

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
17 March 2005 (17.03.2005)

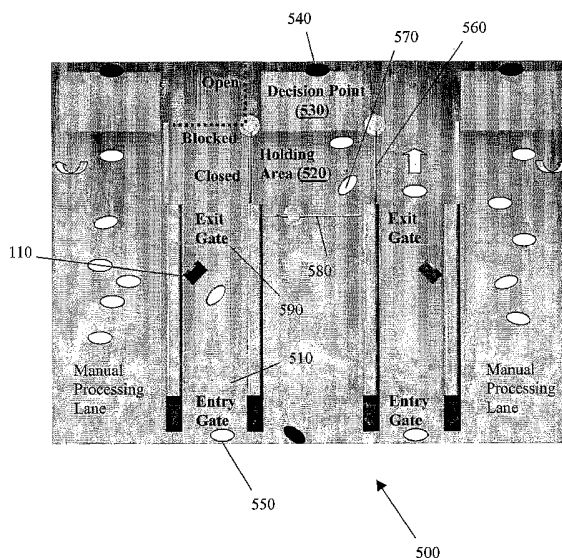
PCT

(10) International Publication Number
WO 2005/024733 A1

- (51) International Patent Classification⁷: **G07C 9/00**, E06B 11/00
- (21) International Application Number: PCT/AU2004/001208
- (22) International Filing Date: 8 September 2004 (08.09.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
2003904900 8 September 2003 (08.09.2003) AU
2003904902 8 September 2003 (08.09.2003) AU
2003904901 8 September 2003 (08.09.2003) AU
- (71) Applicant (for all designated States except US): **INTER-CARD WIRELESS LIMITED** [AU/AU]; Level 7, 130 Macquarie Street, Sydney, New South Wales 2000 (AU).
- (71) Applicant and
(72) Inventor: **REEVES, Peter** [AU/AU]; 21 Pollock Avenue, Wyong, New South Wales 2259 (AU).
- (74) Agents: **CARTER, Chris John** et al.; Davies Collison Cave, Level 10, 10 Barrack Street, Sydney, New South Wales 2000 (AU).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD PROVIDING GATED CONTROL AND PROCESSING OF PERSONS ENTERING OR EXITING SECURE AREAS OR CROSSING BORDERS



(57) Abstract: An access control method and/or system providing automated subject identification and verification processing of subjects attempting to pass through a secure line (such as passengers crossing an immigration primary line at an airport or land-crossing) using personal identification (such as a combination of tokens and biometric access control). A verification station, interlocking subject direction gates and sensors provide a high flow through rate of subjects. Augmented by subject exception processing controls that direct subjects to a holding area, which is operated by an authorised officer, for additional processing while allowing continued processing of subsequent subjects normally.



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

**SYSTEM AND METHOD PROVIDING GATED CONTROL AND PROCESSING
OF PERSONS ENTERING OR EXITING SECURE AREAS
OR CROSSING BORDERS**

5 Technical Field

The present invention relates to a system and/or method providing control and electronic processing of persons, for example, a security control system or method of processing, and in particular, to an improved border or secure area control system and/or method for directing, processing and/or controlling individuals, for example passengers.

10

Background Art

The control and processing of individuals, for example passengers or crew, at checkpoints, for example Immigration checkpoints in an airport, is an important consideration for security of a country, region or area. Checkpoints exist in many situations, for example,
15 railway stations, airport terminals, land crossings, ports, building entrances, secure areas, etc.

In many situations it is an important consideration to efficiently process individuals and avoid delays and crowd build-up. For example, tourism contributes significant revenue to many countries and tourists impressions and experiences at Immigration can be important
20 in terms of generating continuing tourism based revenue. Efficiency must be balanced against security considerations. Crowd management, general access control, room access control, etc. are also important areas requiring security controls.

25 The terms 'transaction point' and 'verification station' are used interchangeably herein to describe the regulatory equipment/processes used to identify, verify and assess a person's right to pass a checkpoint, for example to enter a country via a border crossing.

