capturing of the face image. At 1605, the system encrypts the face image and body temperature using the corresponding public key (Pub_key1) 1510 for the delivery task ID (e.g., corresponding to the “encrypting the second personal data based on the first public key” as described hereinbefore according to various embodiments). At 1606, the system sends the delivery task ID and the encrypted data to the security authentication platform 410 (e.g., corresponding to the “sending an authentication request to the authentication facilitating system, the authentication request comprising the task identification information associated with the task and the second personal data associated with said person encrypted based on the first public key” as described hereinbefore according to various embodiments). At 1607, the system checks if the authentication success received from the security authentication platform. If yes, at 1608, the system grants gate access to the delivery person and records check-in time 1506. Otherwise, at 1609, the system declines the gate access to the delivery person.

[00102] FIG. 16B shows an example of the structure of a two-dimensional barcode database 1323, which may include, but is not limited to, a delivery task ID 1610, and a two-dimensional barcode 1620.

[00103] FIG. 17 shows an example of a flow diagram illustrating the exemplary steps of an authentication program 509 at the security authentication platform 410. At 1701, the system receives a delivery task ID and an encrypted data from a property (e.g., corresponding to the “receiving an authentication request from the access control system, the authentication request comprising the task identification information associated with the task and second personal data associated with said person, the second personal data being encrypted based on the first public key” as described hereinbefore according to various embodiments). At 1702, the system decrypts the data using a corresponding private key (Pri_key1) 1109 for the delivery task ID (e.g., corresponding to the “decrypting the second personal data based on a first private key of the first private-public key pair associated with the task” as described hereinbefore according to various embodiments). At 1703, the system looks up the pre-stored face image 1020 of delivery person ID from the encrypted face image database 526. At 1704, the system decrypts the pre-stored face image of the delivery person using the corresponding private key (Pri_key1) 1109 for the delivery task ID. At 1705, the system executes the facial recognition program 508, which will extract and match the face

features from the face image received from the property and the face image pre-stored. At 1706, the system checks if the facial recognition is successful (e.g., corresponding to the “determining whether the second personal data and the first personal data associated with the task satisfy one or more predetermined authentication conditions” as described hereinbefore according to various embodiments). If yes, at 1707, the system returns “Authentication Success” to the property (e.g., corresponding to the “sending an authentication response to the access control system” as described hereinbefore according to various embodiments), and store check-in time 1106. Otherwise, at 1708, the system returns “Authentication Failed” to the property (e.g., corresponding to the “sending an authentication response to the access control system” as described hereinbefore according to various embodiments). At 1709, the system may inform or send the authentication result to the delivery company. It should be noted that the authentication program may also check if the body temperature of the delivery person is above a threshold 761 (e.g., referring to FIG. 7B) pre-configured by the property. If so, the system may return “Authentication Failed” to the property.

[00104] Once the delivery person completes the delivery task and need to check-out from the property, the delivery person may present the same two-dimensional barcode to the access control system 434.

[00105] FIG. 18 shows an example of a flow diagram illustrating the exemplary steps of a check-out management program 1303. At 1801, the system reads the two-dimensional barcode presented by a delivery person. At 1802, the system grants gate access and record the check-out time 1507. At 1803, the system sends the delivery task ID and check-out time to the security authentication platform.

[00106] FIG. 19 shows an example of a flow diagram illustrating the exemplary steps of a service quality report program 510. At 1901, the system receives a delivery task ID and check-out time from a property (e.g., corresponding to the “receiving task performance information in relation to the task performed at the gated property from the access control system” as described hereinbefore according to various embodiments). At 1902, the system records the check-out time 1107 for the delivery task ID. At 1903, the system measures delivery quality, such as delay in arriving, dwell time at the property, etc. The delay in arriving may be measured using the expected arriving time received in the delivery task information at 0801 and the check-in time. The dwell time at the property may be measured using the check-in and check-out time. At 1904, the system generates a service quality report (e.g., corresponding to the

“generating a service quality report based on the task performance information” as described hereinbefore according to various embodiments), including service quality of the delivery company and benchmarking with other delivery company. The benchmarking may be an index of performance measured in a weighted function of delay in arriving and dwell time at the property over average performance of other delivery companies. At 1905, the system sends the service quality report to the corresponding delivery company of the delivery task ID (e.g., corresponding to the “sending the service quality report to the task management system” as described hereinbefore according to various embodiments).

