

SYSTEM AND METHOD FOR ACCESS CONTROL

FIELD OF INVENTION

5 The invention broadly relates to a system and method for controlling access to one or more locations.

BACKGROUND

10 During an outbreak of an infectious disease (e.g. Influenza A H1N1, Influenza A H5N1 (Avian), Severe Acute Respiratory Syndrome (SARS)), in order to contain the spread of the disease and to facilitate contact tracing (i.e.: the identification and diagnosis of persons who may have come into contact with an infected person), it is common for visitors of a hospital or commercial building and passengers arriving at
15 the airport to fill out health declaration forms and possibly have their body temperatures measured before entry is permitted. However, this practice is time consuming and inconvenient for hospital / building staff, immigration officers and visitors.

20 In order to visit a building or hospital, an individual typically has to queue up to obtain a health declaration form, fill up the form (possibly using the same pen which has already been touched by many people), and finally queue up again to submit the form in exchange for a visitor's pass. The entire process, which typically takes about 10 minutes, is repeated when he visits other buildings and/or hospitals. The process
25 generally involves additional manpower to process the visitors; raises the probability of infection due to close contact between infected visitors, hospital and building staff. In addition, in the event an infected visitor inadvertently enters a location such that contact tracing is required, the process can be slow and tedious as health officials have to first interview the infected visitor to establish his recent whereabouts and thereafter
30 physically checking the records of the places he has visited to obtain a list of persons who may have come into contact with him. Subsequently, health officials typically need to individually contact the persons on the list to inform them to undergo tests to determine if they have been infected. Further, visitors' passes and pens, if not disinfected regularly, can also be a medium for the spread of disease.

A need therefore exists to provide a system and method for controlling access to one or more locations that seeks to address at least one of the abovementioned problems.

5 SUMMARY

In accordance with a first aspect of the present invention, there is provided an apparatus for access control, the apparatus comprising: a label reader for reading an encoded label; and a processor for extracting primary identity information and a
10 health risk score from a read encoded label; wherein access is granted based on the extracted health risk score.

The encoded label may comprise a 2-D barcode.

15 The apparatus may further comprise: a biometric reader for reading biometric data of a person; means for determining symptoms of a communicable disease from the biometric data, means for associating the read biometric data, the determined symptoms, or both, with said person based on the identity information extracted from the read 2-D bar code; and wherein access is further granted based on the
20 determined symptoms.

The biometric reader may comprise a non-contact biometric reader.

The non-contact biometric reader may comprise a temperature sensing
25 device.

The temperature sensing device may comprise an infrared thermometer.

The apparatus may further comprise: means for reading secondary
30 identification information presented by the user, and wherein access is further granted based on a comparison of the first and second identification information.

The means for reading the secondary identification information may comprise one or more of a group consisting of a 1-D barcode reader, the 2-D barcode reader,
35 an iris scanner, a palm vein scanner and a radio-frequency identification scanner.

The apparatus may further comprise an interface for connection to a remote server.

5 In accordance with a second aspect of the present invention, there is provided a method of access control, the method comprising the steps of: reading a an encoded label using a label reader; and extracting primary identity information and a health risk score from the read encoded label by means of a processor; wherein access is granted based on the extracted health risk score.

10 The encoded label may comprise a 2-D barcode.

The method may further comprise the steps of: reading biometric data of a person using a biometric reader; determining symptoms of a communicable disease from the biometric data; associating the read biometric data, the determined
15 symptoms, or both, with said person based on the identity information extracted from the read 2-D barcode; and wherein access is further granted based on the determined symptoms.

The biometric reader may comprise a non-contact biometric reader.
20

The non-contact biometric reader may comprise a temperature sensing device.

The temperature sensing device may comprise an infrared thermometer.
25

The method may further comprise the steps of reading secondary identification information presented by the user, and wherein access is further granted based on a comparison of the first and second identification information.

30 The secondary identification information may be read using one or more of a group consisting a 1-D barcode reader, a 2-D barcode reader, an iris scanner, a palm vein scanner and a radio-frequency identification scanner.

The method may further comprise the steps of connecting to a remote server
35 by means of an interface.

In accordance with a third aspect of the present invention, there is provided a method of contact tracing using the apparatus according to the first aspect of the present invention.