In a networked data communications system, users have access to terminals which are
30 capable of requesting and receiving information from local or remote information sources. In such a system a terminal may be a type of processing system, computer or computerised device, a personal computer (PC), a mobile data terminal, a portable computer, a thin

client, or any other similar type of electronic device. The capability of the terminal to request and/or receive information can be provided by an application program, hardware or other such entity. A terminal may be provided with associated devices, for example a storage device such as a hard disk drive or solid state drive.

5

An information source may be a server or any other type of terminal coupled to an information storage device. The exchange of information (i.e., the request and/or receipt of information) between the terminal and the information source, or other terminal(s), is facilitated by a connection referred to as a communication channel. The communication
10 channel can be physically realised via a metallic cable (for example, a telephone line), semi-conducting cable, electromagnetic signal, optical fibre cable, satellite link or any other such medium or combination thereof connected to a network infrastructure.

A computer network as referenced in this specification should be taken to include all
15 forms of connected or communicating computers or terminals having at least two terminals adapted to communicate with each other. That is, the term computer network should be taken to include any type of terminal, computer, computerised device, peripheral computer equipment, computerised accessory, mobile or cellular phone, digital electronic device or other similar type of computerised electronic device or part thereof
20 which is rendered such that it is capable of communicating with at least one of any of the aforementioned entities. The communication of information or data can occur over any computer network, data communications network, telecommunications network, wireless network, internetwork, intranetwork, LAN, WAN, the Internet and developments thereof, transient or temporary network, combinations of the above or any other type of network
25 providing for communication between computerised, electronic or digital devices.

The reference to any prior art in this specification is not, and should not be taken as, an acknowledgment or any form of suggestion that such prior art forms part of the common general knowledge.

30

Disclosure Of Invention

The present invention can be applied to a flow of people in many circumstances, where each person must be checked or processed to verify the person's authority to enter a certain area or cross a certain boundary. In one particular embodiment, the present

invention is applicable to passenger control at Immigration, however, the reader will appreciate that the present invention could be readily applied to other situations requiring the directing, processing and/or controlling of individuals, for example at the entrance or exit to a building, entertainment arena, secure area, ship or boat, transport terminal, school
5 or university, place of work, or many other such places.

Likewise, although reference is made to passengers, the reader will appreciate that this term should be read to encompass any other label that may be given to a person in a flow of persons, for example, workers, students, officers, members of the public, and the like.

10

Also likewise, reference to a Immigration officer in a particular embodiment of the invention should not be taken to limit the scope of the invention in its broadest form. In other forms of the invention, the role of the Immigration officer is taken by another type of authorised officer, a security officer, crowd controller, employee or the like.

15

Reference is made to a passport, the reader will appreciate that in different applications or embodiments of the present invention, a person can provide other electronically readable documentation, if such documentation is required at all, such as, for example, a drivers license, identity card, membership card, access card, credit card, security token or the like.

20

In a first broad form of the invention, there is provided a method of providing access control of a person attempting to move from a first area to a second area, the method including the steps of: providing a walled passageway between the first area and the second area, the walled passageway including at least: an interface unit to obtain biometric
25 information from the person; and, an exit gate; allowing the person to enter the walled passageway; attempting to identify the person; verifying whether the person is authorised to enter the second area; opening the exit gate and allowing the person to proceed to a control gate, the control gate being set in one of the positions of: closed, thereby directing the person to enter the second area; or blocked, thereby directing the person to a holding
30 area for further processing.

In a second broad form of the invention, there is provided a system for providing access control of a person attempting to move from a first area to a second area, the system including: a walled passageway between the first area and the second area, the walled

passageway including at least: an interface unit to obtain biometric information from the person; and, an exit gate; an holding area; a control gate provided between the exit gate and the second area, the control gate able to be set in at least the positions of closed or blocked; and, a processing system adapted to attempt to identify the person.