10 [00107] FIG. 20 shows an example of the structure of the service quality database 528, which may include, but is not limited to, a delivery task ID 2001, a delivery company 2002, a delivery person ID 2003, a delivery address 2004, an expected arriving time 2005, a check-in time 2006, a check-out time 2007, and a delivery performance 2008.

15 [00108] According to various example embodiments, the access control system at a property may be equipped with facial recognition capability.

[00109] FIG. 21 shows a block diagram illustrating the components in an access control system 434 at a property, according to various other example embodiments (or various second example embodiments). The access control system may include components similar to that described in FIG. 13, and as such common features are not described in the interest of brevity. In various example embodiments, the access control system 434 may further comprise a facial recognition program 2110. The facial recognition program comprises a face feature extraction module 2111.

20 [00110] FIG. 22 shows an example flow diagram illustrating the exemplary steps of a property registration program 502, according to various other example embodiments (or various second example embodiments). At 2201, the system receives registration information from a property. At 2202, the system allows the registering property to configure data communication interfaces. At 2203, the system allows the registering property to register face feature extraction module. At 2204, the system further allows the registering property to configure third party data services. At 2205, the system stores the property information into a property database.

25 [00111] FIG. 23 shows an example flow diagram illustrating exemplary steps of a two-dimensional barcode generator 507, according to various other example embodiments (or various second example embodiments). At 2301, the system sends

delivery task information and a public key (Pub_key1) to the property access control system 434. At 2302, the system receives a delivery task ID and a public key (Pub_key2) from the property. At 2303, the system looks up the pre-stored face image 1020 of delivery person ID from the encrypted face image database 526. At 2304, the system decrypts the pre-stored face image of the delivery person using the corresponding private key (Pri_key1) 1109 for the delivery task ID. At 2305, the system extract face features, such as geometry of face, including pupil size, mouth width, eye size, nose width, head eccentricity, etc., (e.g., corresponding to “extracting features from the first personal data associated with said person” as described hereinbefore according to various embodiments) using the registered face feature extraction module (e.g., registered at 2203 in FIG. 22). At 2306, the system creates one-time passcode by encrypting the delivery task ID, the delivery person ID 1103, and the face features, using the public key (Pub_key2) (e.g., corresponding to “encrypting the task identification information and the person identification information further comprises encrypting said features based on the second public key to produce the first encrypted data associated with the task” as described hereinbefore according to various embodiments). At 2307, the system generates a two-dimensional barcode (using a 2-dimensional barcode generator) by encoding the delivery task ID and the one-time passcode, and stores it in a two-dimensional barcode database 527.

20 **[00112]** FIG. 24 shows an example of flow diagram illustrating the exemplary steps of an access control program 1302, according to various other example embodiments (or various second example embodiments). At 2401, the access control system may read a two-dimensional barcode presented by a delivery person. At 2402, the system decrypts the one-time passcode in the two-dimensional barcode using a private key (Pri_key2) (e.g., decrypting the first encrypted data to obtain the task identification information, person identification information associated with said person, and first personal data associated with said person such as face features for example) by looking up the key pair database 1322 for the corresponding delivery task ID. At 2403, the system checks if the delivery task is registered, by matching the delivery task ID and delivery person ID. If no, at 2409, the system will decline the gate access. If yes in 2403, at 2404, the system obtains face image and body temperature of the delivery person using the face image capturing module 1308 and body temperature measuring module 1309 (e.g., corresponding to the “obtaining second personal data from said person captured in real-time using a real-time personal data capturing device”). At

2405, the system extracts the face features from the face image obtained at 2404. At 2406, the system executes the facial recognition program 2110, by matching the face features obtained from step 2405 and the face features derived from step 2402 (e.g., corresponding to the “determining whether the second personal data and the first personal data associated with the task satisfy one or more predetermined authentication conditions” as described hereinbefore according to various embodiments). At 2407, the system checks if the authentication is successful. If yes, at 2408, the system grants gate access to the delivery person and records check-in time. Otherwise, at 2409, the system declines the gate access to the delivery person.