5 The method may comprise the steps of: obtaining a person's health declaration via a server; calculating the health risk score based on the health declaration; and issuing of the 2-D barcode comprising the primary identity information and the health risk score.

10 The primary identity information of persons granted access may be stored in a database of the apparatus for the contact tracing.

In accordance with a fourth aspect of the present invention, there is provided a method of tracking a person using the apparatus according to the first aspect of the
15 present invention.

 The method may comprise the steps of: obtaining a person's health declaration via a server; calculating the health risk score based on the health declaration; and issuing of the 2-D barcode comprising the primary identity
20 information and the health risk score.

 The primary identity information of persons having used the apparatus may be stored in a database of the apparatus for the tracking.

25 In accordance with a fifth aspect of the present invention, there is provided a system for access control, the system comprising the apparatus according to the first aspect of the present invention and a remote server coupled.

 The server may be configured for obtaining a person's health declaration, for
30 calculating the health risk score based on the health declaration; and for issuing of the 2-D barcode comprising the primary identity information and the health risk score.

BRIEF DESCRIPTION OF THE DRAWINGS

Example embodiments of the 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:

Figure 1 is a schematic drawing illustrating a system for health declaration and access control according to an embodiment of the present invention.

Figure 2 is a flow chart illustrating the steps that a user takes in order to obtain a QR-code, according to an embodiment of the present invention.

Figure 3 is a schematic drawing of a front view of a kiosk according to an embodiment of the present invention.

Figure 4 is a flow chart illustrating the steps a user takes to obtain a visitor's pass in order to gain access into a building, according to an embodiment of the present invention.

Figure 5 is a flow chart illustrating the steps of a method of access control, according to an embodiment of the present invention.

DETAILED DESCRIPTION

Figure 1 is a schematic drawing, illustrating a system for health declaration and access control, generally referred to as reference numeral 100, according to an embodiment of the present invention. The system for health declaration and access control 100 comprises a server 102 and a plurality of kiosks 104a / 104b / 104c (for illustrative purposes, only three kiosks are shown here). The server 102 comprises an internet website 106, a database 107, server software 108 and a web service 109. The server 102 is connected to the plurality of kiosks 104a / 104b / 104c through the web service 109 and they can communicate via telecommunication protocols such as Simple Object Access Protocol (SOAP) or Hypertext Transfer Protocol (HTTP). It will be appreciated by a person skilled in the art that the web service 109 supports interaction between the server 102 and the plurality of kiosks 104a / 104b / 104c over the network. The web service 109 may be a REpresentational State Transfer (RESTful) web service. The database 107 stores data such as a user's health

declaration, personal particulars (name, identity card number, passport number, address, various contact numbers, email address) and travel history. The server software 108 advantageously processes the information exchanged between the plurality of kiosks 104a / 104b / 104c and from the website 106 and stores and/or updates data in the database 107, if necessary. The website 106 is preferably developed using web development techniques such as Asynchronous JavaScript and XML (AJAX). The framework for the server software 108 is preferentially implemented using the Apache AXIS framework.

Users with computers or cellular phones 110a – 100e (for illustrative purposes, only six devices are shown here) can connect to the internet website 106 via telecommunication protocols such as HTTP or Wireless Application Protocol (WAP). The website can send data to a cellular phone (e.g.: 110a) via Short Message Service (SMS) or Multimedia Messaging Service (MMS).

Figure 2 is a flow chart, generally referred to as reference numeral 200, illustrating the steps that a user takes in order to obtain an encoded label, implemented here in the form of a 2-D barcode, preferably in the form of a QR-code, according to an embodiment of the present invention. It will be appreciated by a person skilled in the art that other types of 2-D barcodes, for example ColorCode, Data Matrix, Microsoft Tag and PDF417 may be used as an alternative to the QR-code. At step 202, the user with a computer or cellular phone having internet capabilities accesses the internet website 106. At step 204, the user enters an identification number such as his passport or identity card number to log onto the website 106. At step 206, it is determined, by the identification number, if the user is an existing or new user. If he is a new user, he can register himself at step 208. If he is an existing user, the user enters his password for authentication purposes at step 210. In the event that the entered password is incorrect, the user is able to re-enter his password at step 212. At step 214, upon entering an incorrect password for the second consecutive time, the user's password is re-set. A new password is then sent to the user via email or SMS as shown in step 215. Once a correct password is entered at steps 210 or 212, the user inputs or updates (if applicable) his personal data (e.g.: identity card number, passport number, name, address, various contact numbers) and completes a health declaration that preferentially comprises a series of questions, as shown at step 216. Through the answers that are given in response to the series of questions, a health declaration score is preferably generated. The score is compared to pre-determined values to classify if the user is a "high-risk" individual

who could possibly be infected and can be denied entry to a location or is a "low-risk" individual who does not exhibit symptoms and can be allowed entry to a location.

