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.

[00122] Various examples are provided.

[00123] Example 1 is 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.

[00124] Example 2 is the method according to Example 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 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.

[00125] Example 3 is the method according to Example 2, wherein the authentication code is a graphical barcode.

[00126] Example 4 is the method according to Example 3, wherein the authentication code is a two-dimensional (2D) barcode.

[00127] Example 5 is the method according to any one of Examples 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 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.

[00128] Example 6 is the method according to Example 5, wherein the first task information is sent to the access control system based on the task location information associated with the task.

[00129] Example 7 is the method according to Example 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.

[00130] Example 8 is the method according to any one of Examples 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 request sent to the third party personal data provider.

[00131] Example 9 is the method according to Example 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.

[00132] Example 10 is the method according to any one of Examples 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.

[00133] Example 11 is the method according to any one of Examples 5 to 10, further comprising 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.

[00134] Example 12 is the method according to any one of Examples 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; 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, 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 task do not satisfy the one or more predetermined authentication conditions.

[00135] Example 13 is the method according to Example 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.

[00136] Example 14 is the method according to any one of Examples 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.

[00137] Example 15 is the method according to any one of Examples 5 to 14, wherein the task is a delivery task; and the task management system is associated with a company which provides a delivery service.

[00138] Example 16 is the method according to any one of Examples 1 to 15, wherein the first personal data associated with said person comprises a face image of said person.

[00139] Example 17 is the method according to Example 16, wherein the first personal data associated with said person further comprises a health-related status of said person.

[00140] Example 18 is 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 any one of Examples 1 to 17.

[00141] Example 19 is 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 any one of Examples 1 to 17.

[00142] Example 20 is 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.

[00143] Example 21 is the method according to Example 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 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.

[00144] Example 22 is the method according to Example 21, wherein the authentication code is a graphical barcode.

[00145] Example 23 is the method according to Example 22, wherein the authentication code is a 2D barcode.

[00146] Example 24 is the method according to any one of Examples 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 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.

[00147] Example 25 is the method according to Example 24, further comprising obtaining second personal data from said person captured in real-time using a real-time personal data capturing device.

[00148] Example 26 is the method according to Example 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 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 on the authentication response received.

[00149] Example 27 is the method according to Example 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 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 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 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.

[00150] Example 28 is the method according to Example 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.

[00151] Example 29 is the method according to any one of Examples 20 to 28, further comprising: sending task performance information in relation to the task performed at the gated property to the authentication facilitating system.

[00152] Example 30 is the method according to any one of Examples 20 to 29, wherein the task is a delivery task.

[00153] Example 31 is the method according to any one of Examples 20 to 30, wherein the first personal data associated with said person comprises a face image of said person.

[00154] Example 32 is the method according to Example 31, wherein the first personal data associated with said person further comprises a health-related status of said person.

[00155] Example 33 is 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 Examples 20 to 32.

[00156] Example 34 is 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 Examples 20 to 32.

[00157] Example 35 is 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 Example 18, and the access control system according to Example 33.

[00158] 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 within the meaning and range of equivalency of the claims are therefore intended to be embraced.