10 [00113] FIG. 25 shows a schematic diagram of an overall system, such as the authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various other example embodiments (or various third example embodiments). The system further includes a plurality of E-Commerce platforms 2560. An occupant 432 in a property 430 may request a delivery service to
15 an E-Commerce platform. The E-Commerce platform may select different delivery company to fulfill a delivery task. The selected delivery company will then register the delivery task information to the security authentication platform, as illustrated in FIG. 8.

[00114] Once a delivery task completed, a service quality report program in the
20 security authentication platform may send a service quality report to the corresponding delivery company and the E-Commerce platform of the delivery task.

[00115] A delivery company 420 may also register face images of the delivery persons 422 to the security authentication platform 410, during the delivery company registration process (e.g., corresponding to “the second task information received from
25 the task management system further comprises the first personal data associated with said person, and said obtaining the first personal data associated with said person is obtained from the task management system” as described hereinbefore according to various embodiments). The authentication program 509 will then use the pre-registered face image, instead of obtaining from a third party data service.

30 [00116] FIG. 26A and FIG. 26B show schematic diagrams of an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments.

[00117] FIGS. 27A-27H illustrate exemplary scenarios for authenticating a person for accessing a gated property to perform a task therein, according to various example embodiments.

5 [00118] FIG. 28 illustrates a schematic diagram of an authentication system for authenticating a person for accessing a gated property to perform a task therein, according to various second example embodiments. For example, the authentication facilitating system may include a face feature extraction module. Similarly, the access control system of the gated property may include a face feature extraction module. For example, feature (e.g., facial features) extraction from the first personal data associated
10 with said person may be performed by the authentication facilitating system, while feature extraction from the second personal data associated to the person captured in real-time may be performed by the access control system.

[00119] FIGS. 29A-29B illustrates another exemplary scenario for authenticating a person for accessing a gated property to perform a task therein, according to various
15 second example embodiments. For example, the authentication facilitating system may perform feature extraction from the first personal data associated with said person. The extracted features may be encrypted based on the second public key to produce the first encrypted data associated with the task. The authentication code associated with the task may be generated based on the first encrypted data. For example, the authentication
20 code associated with the task may be sent to the task management system for said person to utilize for accessing the gated property to perform the task. As illustrated in FIG. 29B, the authentication code associated with the task may be received at the access control system when the person associated with the task arrives at the gated property and scans the authentication code. Second personal data captured in real-time may be
25 obtained from said person using a real-time personal data capturing device. The access control system may perform feature extraction from the second personal data associated with said person. Accordingly, a first authentication may be performed to match the task identification information and a second authentication may be performed to match features extracted from the first personal data and features extracted from the second
30 personal data. In other words, both the first authentication and the second authentication may be performed by the access control system.

[00120] Various example embodiments may be used to implement an intermediate platform that provides security authentication to realize a fully automated and contactless delivery service for a gated property, such as condominium, hotel, office,

etc. The system provides security authentication using two-factor and multi-party authentication with asymmetric encryption, without requirement of pre-registration of privacy data (or personal data), such as face image of the delivery person at a property. The system also provides service quality measurement and benchmarking report for a delivery service.

[00121] Various example embodiments also allow a gated property to customize various third party data service for security authentication, such as face image authentication, digital health certificate, with a single interface between the property and the security authentication platform.

10 [00122] While embodiments of the invention have been particularly shown and described with reference to specific embodiments, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come
15 within the meaning and range of equivalency of the claims are therefore intended to be embraced.

