

**Method and Apparatus for biometric authentication with active RFID
in an education or training environment**

TECHNICAL FIELD OF THE INVENTION

5

This invention relates to a method for authenticating a person as having been authorised to be present at or to use a particular facility. The authentication process uses radio frequency identification (RFID) chips provided on conveniently portable authentication devices which authenticates
10 by matching biometric data of a user with a pre-recorded biometric data as reference. Apparatus and system employing such process are also described.

BACKGROUND OF THE INVENTION

15

Prior to commencing teaching in a typical classroom, lecture hall, tutorial or laboratory, the teacher, lecturer or tutor would have to spend a good 5 to 15 minutes to check on the attendance of his students depending on the size of the class. This may be calling out the individual students' names and would
20 require the teacher to commit to memory his students' names to match their faces.

To avoid such hassle, teachers often let an attendance sheet to be passed around the students so that each student may sign thereon against

their name listed in the sheet. Such practice is open to abuse as a present student (or non-authorised person) may sign for an absent one, particularly where attendances count towards performance evaluation of the students.

5 Sometimes, additional particulars such as their matriculation or student number has to be written thereon in addition to their signature but this additional step did little to prevent such abuses, particularly by resolute abusers who may easily memorise such numbers for the absent students. Often, the student may personally mark his own attendance but leave without attending
10 the lecture in a lecture hall or facility that is too large to monitor.

Hence, some schools provide matriculation or student cards, which may contain the student's identification particulars in a magnetic strip, bar code or even smart chip thereon, to the students and require them to slide the card
15 through a reader device to authenticate and record their attendance or for other purposes such as borrowing books from a library. This is still time-consuming especially where a large lecture group of students need to be processed quickly and often a long single file of students is formed as they await their turn to slide or scan their card through a reader one at a time and await for
20 verification as each reading is authenticated at the reader device.

This practice is not able to verify if the person holding the card is the same person, to whom the card is issued to, and does not prevent an impostor from taking possession of the card and proceed to the reader device to have

his attendance taken or recorded. With such system, it is still possible for students to hold their fellow students' card to sign-in on their behalf as there is no means for authenticating that the card holder is the student to whom the card is issued to. Hence, students may still play truant.

5

In a large, sprawling campus, there is also the problem of strangers entering the school premises without being recognised or detected as there is a lack of authentication processes being carried. Even if there are such processes, the stranger may simply meander away from such checkpoints
10 without being discovered.

In US-6,751,734 (NEC Corp.) there is disclosed the use of biometrics, including fingerprints, for authentication purposes with a portable radio frequency identification (RFID) card having biometrics input means, including
15 fingerprint identifying means. There is also provided an encryption method using a secret key to protect the authentication message transmission. While radio frequency is the medium of communication, this prior art appears to employ discrete components such as processor, transmission unit and memory or storage units rather than a integrated circuit such as a radio frequency
20 identification (RFID) chip. There is also no suggestion of deploying it in an education or training environment.

US-2003/0226041 (Innovative Connections) discloses a dual active/passive RFID technology which may be deployed in electronic banking

transactions, point-of-sale (POS) transactions, check-ins by patients into hospitals, or by travelers into airline, etc. There is no suggestion of its use in an educational or training institution for marking attendance of students, for example. This prior art device further requires it to be placed with an RF field in
5 order to be activated.

In US-6,819,219 (IBM Corporation) there is also disclosed a smart card which does not store biometric data on the server system. The biometric data is stored on the card itself so that the biometric authentication process is
10 completed at the card before an authenticated signal is sent via wireless means to a reader terminal. There is no specific mention of radio frequency identification (RFID) chip or whether it could be deployed in an educational or training environment. One limitation of this prior art is that the smart card has to be interrogated by a reader before it can initiate a signal transmission. If
15 multiple smart cards are within the vicinity of the reader's interrogating broadcast, then each of these smart cards may compete to transmit their respective signals resulting in a clash of signals to be received by the reader.