Each time a health declaration is made by the user, a unique health declaration identification number is assigned to that health declaration, and is advantageously represented by a QR-Code. The QR-code is generated at step 218. The QR-Code is preferably embedded with data such as the user's primary identity information (e.g.: identity card number), name, contact numbers, health declaration identification number and the health declaration score. Each QR-Code is tied to both the user's particulars, health declaration score and health declaration identification number.

At step 220, the QR-Code is sent via MMS to the user's cellular phone. In the event that the transmission is unsuccessful or the user does not have a cellular phone, the QR-Code is sent via email to the user as shown at step 222. The user also can have the option of printing out the QR-code, either directly from the website, or later from the received MMS or email.

With the QR-Code obtained at step 224 (i.e.: either displayed on a cellular phone or computer screen; or a physical print-out), the user can visit any location equipped with a kiosk (e.g.: 104a / 104b / 104c), and obtain a visitor's pass without the hassle of continuously queuing up and filling out health declaration forms at every location the user visits.

A validity period of a QR-code can be set for a pre-determined amount of time, for example, 24 hours. In this instance, once the QR-code has expired, the user re-accesses the website 106 and completes another health declaration in order to obtain another valid QR-code for access. The validity period of the QR-code advantageously encourages users to constantly update their health declaration.

30

In addition, the user's health declaration can be modified when the need arises. For example, if the user starts feeling unwell and shows symptoms of the disease, he can update the health declaration accordingly. In other words, the user can create multiple health declarations, each with a unique QR-Code, but there can be at most one valid declaration as previous declarations are superseded by the latest declaration (i.e.: the previous QR-code is invalidated). If the user's QR-code is invalid, upon attempting to gain access at the kiosk 300, access is denied.

Figure 3 is a schematic drawing of a front view of a kiosk, generally referred to as reference numeral 300, according to an embodiment of the present invention. The kiosk 300 is preferably located at the entrance of a commercial building or hospital; or immigration checkpoint in order to control access. The kiosk 300 comprises a surveillance camera 302; a biometric reader, implemented here as a non-contact biometric reader in the form of an infrared thermometer 304; a label reader, for example a 2-D barcode scanner, and implemented here in the form of a micro lens camera 306; a 1D barcode scanner 307; a monitor screen 308; a printer 310; a siren and warning light 312; a panic button 314; a speaker and microphone unit 316; and a main control unit (not shown). Users preferably present their QR-code at the kiosk 300 for verification of their identity and health status to obtain a visitor's pass in order to gain entry into the commercial building or hospital.

The surveillance camera 302 is preferably a high resolution camera such as VARIFOCAL EXTREME III SPORTS CAM (Using EXview-HAD CCD), and is advantageously connected to a recording unit (not shown). The surveillance camera 302 can display its captured images on the monitor screen 308. The surveillance camera 302 can record the activity around the kiosk 300 for security and contact tracing purposes. It will be appreciated by a person skilled in the art that depending on symptoms associated with the communicable disease, various types of biometric readers for reading biometric data of a person can be installed in the kiosk 300. For illustrative purposes, in the event of an outbreak of a disease whereby symptoms include an infected person exhibiting an increased body temperature (e.g.: Influenza A H1N1), the infrared thermometer 304 can be used to measure the user's temperature. The infrared thermometer 304 is preferably of industrial grade, substantially high accuracy, and is capable of long distance temperature measurement such as CT laser LT by optris. The temperature reading can be displayed on the monitor screen 308. If the user exhibits a temperature above a pre-determined threshold, access is denied, an alarm may be triggered and the siren and warning light 312 activated to notify hospital / building staff and/or immigration officers. The user's abnormal temperature reading can be updated in the server 102 so as to prevent the user from making subsequent entries into any other building with a kiosk installed. The infrared thermometer 304 minimizes human contact and is substantially faster compared to other methods of temperature measurement such as ear thermometers. The micro lens camera 306 scans the user's QR-Code and inputs the data to the main control unit. The image of the QR-code can be displayed on a user's