CLAIMS

What is claimed is:

- 5 1. A method of facilitating authentication of a person for accessing a gated property to perform a task therein, using at least one processor of an authentication facilitating system, the method comprising:
- generating a first private-public key pair of the authentication facilitating system, the first private-public key pair being associated with the task;
- 10 obtaining first personal data associated with said person;
- sending first task information associated with the task to an access control system of the gated property, the first task information comprising task identification information associated with the task, person identification information associated with said person, and a first public key of the first private-public key pair;
- 15 receiving, in response to said sending the first task information to the access control system, a second public key of a second private-public key pair of the access control system of the gated property from the access control system, the second private-public key pair being associated with the task; and
- generating an authentication code associated with the task based on the second
- 20 public key for said person to utilize for accessing the gated property to perform the task.
2. The method according to claim 1, wherein said generating the authentication code associated with the task based on the second public key comprises:
- encrypting the task identification information associated with the task and the
- 25 person identification information associated with said person based on the second public key to produce first encrypted data associated with the task; and
- encoding the first encrypted data and the task identification information associated with the task to generate the authentication code associated with the task.
- 30 3. The method according to claim 2, wherein the authentication code is a graphical barcode.
4. The method according to claim 3, wherein the authentication code is a two-dimensional (2D) barcode.

5. The method according to any one of claims 2 to 4, further comprising receiving second task information associated with the task from a task management system for registering the task with the authentication facilitating system, the second task
5 information comprising the person identification information associated with said person and task location information associated with the task,
wherein said generating the first private-public key pair associated with the task is in response to the second task information associated with the task received from the task management system.
- 10 6. The method according to claim 5, wherein the first task information is sent to the access control system based on the task location information associated with the task.
- 15 7. The method according to claim 5 or 6, further comprising sending the authentication code associated with the task to the task management system for said person to utilize for accessing the gated property to perform the task.
- 20 8. The method according to any one of claims 5 to 7, further comprising:
sending a personal data request relating to said person to a third party personal data provider, the personal data request comprising the person identification information associated with said person,
wherein said obtaining the first personal data associated with said person is obtained from the third party personal data provider in response to the personal data
25 request sent to the third party personal data provider.
9. The method according to claim 8, wherein
the personal data request further comprises the first public key, and
the first personal data is encrypted based on the first public key.
- 30 10. The method according to any one of claims 5 to 7, wherein
the second task information received from the task management system further comprises the first personal data associated with said person, and

said obtaining the first personal data associated with said person is obtained from the task management system.

11. The method according to any one of claims 5 to 10, further comprising
5 extracting features from the first personal data associated with said person, wherein
said encrypting the task identification information and the person identification
information further comprises encrypting said features based on the second public key
to produce the first encrypted data associated with the task.

10 12. The method according to any one of claims 5 to 10, further comprising:
receiving an authentication request from the access control system, the
authentication request comprising the task identification information associated with
the task and second personal data associated with said person, the second personal data
being encrypted based on the first public key;
15 decrypting the second personal data based on a first private key of the first
private-public key pair associated with the task;
determining whether the second personal data and the first personal data
associated with the task satisfy one or more predetermined authentication conditions;
and
20 sending an authentication response to the access control system,
wherein the authentication response indicates authentication successful if the
second personal data and the first personal data associated with the task satisfy the one
or more predetermined authentication conditions, and indicates authentication
unsuccessful if the second personal data and the first personal data associated with the
25 task do not satisfy the one or more predetermined authentication conditions.

13. The method according to claim 12, wherein the one or more predetermined
authentication conditions comprises a predetermined matching condition that the
second personal data and the first personal data are determined to match each other.

30 14. The method according to any one of claims 5 to 13, further comprising:
receiving task performance information in relation to the task performed at the
gated property from the access control system;
generating a service quality report based on the task performance information;

sending the service quality report to the task management system.

15. The method according to any one of claims 5 to 14, wherein
the task is a delivery task; and
5 the task management system is associated with a company which provides a
delivery service.
16. The method according to any one of claims 1 to 15, wherein the first personal
data associated with said person comprises a face image of said person.
10
17. The method according to claim 16, wherein the first personal data associated
with said person further comprises a health-related status of said person.
18. An authentication facilitating system for facilitating authentication of a person
15 for accessing a gated property to perform a task therein, the authentication facilitating
system comprising:
a memory; and
at least one processor communicatively coupled to the memory and configured
to perform the method of facilitating authentication of the person for accessing the gated
20 property according to any one of claims 1 to 17.
19. A computer program product, embodied in one or more non-transitory
computer-readable storage mediums, comprising instructions executable by at least one
processor to perform the method of facilitating authentication of the person for
25 accessing the gated property according to any one of claims 1 to 17.
20. A method of controlling access of a person to a gated property to perform a task
therein, using at least one processor of an access control system of the gated property,
the method comprising:
30 receiving first task information associated with the task from an authentication
facilitating system, the first task information comprising task identification information
associated with the task, person identification information associated with said person,
and a first public key of a first private-public key pair of the authentication facilitating
system;