5

Other biometric identification systems, besides facial recognition, can be implemented with the present systems, for example fingerprint or iris recognition, by incorporating appropriate recognition software and hardware.

10 **Brief Description Of Figures**

The present invention should become apparent from the following description, which is given by way of example only, of a preferred but non-limiting embodiment thereof, described in connection with the accompanying figures.

15 Fig. 1 illustrates an example perspective view of the F-Point and S-Point systems according to an embodiment of the present invention;

Fig. 2 illustrates an example sectional view of the F-Point and S-Point systems according to an embodiment of the present invention;

20 Fig. 3 illustrates an example of the Passenger Interface Unit (PIU) according to an embodiment of the present invention;

Fig. 4 illustrates an example plan view of the F-Point system configured as a four gate array according to an embodiment of the present invention;

Fig. 5 illustrates an example perspective view of the S-Point system according to an embodiment of the present invention;

25 Fig. 6 illustrates an example plan view of the S-Point system according to an embodiment of the present invention;

Fig. 7 illustrates an example of a possible software architecture according to an embodiment of the present invention;

30 Fig. 8 illustrates an example flow chart of the process steps for providing automated processing according to an embodiment of the present invention;

Fig. 9 illustrates an example flow chart (continued from Fig. 8) of the process steps for providing automated processing according to an embodiment of the present invention;

Fig. 10 illustrates an example flow chart (continued from Fig. 9) of the process steps for providing automated processing according to an embodiment of the present invention;

Fig. 11 illustrates an example flow chart (continued from Fig. 10) of the process steps for providing automated processing according to an embodiment of the present invention; Fig. 12 illustrates an example of the transaction delivery sequence according to an embodiment of the present invention.

5

Modes For Carrying Out The Invention

The present invention should become apparent from the following description, which is given by way of example only, of a preferred but non-limiting embodiment thereof, described in connection with the accompanying figures.

10

The preferred embodiments are generally described with reference to passenger control at Immigration, however, the reader will appreciate that the present invention could be readily applied to other situations requiring the directing, processing and/or controlling of individuals, for example at the entrance to a building, etc., and the Immigration officer is interchangeable with a security officer or the like.

15

A Trust Point (herein referred to as T-Point) is a known system using an electronic passport reader to allow the introduction of SC37/ICAO (International Civil Aviation Authority) standards for face recognition processing. This design is considered to provide a low level of physical security due to the nature of peoples movements in front of a kiosk (eg. a Immigration desk) and should only be relied upon for use by trusted passengers.

20

A Flow Point (herein referred to as F-Point) is an alternate design with a single exit and is illustrated in Fig. 1 and Fig. 2. The F-Point provides a semi-automated border control system, in that a Immigration officer is required to direct any 'exception' passengers but 'cleared' passengers can pass through in an automated manner. In a specific example, the side gate enclosure 100 can be less than 200mm wide. The F-Point is designed to be face recognition friendly with only a single vertical structural support for a Passenger Interface Unit 110 and a light over display. The entry gates 120 shown in Figs. 1 and 2 are optional and can be included into the passenger flow control processing logic.

25

30

A Secure Point (herein referred to as S-Point) is an improvement that extends the F-Point concept and can be used for secure processing of persons with face recognition. In a

particular form, the S-Point can also utilise the design embodiments illustrated in Fig. 1 and Fig. 2.

5 A Virtual Point (herein referred to as V-Point) does not require a fixed physical transaction point or gate for the processing of passengers. The V-Point can make use of arrays of passenger tracking systems providing a virtual transaction point or gate.

Each of these systems may include a Decision Point (herein referred to as D-Point), which includes a computer-based application. The application can incorporate an electronic
10 document reader and an OCR (Optical Character Recognition) reader, for example designed to be used by an Immigration Officer on a primary line to support or perform passenger exception processing.

The application could also be used to actively monitor and control various transaction
15 points that may be in use (that is T-Points, F-Points, S-Points and/or V-Points), to assist passengers using transaction points, and to set the operational state of a transaction point(s) to 'in service' or 'out of service'. A D-Point can be designed to a variety of requirements.