US-6,700,491 (Sensormatic Electronics) further discloses a label or tag
20 (i.e. smaller than a portable credit card size) using active RFID technology wherein the electrodes of its thin film battery are adapted to function as dipole antenna as well. This patent discloses its use for labelling or tagging purposes and there is no disclosure on biometric authentication means or deployment in an educational or training environment.

The main difference between active RFID and passive RFID chips is their power supply. An active RFID device uses a battery within the device. A passive RFID depends on RF energy transferred from a reader to power the tag. Although active RFID is more expensive, as a result, than passive RFID, it is a technology that allows RFID devices to be continuously powered, and to generate high-level signals back to the reader, even with only low-level signals generated from the device. Generally, passive RFID can only transmit over a range of not more than 300 feet.

These distinctions translate into differences in communications range, the ability to collect information from multiple devices, functionality and interference in metallic and wet environments, and opportunities to integrate with other sensor technologies. Active ID cards performed much better in a number of situations, e.g. when the employee passed through the center of a wide doorway or entrance and may not go near a reader; when the card is held against the body; and when multiple RFID tags needed to be read simultaneously, for example.

An active RFID device also has the advantage of transmitting stronger signals above ambient electromagnetic noise and other interference levels and may be able to facilitate broad band or spectrum for communication with room for added security measures such as encryption, etc. With on-board power supply of its own, an active RFID device is able to support more memory and to contain more data compares to a passive device.

Due to the need to incorporate battery source into the device, if an active RFID tag or card is able to be integrated into a credit card size or ID badges that may be carried in a variety of configurations: in a wallet, in a computer bag, and hanging as a pendant from a necklace or key chain for instance.

5

An active RFID technology is also able to power other circuitry apart from RFID chip on-board for additional functionality such as sensing, location sensing and display. For example, one potential application of active RFID is providing indoor positioning system (IPS) which is analogous to the global positioning system (GPS) for outdoor use using a network of orbiting satellites. In place of the satellites, a centrally-linked network of RFID readers, which positions are predetermined, may be provided to locate people, mobile equipment, vehicles or devices within a building complex or campus.

Any discussion of documents, devices, acts or knowledge in this specification is included to explain the context of the invention. It should not be taken as an admission that any of the material forms a part of the prior art base or the common general knowledge in the relevant art in Singapore or elsewhere on or before the priority date of the disclosure and claims herein. All statements as to the date or representation as to the contents of these documents is based on the information available to the applicant and does not constitute any admission as to the correctness of the dates or contents of these documents.

SUMMARY OF THE INVENTION

Accordingly, one aspect of our invention is to provide for a method of authenticating a person's identify in an educational or training environment by using one or more of his biometric features. Another aspect of the invention is to use active RFID technology so that wireless transmission of signals may be processed at a larger distance to avoid queues from forming when many persons are required to be authenticated within a short time such as attendance in a classroom in an educational or training environment.

Further aspects of the invention includes enabling a person supervising the authentication process, such as a lecturer or tutor, to quickly collate and compile records of the authentication process for attendance reporting and referring to background records of each student or authenticated persons. To this end, data processing means is provided with suitable interfacing to enable the lecturer to record attendances, assignment, test marks, etc. Yet a further application of our invention, when the RFID readers are mapped and centrally linked, is to provide for an indoor positioning system.

In the general aspect of the present invention, a method is provided for authenticating a person's identity in an educational or training environment. The method comprises sensing a first biometric feature of an authentication-seeking person on a portable identification device; converting said first biometric feature into a first input biometric data on said portable identification

device; comparing said first input biometric data against a reference data including a first stored biometric data of an authorised person pre-recorded on said portable identification device; upon matching said first input biometric data with said first stored biometric data, generates an authenticated signal unique
5 to said authorised person via radio frequency from said portable identification device; receiving said radio frequency authenticated signal by a signal reader linked to a database containing records of authorised persons; identifying said authorised person's authenticated signal with said authorised person's record on said database; and collating said authorised person's record with other
10 authorised person's records in said database for data processing.