generating a second private-public key pair of the access control system of the gated property, the second private-public key pair being associated with the task;

5 sending, in response to said receiving the first task information from the authentication facilitating system, a second public key of the second private-public key pair to the authentication facilitating system;

receiving an authentication code associated with the task upon being utilized by said person for accessing the gated property to perform the task, the authentication code being generated based on the second public key; and

10 determining whether to grant access to said person to access the gated property based on the authentication code received.

21. The method according to claim 20, wherein

the authentication code associated with the task has encoded therein first encrypted data and the task identification information associated with the task; and

15 the first encrypted data associated with the task comprises the task identification information associated with the task and the person identification information associated with said person encrypted based on the second public key.

22. The method according to claim 21, wherein the authentication code is a
20 graphical barcode.

23. The method according to claim 22, wherein the authentication code is a 2D barcode.

25 24. The method according to any one of claims 21 to 23, further comprising:

decoding the authentication code to obtain the first encrypted data and the task identification information associated with the task; and

30 decrypting the first encrypted data based on a second private key of the second private-public key pair associated with the task to obtain the task identification information associated with the task and the person identification information associated with said person.

25. The method according to claim 24, further comprising obtaining second personal data from said person captured in real-time using a real-time personal data capturing device.

5 26. The method according to claim 25, further comprising:
encrypting the second personal data based on the first public key; and
sending an authentication request to the authentication facilitating system, the authentication request comprising the task identification information associated with the task and the second personal data associated with said person encrypted based on
10 the first public key; and
receiving, in response to the authentication request sent to the authentication facilitating system, an authentication response from the authentication facilitating system,
wherein said determining whether to grant access to said person is further based
15 on the authentication response received.

27. The method according to claim 25, wherein
the first encrypted data associated with the task further comprises features extracted from first personal data associated with said person encrypted based on the
20 second public key, and
the method further comprises:
decrypting the first personal data based on the second private key of the second private-public key pair associated with the task;
determining whether the second personal data and the first personal data
25 associated with the task satisfy one or more predetermined authentication conditions; and
generating an authentication response based on said determining whether the second personal data and the first personal data associated with the task satisfy one or more predetermined authentication conditions, wherein
30 the authentication response indicates authentication successful if the second personal data and the first personal data associated with the task satisfy the one or more predetermined authentication conditions, and indicates authentication unsuccessful if the second personal data and the first personal data associated with the task do not satisfy the one or more predetermined authentication conditions, and

said determining whether to grant access to said person is further based on the authentication response generated.

28. The method according to claim 27, wherein the one or more predetermined authentication conditions comprise a predetermined matching condition that the second personal data and the first personal data are determined to match each other.

29. The method according to any one of claims 20 to 28, further comprising:
sending task performance information in relation to the task performed at the gated property to the authentication facilitating system.

30. The method according to any one of claims 20 to 29, wherein the task is a delivery task.

31. The method according to any one of claims 20 to 30, wherein the first personal data associated with said person comprises a face image of said person.

32. The method according to claim 31, wherein the first personal data associated with said person further comprises a health-related status of said person.

33. An access control system for controlling access of a person to a gated property to perform a task therein, the access control system comprising:
a memory; and
at least one processor communicatively coupled to the memory and configured to perform the method of controlling access of the person to the gated property according to any one of claims 20 to 32.

34. A computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform the method of controlling access of the person to the gated property according to any one of claims 20 to 32.

35. An authentication system for authenticating a person for accessing a gated property to perform a task therein, the authentication system comprising:

the authentication facilitating system according to claim 18, and
the access control system according to claim 33.