20 A Passenger Tracking System (PTS) may also be utilised that is capable of being used within and around various transaction points so as to monitor passenger physical movements and thereby increases physical border security. The passenger tracking system lends itself to provide an additional level of security.

25 Embodiments of the present invention can thus provide:

- (a) a staged approach to implementing automated border crossing systems at airports.
- (b) a system for processing aircrew using data stored in a SQL database and/or a passport RF chip – depending on the age of a passport.
- (c) more transaction points to cater for increased volumes of passengers.
- 30 (d) biometrics or different templates used in passports.
- (e) design of a transaction point to make authentication transactions intuitive for passengers and crew who travel infrequently, i.e. processing without a person necessarily having to stop at a fixed transaction point.

Flow Point (F-Point) Design

The F-Point, when utilised in a Immigration context, can include:

- (1) A single gate array 100 that can be installed in multiple instances and which can be controlled by a single Immigration officer operating a D-Point;
- 5 (2) Pass through processing of passengers allowing controlled and uninterrupted passenger flow – the design requires the manual direction of exception passengers to a primary line workstation, including a D-Point, allowing for manual processing of passengers who cannot, for whatever reason, be processed by the F-Point;
- (3) A Passenger Tracking System (PTS) that provides passenger movement information,
10 such as when two or more passengers are in the gate enclosure at any one time or if a passenger has left luggage in the gate enclosure;
- (4) A compact Passenger Interface Unit (PIU) 110 that is intuitive and non-intrusive to a passenger, and is face recognition friendly. The PIU can automatically adjust to a passenger's height by moving the PIU to be at passenger face height. Referring to Fig.
15 3, the PIU 110 includes:
 - (A) A linear polarised backlit display 310 to provide uniform light on a passenger's face, which in conjunction with a linear filter over the camera lens, reduces/eliminates glare on glasses;
 - (B) A compact LCD display 320 and speaker to provide visual/audio cues to the
20 passenger; and,
 - (C) A camera (not illustrated) to capture a video stream to be processed by a software application on a Biometric Processing Unit;
- (5) An electronic document reader 130, for example an ISO14443 Type B contactless chip reader that is compliant and tested with ICAO standards for face and fingerprint
25 recognition processing requirements;
- (6) An Overhead Information System (OIS) that provides uniform and diffused down lighting over the gate area, visual cues by way of illuminated graphics to passengers (such as enter, stop, out of service, etc.), and status indicators to provide visual cues to the Immigration officer manning a holding area on the processing status of a gate
30 array comprising F-Points;
- (7) An Operational Control and Monitoring System (OCMS) allowing remote monitoring and control of the F-Point, providing status, alarms, warnings and control of the F-

Point, as well as recording access and maintenance functions performed by authorised technicians;

(8) An interface to a D-Point unit, being, for example, a PC based application incorporating:

5 (A) A touch screen, a PC, a keyboard and/or a mouse;

(B) An interface with the Immigration Entry/Exit Authorisation system;

(C) An OCR passport reader (optional); and,

(D) An electronic document reader;

10 which allows a Immigration officer to monitor and control the F-Point as well as allowing manual processing of passengers who are referred to the holding areas;

(9) A Biometric Control Unit (BCU) including a computer processing system, for example a PC, a UPS and control software for controlling:

(A) The customer interacting with the electronic document reader to access ICAO face image and passport information;

15 (B) The biometric processing and sequencing with the passenger interface unit;

(C) The systems interface to the Immigration Entry/Exit Authorisation system;

(D) Communications with servers;

(E) Systems interface to the OCMS;

(F) Logic control of the swing gates and sensor arrays;

20 (G) The movement of a passenger within the gate by the passenger tracking system; and,

(H) The overhead information system.

25 The F-Point affords a medium level of passenger movement assurance in that the design is a semi-automated border control system flow requiring little or no manual intervention by a Immigration officer during the normal processing phase.