In a preferred embodiment of this aspect of our invention, the biometric feature includes a finger-print as the first stored biometric data, which may preferably be stored in a non-volatile memory means, including a flash
15 memory. Preferably, a second stored biometric data of said authorised person is further pre-recorded on said portable identification device and a second input biometric data is correspondingly sensed, converted, compared and matched in place of said first input biometric data, upon which an authenticated signal unique to said authorised person is generated via radio frequency from said
20 portable identification device.

In another preferred embodiment, the signal reader is identifiable with its location within said educational or training environment. In yet another preferred embodiment, a person supervising the location is able to compile and

process the collated records for any one or more purposes including attendance, indoor positioning and locating, verification including visual validation, authorising and like administrative and/or security functions.

5 As a specific embodiment, the supervising person is a lecturer supervising his classroom as the identifiable location, and who is able to compile a list of students as authorised persons; and wherein the administrative and/or security functions includes, indoor positioning system, verifying visually the attending students, assigning attendance credits, and allowing temporary
10 access permission to assigned equipment, rooms, and like facilities within said classroom. Preferably, the facilities are equipped with secondary signal readers which may read unique authenticated person signals assigned to the specific signal reader by said lecturer.

15 In a second aspect of the invention, it is provided a portable identification device for identifying an authorised person in an educational or training environment wherein the device comprising a biometric sensor; a radio-frequency identification (RFID) chip comprising a stored first biometric reference data; and a battery power source for powering said RFID chip;
20 wherein biometric data acquired by said biometric sensor is sent to the RFID chip to be compared with said first biometric reference data stored therein, and upon matching said acquired biometric data with said stored biometric reference data, said RFID chip transmits a unique radio frequency authentication signal.

Preferably the biometric sensor is a fingerprint sensor, including a suitable optical method or capacitance method. Preferably still, the RFID chip is a hybrid active-passive RFID chip which will be powered by the greater of
5 incident radio frequency (RF) energy incident on said RFID chip or the power supplied by the battery. The device is preferably the size of a credit card. A second biometric reference data is preferably stored in addition to the first reference data.

10 In one preferred embodiment, the device is used with a radio frequency signal reader which is identified with a location within the educational or training environment. Preferably, the device is used with a signal reader which is linked to a server comprising a database of authorised persons' records identifiable by their respective unique radio frequency authentication signals. The portable
15 identification device preferably includes means for detecting radio frequency of a range emitted by other portable identification devices issued by the same authority and which means delays the transmission of authenticated signal upon such detection.

20 In a third aspect of the invention, there is provided a radio frequency identification (RFID) authentication system for an educational or training environment comprising a portable identification device, a radio frequency signal reader and a central server wherein the portable identification device has biometric authentication means which, upon authentication, transmit a

authentication signal unique to an authorised person assigned to said portable identification device; the radio frequency signal reader is capable of receiving said unique authentication signal and is linked to enable transmission of such signal to a central server; and wherein the central server comprises a database
5 of authorised persons' records identifiable by their respective unique radio frequency authentication signals.

Preferably, the signal reader may be identified by its location within the educational or training environment; and the central server further comprises a
10 data processing means for collating authorised persons' records for supervisory control purposes.

In one preferred embodiment of the RFID authentication system, the data processing means includes further compiling and processing of said
15 collated records for any one or more purposes including attendance, indoor positioning and locating, verification including visual validation, authorising and like administrative and/or security functions.

In another preferred embodiment, a person having supervisory control
20 over said data processing means may be a lecturer supervising his classroom as the identifiable location, and who is able to compile a list of students as authorised persons. Preferably, the administrative and/or security functions includes, indoor positioning system, verifying visually the attending students, assigning attendance credits, and allowing temporary access permission to

assigned equipment, rooms, and like facilities within said classroom. Preferably still, the facilities are equipped with specific signal readers which may read unique authenticated person signals assigned to said specific signal readers by said lecturer.