cellular phone (via SMS, MMS, web browser or email) or physically printed out by the user on a piece of paper so that the micro lens camera 306 can scan the image. The panic button 314 can be pressed by the user to alert hospital / building staff and/or immigration officers in the event that the user requires immediate assistance. The speaker/microphone unit 316 facilitates intercommunication while advantageously minimizes contact between the user at the kiosk 300 and hospital / building staff and/or immigration officers.

An additional layer of security is advantageously established with the use of the 1D barcode scanner 307. The 1D barcode scanner 307 can be used to scan 1D barcodes on, for example, a user's identity card or passport and inputs the secondary identity information to the main control unit. This two-factor authentication discourages a person from using someone else's QR-code to gain access. If a user's identity card or passport does not correspond to his QR-code, access can be denied. It will be appreciated by a person skilled in the art that the micro lens camera 306 may also be used to scan the 1-D barcode.

The additional layer of security can alternatively or additionally be established with the use of non-contact identification means such as an iris scanner (not shown), palm vein scanner (not shown) or radio-frequency identification (RFID) scanner (not shown), in different embodiments.

If it has been determined that the user's identity corresponds to the QR-code, the score embedded in the QR-code indicates that he is a high-risk person and the user's current body temperature is below the pre-determined threshold, the printer 310 can print out a visitor's pass to allow the user access to the location. The entire process of scanning, authentication and issuance of the visitor's pass may be advantageously completed in less than 10 seconds.

The main control unit (not shown) is connected to, among other things, the micro lens camera 306 and the 1D barcode scanner 307. The images obtained by the micro lens camera 306 and the 1D barcode scanner 307 are sent to the main control unit for processing. The processor (not shown) at the main control unit can extract primary identity information and the health risk score from the QR-code. The main control unit advantageously comprises an interface for connection to the server 102.

A face recognition system can be implemented using the surveillance camera 302. Images of the user's face can be captured by the surveillance camera and selected facial features are compared to stored facial images in a local database in order to determine the user's identity. This provides another layer of security to encourage the user to use his personal QR-code. It will be appreciated by a person skilled in the art that because of the substantial storage space required to store facial images, the face recognition system may be more suitable for local implementation in a location with a regular pool of visitors rather than for multiple locations comprising a large group of people. However, future advances in technology may enable face recognition to be implemented across a larger number of locations.

Application software is installed in the main control unit and can be used to interact with the server software 108 through the web service 109. The application software is preferably configured in an offline mode where data can be transmitted/received in a batch mode or only when the server polls for data from the main control unit. Data that is communicated between the main control unit and the server 102 includes QR-Code validity and reporting of the user's location. In this instance, the data is communicated asynchronously in that if the server is under maintenance or inoperable, data can be stored locally and subsequently sent when the server 102 is online. The offline mode also advantageously reduces the bandwidth required when compared to the online mode as data is not exchanged continuously. Moreover, the two-factor authentication, as described above, can be implemented in the offline mode. A user's identity card or passport can be compared to his identity embedded in the QR-code without a need for a continuous connection to the server.

Alternatively, the application software can be configured to be continuously online and connected to the server 102. In this configuration, data is continuously transmitted and received to/from the server 102.

The offline mode of operation may be preferred over the online mode so as to avoid e.g. problems associated with break-down of online connectivity, and speed limitations due to bandwidth constraints. A 2-D barcode is used in a preferred embodiment for storing at least the primary identity information and the health risk score such that the primary identity information and the health risk score can be extracted from the 2-D barcode without the need to interrogate an additional database, thus advantageously enabling offline operation.

Compared to a 1-D barcode, a 2-D barcode may further be preferred because it can be captured and displayed by a number of mobile devices comprising a digital camera and can be read/scanned using existing image processing technology. On the other hand, a 1-D barcode can not typically be captured and displayed on such mobile devices in a manner suitable for scanning by conventional 1-D barcode scanners.