30 Exception passengers are held in the gate until the Immigration officer acknowledges that the passenger in the gate requires to be processed manually. The Immigration officer acknowledges this by either pressing a button (identified by a gate number) or by interacting with a touch screen in the appropriate D-Point application design.

In a flow through design (such as the F-Point and the S-Point), passengers are not directed back into a queue area under any circumstances, thereby increasing throughput of passengers through the transaction point.

5

In an F-Point, if a passenger has not placed their electronic passport successfully onto the reader 130 within a configurable timeout period (the inactivity period - say 6 seconds after entering the gate), the F-Point can classify the passenger as an exception and raise a 'direct the passenger to the holding area' to the Immigration officer, thereby avoiding congestion of the F-Point.

10

In an F-Point, left and right gate arrays operate independently of each other. In a gate clear mode, the F-Point knows that no one is in the gate area. The entry gates (if entry gates are provided) are open and the exit gates are closed. In gate occupied mode, passenger processing occurs. If, at any time, the processing fails, the passenger can be treated as an exception passenger.

15

If the passenger is treated as an exception, the controlling Immigration officer can be informed audibly and visually of the exception, and be required to acknowledge the exception message raised in that gate by either:

20

- (1) Basic D-Point - pushing a button matched to the gate number in question which can open the exit gate;
- (2) Advanced D-Point - pushing a button on a touch screen display on the D-Point mounted on their workstation (which can also provide details of the exception that occurred) which opens the exit gate.

25

Once the passenger (and luggage) has cleared the gate, the exit gate closes and the gate is considered to be in gate clear mode.

When a passenger has entered the gate area, the following high level operations occur.

30

- (1) Wait for Electronic Travel Document (ETD):

Process: The F-Point:

- (A) Automatically closes the entry gate (optional);
- (B) Registers the height of the passenger entering the gate area;

- (C) Adjusts the height of the PIU such that the PIU moves to the same level as the passenger's face;
- (D) Displays on the LCD display in the PIU a series of graphics or streamed video to direct the passenger to place their ETD on the reader;
- 5 (E) Starts the timeout loop counter on the inactivity period.

Results: The passenger either:

- (F) Valid: Places their ETD on the reader and the ETD is valid;
- (G) Exception: Two or more passengers enter the gate area, in which case the processing fails and they are treated as exception passengers – no delay;
- 10 (H) Exception: Passenger fails to place their ETD on the reader – inactivity period delay;
- (I) Exception: Reader fails to read the ETD – ETD has failed or is fraudulent – read period delay.

15

(2) Biometric Processing:

Process: If the ETD read is valid:

- (A) The ICAO enrolment image is made available to the biometric control unit (BCU);
- 20 (B) The polarised illuminated ring around the PIU lights up drawing the passengers attention to the PIU;
- (C) The LCD in the PIU indicates to the passenger to remove dark glasses, wait and to look at the camera;
- (D) The BCU starts the BCU timeout counter (configurable - say 3 seconds);
- 25 (E) The camera commences framing images of the passenger and passing them to the BCU for processing;
- (F) The BCU compares captured images with the ICAO reference enrolment image;
- (G) If the verification exceeds the configurable system threshold level set within the BCU timeout period, the passenger has passed biometric processing;
- 30 (H) The polarised light ring around the PIU is turned off and the passenger is requested by the PIU LCD display to pickup their ETD and luggage and be ready to proceed through the exit gate.

Results: The passenger either:

- (I) Valid: Passes biometric processing; or
- (J) Exception: Face is not found and the passenger is treated as an exception passenger – biometric timeout delay;
- 5 (K) Exception: Face is found but does not meet the threshold level – biometric timeout delay;
- (L) Exception: Face is found but the level of recognition is extremely low (configurable) – warning raised.