5

Other aspects and preferred aspects are disclosed in the specification and / or defined in the appended claims, forming a part of the description of the invention.

10

Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

15

BRIEF DESCRIPTION OF THE DRAWINGS

20

The present invention will be better understood with the following detailed description with reference to the accompanying drawings which describe specific embodiments as non-limiting examples or illustration, in which:

FIGURE 1 shows a wireless authentication device with its unit subsystem layout in the form of a credit card according to a general embodiment of our present invention;

5

FIGURE 2 shows a functional block diagram of the device in FIG. 1;

FIGURE 3 shows a flowchart of the authentication process according one embodiment of our invention;

10

FIGURE 4 shows a flowchart of software for displaying an application interface according to another embodiment of our invention;

FIGURE 5 shows a flowchart of software for displaying an application for attendance marking of one situation;

15

FIGURE 6 shows a flowchart of software for displaying an application for attendance marking of a second situation;

FIGURE 7 shows a flowchart of software for displaying an application for attendance marking of a third situation; and

20

FIGURE 8 shows a flowchart of software for maintaining peripheral security of a school.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

5 The following preferred embodiments to be described in detail are intended for the purpose of keeping track of persons or personnel, including but limited to students, trainees, conference attendees, etc. for ease of monitoring individual movement within a specific defined area such as a building complex or campus. The invention will illustrate its function as a first line of defence in
10 detecting the presence of unauthorised persons in the area and restrict them from entering. Simply unmanned checkpoints such as auto-open sliding door, electromagnetically-locked doors or turnstiles may be deployed to stop such unauthorised persons from entering the area or building.

15 The wireless authentication device in the form of a credit card size device will now be described with reference to FIGURE 1 wherein is shown 4 main functional components accommodated within the device housing (10). The 4 main functional components are a biometric sensor (12), a power supply subsystem (14), a microcontroller (16) and an active RFID subsystem (18). It
20 should be noted that these functional components may be physically integrated into a single RFID integrated circuit (IC) device or microchip except for the power source (14) so that it may be replaceable. For example, a RFID chip incorporating an EEPROM would have sufficient storage for holding two biometric data.

In FIGURE 2, the four components are shown as separate functional blocks for ease of describing the functions thereof. Generally, the wireless authentication device, which is in the form of a portable identification device, comprises a biometric sensor (12), a RFID chip (18) and a battery power source (14) for providing direct current power supply for the operation of the device, including the biometric sensor and RFID subsystem (18) or chip. Accordingly, in this specification, the terms “RFID subsystem” and “RFID chip” may be employed interchangeably. The biometric sensor (12) may be a suitable sensor for reading the particular biometric characteristics which may be facial features, iris colour or pattern, retina pattern, palm or finger prints, etc.

For the present exemplary embodiment, only finger printing as the biometric feature will be described herein although it is possible to provide for suitable sensors for other biometric feature. For example, an iris scanning sensor may require soft laser or infra-red scanning light source in addition to an image capture device on board the device which may require higher DC power consumption. For finger print sensing the two main sensing methods are the optical method in which an image capture device such as a charge coupled device (CCD) may be used using backlit with LED or using ambience light to record the finger print. Alternatively, a capacitance sensor may be used for measuring the differences in capacitance of the finger print pattern in contact with the capacitance sensor surface (such as that proposed in Inglis, *et al.* “A robust 1.8V, 250μW direct contact 500 dpi fingerprint sensor” paper in *IEEE*

/SSCC98, SA17.7, p. 284-285, 1998).

