

CLAIMS

1. A method for verification of presence, comprising:

5 reading an identifier from a Near Field Communication (NFC) tag fixedly coupled to a location by a NFC-enabled device, wherein the identifier is associated with the location;

recording a check-in time according to the time of reading the identifier;

verifying the received identifier against an identifier database to identify the location corresponding to the received identifier;

10 generating a query based on the verified location to solicit a user input entered by a user in charge of the location;

receiving the user input by the NFC-enabled device; and

recording a check-out time according to the time of receiving the user input, wherein the user input is generated according to the following steps:

15 generating a password component from a plurality of characters of a pre-assigned password which is associated with the user; and

randomly inserting a non-password component into the generated password component;

20 wherein the non-password component includes a plurality of variable characters, determined by the user or a user device;

~~wherein randomly inserting the non-password component includes: inserting and the~~
plurality of variable characters are inserted at non-adjacent positions in the generated password component,

25 wherein at least some of the variable characters of the non-password component are arranged in a predefined sequence to reflect a predetermined information which is not password-related information and is determined by the user.

30 2. The method of claim 1, wherein the predetermined information determined by the user comprises at least one of feedback information about a service quality or amount of monetary reward.

23. The method of claim 1, further comprising:
ascertaining a duration of presence based on the check-in time and the check-out time.
34. The method of claim 1, wherein the pre-assigned password includes a plurality of sub-passwords, each sub-password having a plurality of characters provided in a predefined sequence,
wherein generating a password component includes:
dividing each sub-password into a plurality of subsets,
wherein randomly inserting a non-password component includes:
interposing the subsets of one sub-password with the subsets of at least another sub-password, wherein an aggregation of the interposed subsets of each sub-password conforms to the corresponding defined sequence of the each sub-password.
45. The method of claim 1, wherein the pre-assigned password includes a plurality of characters in a non-defined sequence, and
wherein generating a password component includes generating a random permutation of the plurality of characters.
- ~~5. The method of claim 1, wherein the non-password component includes at least one variable character to reflect an evaluation of a service rendered between the check-in time and the check-out time and/or a monetary value determined by the user.~~
- ~~6. The method of claim 1, wherein at least some of the variable characters of the non-password component are arranged in a sequence to reflect a pre-determined information determined by the user.~~
- ~~76. The method of claim 1, the pre-assigned password or at least part of the pre-assigned password which is associated with the user is generated by a key token assigned to the user, or sent to the user by a SMS.~~

| 87. The method of claim 1, further comprising:

after receiving the user input, verifying a presence of a pre-assigned password within the received user input, wherein the pre-assigned password is
5 associated with the user and stored in a first database.

| 98. The method of claim 87, wherein the pre-assigned password includes a plurality of characters provided in a non-defined sequence, and wherein verifying a presence of the pre-assigned password includes verifying a presence of all the plurality of
10 characters of the pre-assigned password in the received user input.

| 109. The method of claim 87, wherein the pre-assigned password includes a plurality of sub-passwords, each sub-password including a plurality of characters provided in a predefined sequence,

15 wherein verifying a presence of the pre-assigned password includes verifying a presence of all of the plurality of characters of each sub-password within the user input and verifying an aggregation of the verified characters corresponding to each sub-password conforms to the corresponding predefined sequence of the each sub-password.

20

| 1110. The method of any one of claims 87 to 109, further comprising:

identifying the non-password component based on the verified presence of the pre-assigned password within the received user input,

25 | 1211. The method of claim 1110, further comprising:

ascertaining a validity of the user input by comparing the non-password component against a second database which includes a plurality of historical non-password components from the user; and

establishing the user input is valid and storing the non-password component
30 in the second database if the non-password component does not correspond to any of the plurality of historical non-password components.

4312. The method of claim 1, further comprising:

ascertaining a validity of the received user input by comparing the received user input against a third database which includes a plurality of historical user inputs from the user; and

5 establishing the received user input is valid and storing the received user input in the third database if the received user input does not correspond to any of the plurality of historical user inputs.

10 1413. A non-transitory computer readable medium encoded with program code operable, when loaded on a computer, to effect the method of any of claims 1 to 1312.

15 1514. A system for verification of presence, comprising:

a Near Field Communication (NFC) tag fixedly coupled to a location, the NFC tag being assigned an identifier associated with the location;

a NFC-enabled device comprising a NFC tag reader, a memory, a processor communicatively coupled to the NFC tag reader and the memory, and configured to execute program code stored in the memory, the program code comprising:

20 an application module configured to: cause the tag reader read the NFC tag,

verify the identifier read by the tag reader against an identifier database to identify the location corresponding to the received identifier,

generate a query based on the verified location,

25 receive a user input entered by a user in response to the query,

record a time of reading the identifier as a check-in time,

record a time of receiving the answer as a check-out time,

30 wherein the user input includes a password component generated from a plurality of characters of a pre-assigned password which is associated with the user and a non-password component, ~~wherein the password component includes a plurality of characters, the non-password component which~~ includes a plurality of variable characters ~~determined by a user or a user device~~, and the plurality of

variable characters of the non-component password are randomly inserted at non-adjacent positions in the generated password component, wherein at least some of the variable characters of the non-password component are arranged in a predefined sequence in the password component to reflect a predetermined
5 information which is not password-related information and is determined by the user;
and

the system further comprising:

a verification module configured to verify a presence of a pre-assigned password within the user input and identify the non-password component based on
10 the verified presence of the pre-assigned password within the received user input, wherein the pre-assigned password is stored in a first database and associated with the user.

15 15. The system of claim 14, wherein the predetermined information determined by the user comprises at least one of feedback information about a service quality or amount of monetary reward.

20 ~~16. The system of claim 15, wherein at least some of the variable characters of the non-password component are arranged in a sequence to reflect a pre-determined information determined by the user.~~

~~17. The system of claim 16, wherein the non-password component includes an evaluation of a service rendered between the check-in time and the check-out time.~~

25 ~~18. The system of claim 16, wherein the non-password component includes a monetary reward value.~~

30 ~~19~~16. The system of claim 15, wherein the verification module is further configured to:

ascertain a validity of the user input by comparing the non-password component against a second database which includes a plurality of historical non-password components from the user,

establish the user input is valid if the non-password component does not
5 correspond to any of the plurality of historical non-password components, and store the non-password component in the second database.

2017. The system of any one of claim 14 to claim 16, wherein the verification
module is stored in the memory of the NFC-enabled device included in the program
10 code stored in the memory of the NFC-enabled device, or stored in a remote server
which is communicatively coupled to the NFC-enabled device.

218. The system of claim 2017, wherein the identifier database, the first database
15 and the second database are stored in the memory of the NFC-enabled device.

219. The system of claim 14, wherein the pre-assigned password includes a
plurality of characters provided in a non-defined sequence, and
wherein the verification module is further configured to:
20 verify a presence of all the plurality of characters of the pre-assigned
password in the received user input.

220. The system of claim 14, wherein the pre-assigned password includes a
plurality of sub-passwords, each sub-password including a plurality of characters
25 provided in a predefined sequence,

wherein the verification module is further configured to:
verify a presence of all of the plurality of characters of each sub-
password within the user input, and
verify an aggregation of the verified characters corresponding to each
30 sub-password conforms to the corresponding predefined sequence of the
each sub-password.