10 (3) Immigration Processing:

Process: If the passenger passes biometric processing:

- (A) Selected information read from the ETD is passed through the Immigration Entry/Exit Authorisation system interface to external systems for processing;
- (B) The application starts the immigration timeout counter (configurable, say 6 -
15 10 seconds);
- (C) Subject to the the Immigration Entry/Exit Authorisation system clearance response message or immigration timeout, the passenger is either cleared or is classified as an exception passenger.

20 Results: The passenger either:

- (D) Valid: Places immigration processing; or
- (E) Exception: the Immigration Entry/Exit Authorisation system clearance failed – the Immigration Entry/Exit Authorisation system response delay;
- (F) Exception: the Immigration Entry/Exit Authorisation system clearance timeout
25 - immigration timeout delay.

(4) Processing Complete:

If the passenger has passed each of the read ETD, biometric and immigration clearance processes, the passenger is considered cleared and the following can occur:

- 30 (A) A gate clear timeout commences, (configurable, say 3 seconds);
- (B) The exit gate opens;
- (C) The passenger clears the gate, the exit gate closes, the entry gate (if fitted) opens and the system is returned to gate clear mode ready to process the next passenger.

Fig. 4 illustrates a F-Point four gate array, constructed of either complete F-Point units 100 with half entry gate flaps, or sectional F-Point units arranged with full entry gate flaps. Each F-Point passenger gate section 410, directs a passenger past a PIU 110. Exit gates 420 open after processing to allow an Immigration officer 430 to direct a passenger to a holding area 440 for manual processing, if required.

There may be restrictions of use to specific passengers using F-Point (or S-Point) who may be required to be manually processed by Immigration officers on the primary line due to issues such as persons below the minimum agreed height/reach ranges; children below a minimum age; adults with children; persons in wheelchairs.

Secure Point (S-Point) Design

A Secure Point (or S-Point) is designed to be used by passengers to facilitate relatively fast and secure processing of passengers with electronic travel documents. S-Points are preferably installed as a tandem array of two gate lanes. Referring to Figs. 5 and 6, an S-Point 500 is an arrangement of two F-Points which have been improved to include entry gates 510 with the addition of a holding area 520 and associated interlocking gate logic and a D-Point 530 (optional). An S-Point can use the document reader 130 and PIU 110 as described for the F-Point.

Generally, S-Point is a security access control method and system allowing for a fully automated and secure subject identification and verification processing system for subjects attempting to pass through a secure line (such as passengers crossing an immigration primary line at an airport or land-crossing) using personal identification technologies (such as a combination of tokens and biometric access control technologies) incorporating verification stations, interlocking of subject direction gates and sensors providing a high flow through rate of subjects, augmented by exception processing controls that direct subjects to a holding area which is operated by an authorised officer (person(s)), for additional processing while allowing the system to continue processing subsequent subjects normally.

In a particular embodiment, S-Point includes a software logic and automated control program combined with personal identification and verification technologies incorporating a left hand and right hand verification station. Also included is an array of sensors to determine whether an area is clear or occupied and which direction a subject is moving
5 and two enclosed gate control areas in an array. A controlled secure area featuring an entry and exit point and side walls that are sufficiently high to not allow subjects to pass objects to other subjects is also provided. The walls contain the subject while identification / verification processing is being performed.

10 Also provided is an entry gate that either allows (in the open position) or disallows (in the closed position) a subject to enter the identification/verification station dependant on whether the prior subject is being processed and an exit gate that either contains the subject while the subject is being processed (in the closed position) or which open to allow the passenger to proceed forward to clear the verification station.

15

Furthermore, a holding area automatically controlled by S-Point and operated by an authorised officer using a system of interlocking gates includes two control gates (one for each verification station) which operate independently allowing subject processing to continue, operating in one of three gated positions (closed, open and blocked). This
20 directs passengers through the primary line on the condition they have been verified and cleared to pass through by the system (control gate remains in the closed position – the default position), or to the holding area for exception subjects if they have not been recognized or cleared by the system (control gate swings from open position to blocked position directing subject into holding area and then swings back to closed position once
25 the subject has entered the holding area to allow the verification station to continue processing other subjects).