The authorized person, such as a registered student of the educational institution, may have his finger print captured by a special registration machine and stored permanently on the portable identification device (10) as first biometric reference data. This may include providing the circuit board of the device openly accessible with the device housing opened to enable the registration machine write to a non-volatile, write-once- read-only-memory (ROM) module of the device, which may be associated with either the RFID chip or biometric sensor. The housing halves may then be irreversibly snapped in place with the circuit board inside or permanently sealed by ultrasound or microwaves leaving no part of the circuit board accessible externally for hacking, and any attempt to open the housing will damage the device irreparably.

15

Alternatively, an authorised person, to whom the portable identification card is issued to, may be required to register his biometric feature, i.e. having a specific finger print taken with a special machine in full control by the particular authority (e.g. a university administrator's office) that may write to the card by wireless signal contact (e.g. where the card may be slotted into the machine to be written) or by special wireless or radio frequency encrypted signal. This biometric data may then be stored on the card (10) as a first biometric reference data so that a person seeking to authenticate himself will need to have his finger print scanned and compared against this first biometric

20

reference data. The comparison may be made by comparing binary data converted from the biometric data acquired and stored from the optical or capacitance methods of sensing fingerprint patterns.

5 As a “double-blind” measure, no specific digit or finger is designated to be used and only the authorised person would remember which of his ten digits has been registered as the finger print’s first biometric reference data. In the event that the first digit is not able to be scan (e.g. covered with healing tape due to injury) a second biometric reference data may be similarly registered on
10 the portable identification card so that, for instance, another hand’s finger print may be used.

With regard to the battery power, a power management subsystem may be provided integrally with the device in the form of a simple resistor or
15 transistor, or with the RFID itself so that on board power may be automatically switched on or off depending on the available incident RF energy from the RFID reader.

Depending on the design and configuration of the device, other discrete
20 components may be provided if no suitable RFID chip having all the desirable features according to the present invention may be sourced. For example, a microcontroller (16) for activating the RFID chip, particular the transmission of the authenticated signal to a reader, may be provided.

As shown in the form of a process flowchart in FIGURE 3, the authentication process (32) starts with the person seeking authentication having his finger print scanned (34) on the biometric sensor. The finger print image captured may be converted into an input biometric data and compared
5 against the reference data which has been pre-recorded on the portable identification device or card. Upon matching (36) the input data with the reference data, the active RFID is activated (37) to transmit a confirmation or authenticated signal (38) to an authentication terminal or reader to be accepted. If it does not match then authentication process is aborted or ends
10 prematurely (39).

Upon successful authentication, many different functions and applications may be had with further data processing. By “data processing” we mean any software algorithm or process flow that includes automated collating and recording of the authenticated persons for further use such as automatic
15 attendance marking, recording keeping and updating (e.g. assigning or lending laboratory equipment and library books, checking a particular student’s schedule of core and elective classes, credit hours earned to date, assignments due, etc. some of which we shall explain further in the following.

20 If the signal receiving terminal or RFID signal readers are identifiable with its location within the educational institution and centrally linked to a server, the specific location of the card holder may be pinpointed which an area geometry algorithm when 3 or more readers are able to pick up signals from the card, particularly if the card is configured to transmit a unique code in a

constant ping without being authenticated or when it is not used by the card holder for authentication purposes. This is possible with the use of active RFID which distance of signal transmission is much longer and without the need for a reader to send interrogating signal to it. This feature may therefore be used to
5 provide for an indoor positioning system (IPS) analogous to the manner the global positioning system (GPS) works. To address privacy concerns, an external switch may be provided to enable the card holder to switch off the constant pinging signal if such privacy is deemed important.

10 A person supervising a particular location installed with a RFID signal reader, such as a tutor supervising a laboratory, may be enabled via a computer terminal at the laboratory linked to a central server to compile and process the records of the authenticated persons collated from a database maintained at the central server. The compiled and processed records may be
15 carried out for attendance recording, verification, including visual validation, authorisation from the supervisor (e.g. for the use of specific laboratory equipments, use of special laboratory rooms or workstations) and other administrative and/or security functions.