Figure 4 is a flow chart, generally referred to as reference numeral 400, illustrating the steps a user takes to obtain a visitor's pass in order to gain access into a building, according to an embodiment of the present invention. At step 402, the user approaches the kiosk 300 and is captured by a surveillance camera for security and subsequent contact tracing purposes, if necessary. At step 404, the user can scan his QR-code at the micro lens camera 308. If the health score embedded in his QR-code indicates that the user is infected, or the QR-code is unable to be read or is invalid, access is denied, and a message is displayed on a monitor at the kiosk for the user to approach building staff for assistance, at step 406. The user can communicate with building staff via the speaker/microphone unit 316. At step 408, the user's "high-risk" status, indicated by his health score, can be updated in the server so as to prevent the user from making subsequent entries into any other building equipped with a kiosk. At step 410, if the score embedded in the QR-code indicates that the user is not infected, he can scan his 1D barcode (e.g.: on his identity card) at the barcode scanner 307 for a second level of authentication. At step 412, if it is determined that the QR-code and the 1D barcode do not correspond or if the user does not have a suitable 1D barcode (e.g.: a foreigner without an identity card), access is denied and a message is displayed on a monitor at the kiosk for the user to approach building staff for assistance for physical verification of the user's identity. Instead of 1D barcode scanning, face recognition, iris scanning, palm vein scanning or RFID scanning may be carried out for the second level of authentication, in different embodiments, either alternatively or additionally. At step 414, if it is verified through the scanning of the QR-code and the 1D barcode that the user is using his own QR-code, the user's body temperature is measured by an infrared thermometer. At step 416, if the user's temperature is above a pre-determined threshold, access is denied, an alarm may be triggered and a siren and warning light activated to notify building staff. The user's "high-risk" status, indicated by his abnormal temperature reading, can be updated in the server so as to prevent the user from making subsequent entries into any other building equipped with a kiosk, as shown at step 408. At step 418, if it is verified through the scanning of the QR-code and the 1D barcode that the user is using his

own QR-code, the score embedded in the QR-code indicates that he is not infected and the user's body temperature is below the pre-determined threshold, a visitor's pass is printed out. The user can now enter the building with the visitor's pass.

5 Whenever a user is issued a visitor's pass, it can be assumed that he has entered the building and this information is sent to the server 102. The server software 108 establishes a list of visitors for every building that is equipped with a kiosk. The list of visitors facilitates the contact tracing of persons who have come into contact with a known infected user. When a user has been determined to be infected, 10 for example, when positively diagnosed by a doctor, the server 102 is updated. In this instance, the infected user's past whereabouts can be compiled and other users who have possibly come into contact (e.g.: gained access to the same location as the infected user) with the infected user can be traced. An alert list of all the possible users that may have come into contact with the infected person is generated. SMSes 15 can be advantageously sent to all users on the alert list to inform them to undergo tests to determine if they have been infected.

 In addition, the alert list of all possible infected users can be sent to all the kiosks in the system. In the event that a user on the list attempts to enter a location, 20 the user is denied entry. In this manner, if the user has not yet undergone tests, health officials may track down his location and request building staff to physically inform him to undergo tests.

 Figure 5 is a flow chart, generally referred to as reference numeral 500, 25 illustrating the steps of a method of access control, according to an embodiment of the present invention. At step 502, an encoded label is read using a label reader. At step 504, primary identity information and a health risk score are extracted from the read encoded label by means of a processor. Access is granted based on the extracted health risk score.

30

 Embodiments of the present invention provide a system for health declaration and access control, which allows users to complete an internet website based health declaration form in order to attain a QR-code, subsequently using the QR-code to access locations that comprise a non-contact, self-service kiosk. The kiosk only 35 permits entry to non-high risk users (based on the health declaration) and those without temperature symptoms in order to limit the spread of the infectious diseases and facilitates contact tracing in the event that a visitor who has initially gained

access is subsequently infected. The system advantageously does not require additional manpower to process the visitors; does not raise the probability of infection as close contact between possibly infected persons, hospital and building staff is minimized; and substantially reduces the time visitors have to spend queuing up to gain access to the location.