A Decision Point (D-Point) includes a PC system with a token reader and operated by an authorised officer allows for manual enquiries and verification processing of exception
30 subjects who have been subsequently cleared to exit the holding area under the direction and control of the authorised officer. Such persons proceed past the primary line through

one of the control gates (by the exit gate in the verification station remaining closed while the control gate swings from closed position to open position to allow the subject to move out of the holding area and past the primary line at which time the control gate returns to the closed position allowing the verification station to continue processing other subjects.

5 Alternatively, the subject passes through an access gate controlled by an authorised officer to escort 'at risk' subjects to another location, such as a secure office, for further processing. This may be supervised by one or two authorised officers.

S-Point provides fully automated and secure handling of three types of subjects who are

10 processed normally and allowed entry by the system (normal processing), and are not processed normally and require secondary consideration to gain entry (exception processing). This may be due to the subject not being recognised by the system for the following reasons (in which case the system can, after a configurable timeout period, allow the verification station to automatically direct the subject to the holding area for

15 manual processing): the inability of the system to validate the subject in system databases or information systems the system draws upon; the inability of the system to successfully process the subject using the biometric validation or combination of biometric validation processes; the subject does not have a token (such as an electronic passport) if so required by system processing; their token (such as an electronic passport) if so required, cannot be

20 read by the system (for reasons such as the positioning or alignment of the token by the subject to the token reader, a malfunction or failure of the token itself or the subject has not placed their token onto the token reader and hence cannot be assessed); or the subject is recognised but is not permitted to pass the primary line due to restrictions on entry mandated by the processing authority in which case, the subject would be automatically

25 directed by verification station to the holding area for additional manual processing and potentially to be escorted through the access for additional processing by others.

The S-Point, when utilised in a Immigration context, can include:

- (1) A tandem gate design 500, gates are installed in pairs with a holding area 520
- 30 and can be controlled by a single Immigration officer 540;
- (2) Pass through processing of passengers allowing secure and uninterrupted
- passenger 550 flow – the design incorporates a holding area 520 in front of the

existing primary line allowing for manual processing of passengers who cannot, for whatever reason, be processed by the S-Point;

- 5 (3) A Passenger Tracking System (PTS) that provides passenger movement information, such as when two or more passengers are in the gate enclosure at any one time or if a passenger has left luggage in the gate enclosure;
- (4) A compact Passenger Interface Unit (PIU) 110 that is intuitive and non-intrusive to a passenger, and is face recognition friendly. The PIU can automatically adjust to a passenger's height by moving the PIU to be at passenger face height. The PIU includes:
- 10 (A) A linear polarised backlit display to provide uniform light on a passenger's face, which in conjunction with a linear filter over the camera lens, reduces/eliminates glare on glasses;
- (B) A compact LCD display and speaker to provide visual/audio cues to the passenger; and,
- 15 (C) A camera to capture a video stream to be processed by a software application on a Biometric Processing Unit;
- (5) An electronic document reader 130, for example an ISO14443 Type B contactless chip reader that is compliant and tested with ICAO standards for face and fingerprint recognition processing requirements;
- 20 (6) An Overhead Information System (OIS) that provides uniform and diffused down lighting over the gate area, visual cues by way of illuminated graphics to passengers (such as enter, stop, out of service, etc.), and status indicators to provide visual cues to the Immigration officer manning a holding area on the processing status of a gate array comprising S-Points;
- 25 (7) An Operational Control and Monitoring System (OCMS) allowing remote monitoring and control of the S-Point, providing status, alarms, warnings and control of the S-Point, as well as recording access and maintenance functions performed by authorised technicians;
- (8) An interface to a D-Point unit, being, for example, a PC based application
- 30 incorporating:
- (A) A touch screen, a PC, a keyboard and/or a mouse;
- (B) An interface with the Immigration Entry/Exit Authorisation system;
- (C) An OCR passport reader (optional); and,
- (D) An electronic document reader;

which allows an Immigration officer to monitor and control the S-Point as well as allowing manual processing of passengers who are referred to the holding areas;