20 An extended feature of such records compilation and processing software is to enable the supervisor to have secondary RFID signal readers attached to the equipment, room or computers under his control so that each of the facility will only work for a specific student so assigned thereto by the supervising lecturer.

Accordingly, from the above examples of applications and functions that our invention is capable of being adapted for, it is apparent that the 3 main components of our system, i.e. the RFID biometric authentication card, RFID authenticated signal reader and the software (incorporating the database of authorised persons and software for processing the data gleaned from the database) are flexible enough to spawn various other applications. The algorithms of specific applications will now be described in some detail.

FIGURE 4 shows a basic attendance application wherein a software interface (40) is provided to enable a supervisor, such as a lecturer, to compile an attendance list whereby a list of absentees (42) are separately compiled and displayed together with their photographs and possible reasons (e.g. whether an application or notice of absence have been made earlier, possible conflict with another class, sick or hospitalisation leave, holidays or festivals, etc.) and whether any of the possible reasons may be validated. For more urgent or important cases of absenteeism, a further step may be provided to display the personal information (44) of the student, such as his parents, guardian or next-of-kin, etc. Another further option is to provide an option to the lecturer to view the absentee's attendance records (46) for the past few days or weeks to see if a particular attendance pattern may be recognised.

Apart from the above example, software applications may also be written to provide for attendance recording of other education or training situations

such a seminar or conference, National Service or reservist call-up, industrial training for a group of production workers in a factory, etc.

As shown in FIGURE 5, a suggested flowchart of a software application for attendance-taking of a seminar or conference may commence with a database having been built from the participants' registration process before hand. A participant who arrives at the venue of the seminar or conference (50) will place their finger on the biometric sensor to have their finger print scanned and authenticated (52). Upon successful authentication (54), the participant's record will be updated accordingly (56) and included in the list of attendees. A separate list of participants who failed the authentication process or simply fail to turn up for the authentication process is compiled (53). A supervisor, i.e. a member of the seminar or conference organizer, may then link (55) each absentee to their records contained in the database to display (57) their photographs, contact particulars, including next-of-kin or companies sponsoring their attendance to alert them of the absence. At the end of the seminar or conference, the database is able to generate statistics on the attendance (58) for review, management evaluation and records purpose.

FIGURE 6 shows a suggested flowchart of a software application for attendance-taking of a National Service reservist training or a military unit's duty call-up (60) wherein the RFID authentication system according to the present invention may be employed. The reservists may authenticate themselves by having their finger print scanned on their respective active RFID

cards (62) as they assemble in a hall or briefing room. Upon successful authentication (64), their attendance will be recorded in the database (66). On the other hand, those absent or failed to be authenticated (65) will be compiled into a separate list. The commander of the unit may be able to access the list

5 of the absentees from a computer and the application may compile the list together with the absentees' photos displayed on the computer screen (67) with the reason of absence, if any. Each photo or record may contain a link that will show the full contact particulars for the absentee, such as the address, contact number, next-of-kin's name, address and contact number (69). At the end of

10 the briefing, the database system is able to generate a statistics of attendance for viewing and logging purposes (68).

FIGURE 7 shows a suggested flowchart of a software application for marking attendance of a group of production workers selected for a particular

15 industrial training class. The workers may have their usual security cards provided in the form of the RFID authentication card according to the present invention as their usual attendance-taking means upon arrival at the factory (70) to commence their daily work. A manager may select a group of workers for a particular industrial training and may program a RFID reader at the

20 training room to admit this group of workers and to record their attendance (72) upon their arrival at the training room and upon successful authentication process (74). The database system will then update the status of attendance (76) of each production worker and compile a list of absentees (75). A supervisor or trainer will be able to access the list of absentees from a

computer. Upon clicking the name of the absentee in the list, the database system will provide the attendees' photo and reason of absence if any (77).