It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the embodiments without departing from a spirit or scope of the invention as broadly described. The embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. An apparatus for access control, the apparatus comprising:
a label reader for reading an encoded label; and
5 a processor for extracting primary identity information and a health risk score
from a read encoded label;
wherein access is granted based on the extracted health risk score.
2. The apparatus as claimed in claim 1, wherein the encoded label comprises a
10 2-D barcode.
3. The apparatus as claimed in any one of claims 1 or 2, further comprising:
a biometric reader for reading biometric data of a person;
means for determining symptoms of a communicable disease from the
15 biometric data,
means for associating the read biometric data, the determined symptoms, or
both, with said person based on the identity information extracted from the read 2-D
bar code; and
wherein access is further granted based on the determined symptoms.
20
4. The apparatus as claimed in claim 3, wherein the biometric reader comprises
a non-contact biometric reader.
5. The apparatus as claimed in claim 4, wherein the non-contact biometric
25 reader comprises a temperature sensing device.
6. The apparatus as claimed in claim 5, wherein the temperature sensing device
comprises an infrared thermometer.
- 30 7. The apparatus as claimed in any one of the preceding claims; further
comprising means for reading secondary identification information presented by the
user, and wherein access is further granted based on a comparison of the first and
second identification information.
- 35 8. The apparatus as claimed in claim 7, wherein the means for reading the
secondary identification information comprises one or more of a group consisting of a

1-D barcode reader, the 2-D barcode reader, an iris scanner, a palm vein scanner and a radio-frequency identification scanner.

5 9. The apparatus as claimed in any one of the preceding claims, further comprising an interface for connection to a remote server.

10. A method of access control, the method comprising the steps of:
reading an encoded label using a label reader; and
10 extracting primary identity information and a health risk score from the read encoded label by means of a processor;
wherein access is granted based on the extracted health risk score.

11. The method as claimed in claim 10, wherein the encoded label is a 2-D
15 barcode.

12. The method as claimed in any one of claims 10 or 11, further comprising the steps of:
reading biometric data of a person using a biometric reader;
20 determining symptoms of a communicable disease from the biometric data;
associating the read biometric data, the determined symptoms, or both, with said person based on the identity information extracted from the read 2-D barcode;
and
wherein access is further granted based on the determined symptoms.

25 13. The method as claimed in claim 12, wherein the biometric reader comprises a non-contact biometric reader.

14. The method as claimed in claim 13, wherein the non-contact biometric reader
30 comprises a temperature sensing device.

15. The method as claimed in claim 14, wherein the temperature sensing device comprises an infrared thermometer.

35 16. The method as claimed in any one of claims 10 to 15, further comprising the steps of reading secondary identification information presented by the user, and

wherein access is further granted based on a comparison of the first and second identification information.

17. The method as claimed in claim 16, wherein the secondary identification information is read using one or more of a group consisting a 1-D barcode reader, a 2-D barcode reader, an iris scanner, a palm vein scanner and a radio-frequency identification scanner.

18. The method as claimed in any one of the preceding claims, further comprising the step of connecting to a remote server by means of an interface.

19. A method of contact tracing using the apparatus as claimed in any one of claims 1 to 9.

20. The method as claimed in claim 19, comprising the steps of:
obtaining a person's health declaration via a server;
calculating the health risk score based on the health declaration; and
issuing of the 2-D barcode comprising the primary identity information and the health risk score.

21. The method as claimed in claim 20, wherein the primary identity information of persons granted access is stored in a database of the apparatus for the contact tracing.

22. A method of tracking a person using the apparatus as claimed in any one of claims 1 to 9.

23. The method as claimed in claim 22, comprising the steps of:
obtaining a person's health declaration via a server;
calculating the health risk score based on the health declaration; and
issuing of the 2-D barcode comprising the primary identity information and the health risk score.

24. The method as claimed in any one of claims 22 or 23, wherein the primary identity information of persons having used the apparatus is stored in a database of the apparatus for the tracking.

25. A system for access control, the system comprising:
the apparatus as claimed in any one of claims 1 to 9; and
a remote server coupled.

5 26. The system as claimed in claim 25, wherein the server is configured for
obtaining a person's health declaration, for calculating the health risk score based on
the health declaration; and for issuing of the 2-D barcode comprising the primary
identity information and the health risk score.