If there are no reasons of absence shown, the supervisor is able to
5 obtain the absentee's particulars (79) by clicking on his or her photo display on the monitor. The absentee's particulars will contain his or her home address, contact number, next-of-kin's name, contact number and address. At the end of the day, the database system is able to generate a statistics attendance report (78) for viewing and logging purposes.

10

As another application of our invention, the apparatus for biometric authentication with active RFID may be deployed to monitor and protect an educational institution's perimeter such as to deter and monitor strangers entering the school premises. An exemplary logic flow of such an application is
15 shown in FIGURE 8.

A camera and laser sensor may be mounted at every gate of the school to serve as a second tier security to detect strangers entering school premises who may be differentiated from a student entering the school premise because
20 a student would have to authenticate himself/ herself using the biometric authentication apparatus with active RFID.

A successful authentication may be based on two checks, one from the biometric authentication and the other on the laser sensor in sensing a person

entering into school premises. At any one time should the authentication is unsuccessful, security guards at the guardhouse will be alerted and they would be able to monitor the situation from the security camera mounted at the respective gates.

5

The process flow of the authentication is still the same as the afore-described applications, with the addition of another laser sensor as an additional security check.

10

While this invention has been described in connection with specific embodiments thereof, it will be understood that it is capable of further modification(s). This application is intended to cover any variations uses or adaptations of the invention following in general, the principles of the invention and including such departures from the present disclosure as come within known or customary practice within the art to which the invention pertains and as may be applied to the essential features hereinbefore set forth.

15

As the present invention may be embodied in several forms without departing from the spirit of the essential characteristics of the invention, it should be understood that the above described embodiments are not to limit the present invention unless otherwise specified, but rather should be construed broadly within the spirit and scope of the invention as defined in the appended claims. Various modifications and equivalent arrangements are

20

intended to be included within the spirit and scope of the invention and appended claims. Therefore, the specific embodiments are to be understood to be illustrative of the many ways in which the principles of the present invention may be practiced. In the following claims, means-plus-function clauses are
5 intended to cover structures as performing the defined function and not only structural equivalents, but also equivalent structures. For example, although a nail and a screw may not be structural equivalents in that a nail employs a cylindrical surface to secure wooden parts together, whereas a screw employs a helical surface to secure wooden parts together, in the environment of
10 fastening wooden parts, a nail and a screw are equivalent structures.

“Comprises/comprising” when used in this specification is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features,
15 integers, steps, components or groups thereof.”

CLAIMS

- 1 A method of authenticating a person's identity in an educational or training environment comprising
 - 5 (i) sensing a first biometric feature of an authentication-seeking person on a portable identification device;
 - (ii) converting said first biometric feature into a first input biometric data on said portable identification device;
 - (iii) comparing said first input biometric data against a reference data including a
 - 10 first stored biometric data of an authorised person pre-recorded on said portable identification device;
 - (iv) upon matching said first input biometric data with said first stored biometric data, generates an authenticated signal unique to said authorised person via radio frequency from said portable identification
 - 15 device;
 - (v) receiving said radio frequency authenticated signal by a signal reader linked to a database containing records of authorised persons;
 - (vi) identifying said authorised person's authenticated signal with said authorised person's record on said database; and
 - 20 (vii) collating said authorised person's record with other authorised person's records in said database for data processing.

2. A method according to Claim 1 wherein the biometric feature includes a finger-print.

3. A method according to Claim 1 wherein the first stored biometric data is stored in a non-volatile memory means, including a flash memory.
- 5 4. A method according to Claim 1 wherein a second stored biometric data of said authorised person is further pre-recorded on said portable identification device and a second input biometric data is correspondingly sensed, converted, compared and matched - i.e. steps (i), (ii), (iii) and (iv) - in place of said first input biometric data, upon which an authenticated signal unique to
10 said authorised person is generated via radio frequency from said portable identification device.
5. A method according to Claim 1 wherein the signal reader is identifiable with its location within said educational or training environment.
- 15 6. A method according to Claim 5 wherein a person supervising the location is able to compile and process said collated records for any one or more purposes including attendance, indoor positioning and locating, verification including visual validation, authorising and like administrative and/or
20 security functions.
7. A method according to Claim 6 wherein:
- the person is a lecturer supervising his classroom as the identifiable location, and who is able to compile a list of students as authorised

persons; and wherein

- the administrative and/or security functions includes, indoor positioning system, verifying visually the attending students, assigning attendance credits, and allowing temporary access permission to assigned equipment, rooms, and like facilities within said classroom.

5

8. A method according to Claim 7 wherein the facilities are equipped with secondary signal readers which may read unique authenticated person signals assigned to the specific signal reader by said lecturer.

10

9. A portable identification device (10) for identifying an authorised person in an educational or training environment comprising:

- a biometric sensor (12);
- a radio-frequency identification (RFID) chip (18) comprising a stored first biometric reference data; and
- a battery power source (14) for powering said RFID chip;

15

wherein biometric data acquired by said biometric sensor (12) is sent to the RFID chip (18) to be compared with said first biometric reference data stored therein, and upon matching said acquired biometric data with said stored biometric reference data, said RFID chip transmits a unique radio frequency authentication signal.

20

10. A portable identification device according to Claim 9 wherein the biometric sensor is a fingerprint sensor, including a suitable optical method or

capacitance method.

11. A portable identification device according to Claim 9 wherein the RFID
chip is a hybrid active-passive RFID chip which will be powered by the greater
5 of incident radio frequency (RF) energy incident on said RFID chip or the power
supplied by the battery.

12. A portable identification device according to Claim 9 wherein the device
is about the size of a credit card.

10

13. A portable identification device according to Claim 9 wherein a second
biometric reference data is stored in addition to the first reference data.

14. A portable identification device according to Claim 9 in use with a radio
15 frequency signal reader which is identified with a location within the educational
or training environment.

15. A portable identification device in use with a signal reader according to
Claim 14 wherein the signal reader is linked to a server comprising a database
20 of authorised persons' records identifiable by their respective unique radio
frequency authentication signals.

16. A portable identification device according to Claim 9 including means for
detecting radio frequency of a range emitted by other portable identification

devices issued by the same authority and which means delays the transmission of authenticated signal upon such detection.

17. A radio frequency identification (RFID) authentication system for an educational or training environment comprising a portable identification device, a radio frequency signal reader and a central server wherein:

- said portable identification device has biometric authentication means which, upon authentication, transmit a authentication signal unique to an authorised person assigned to said portable identification device;
- 10 - said radio frequency signal reader is capable of receiving said unique authentication signal and is linked to enable transmission of such signal to a central server; and wherein
- said central server comprises a database of authorised persons' records identifiable by their respective unique radio frequency authentication signals.

18. An RFID authentication system according to Claim 17 wherein:
- the signal reader may be identified by its location within the educational or training environment;
 - 20 - the central server further comprises a data processing means for collating authorised persons' records for supervisory control purposes.

19. An RFID authentication system according to Claim 18 wherein the data processing means includes further compiling and processing of said collated

records for any one or more purposes including attendance, indoor positioning and locating, verification including visual validation, authorising and like administrative and/or security functions.

5 20. An RFID authentication system according to Claim 19 wherein:

- a person having supervisory control over said data processing means is a lecturer supervising his classroom as the identifiable location, and who is able to compile a list of students as authorised persons; and wherein
 - the administrative and/or security functions includes, indoor positioning
- 10 system, verifying visually the attending students, assigning attendance credits, and allowing temporary access permission to assigned equipment, rooms, and like facilities within said classroom.

21. An RFID authentication system according to Claim 20 wherein the

15 facilities are equipped with specific signal readers which may read unique authenticated person signals assigned to said specific signal readers by said lecturer.