- 5 (9) A Biometric Control Unit (BCU) including a computer processing system, for example a PC, a UPS and control software for controlling:
- (A) The customer interacting with the electronic document reader to access ICAO face image and passport information;
 - (B) The biometric processing and sequencing with the passenger interface unit;
 - (C) The systems interface to the Immigration Entry/Exit Authorisation system;
 - 10 (D) Communications with servers;
 - (E) Systems interface to the OCMS;
 - (F) Logic control of the swing gates and sensor arrays;
 - (G) The movement of a passenger within the gate by the passenger tracking system; and,
 - 15 (H) The logic control of the swing gates and sensor arrays;
 - (I) The interlocking of control gates 560 in the holding area 520; and,
 - (J) The overhead information system.

The S-Point affords the highest level of passenger movement assurance in that the design
20 is a fully automated border control system requiring no manual intervention by a Immigration officer 540 in the processing phase. Exception passengers (eg. 570) are automatically directed into a holding area immediately in front of the exception processing workstation on the primary line.

25 Once a passenger is processed, the Immigration officer directs the passenger using either a control gate 560 to exit between the primary line workstations or an access gate 580 so as to be escorted by another Immigration officer back into the queue area. When the control gates 560 are being operated, the gate lane exit gates 590 do not operate (gates are interlocked), which means that a passenger being processed by the S-Point 500 cannot
30 interfere with the cleared exception passenger being direct out of the holding area by the Immigration officer. The control gates 560 can thus be in three alternate states of open, blocked or closed as illustrated.

In an S-Point, if a passenger has not placed their electronic passport successfully onto the reader within a configurable timeout period (the inactivity period - say 6 seconds after entering the gate), the S-Point can classify the passenger as an exception and direct the passenger to the holding area 520, thereby avoiding congestion of the S-Point.

5

In an S-Point, the left and right gate arrays operate independently of each other, as does the operation of the control gate. The only exception is the interlocking of the exit gate and the control gate of the same gate array in the event that two passengers are attempting movements at the same time.

10

In gate clear mode, the S-Point knows that no one is in the gate area. The entry gates are open and the exit gates are closed. In gate occupied mode, passenger processing occurs. If at any time the processing fails, the passenger can be treated as an exception passenger.

15 If the passenger is treated as an exception, the control gate on the gate array swings into the blocked position, the exit gate then opens and the passenger is directed by the LCD of the PIU to proceed into the holding area. If a D-Point is configured, a message is sent to the Immigration officer operating the D-Point about the nature of the exception and any other available information related to the cause of the exception.

20

Once the passenger (and luggage) has cleared the gate and is in the holding area, the exit gates close, the control gate swings back into the closed position and the gate returns to gate clear mode.

25 When a passenger has entered the gate area, the following high level operations can occur as previously described for the F-Point under the broad headings of (1) Wait for Electronic Travel Document (ETD); (2) Biometric Processing; and (3) Immigration Processing.

For the (4) Processing Complete step:

30 If the passenger has passed each of the read ETD, biometric and immigration clearance processes, the passenger is considered cleared and the following can occur:

(A) A gate clear timeout commences, (configurable, say 3 seconds);

(B) The gate control application checks that the control gate is not being operated by the Immigration officer, if it is then processing waits until the Immigration operation is completed;

(C) The control gate is closed and the exit gate is open;

5 (D) The passenger clears the gate, the exit gate closes, the entry gate opens and the system is returned to a gate clear mode ready to process the next passenger.

Decision Point (D-Point) Design

Three main types of D-Points could optionally be provided.

10

(1) Basic D-Point:

Each of the T-Point, F-Point and S-Point designs can use a single basic D-Point configuration which comprises an array of contact switches and indicator lights mounted into a workstation on the primary line that allows the Immigration officer manning the workstation to control the operation of the gates (indicators and switches are supplied for
15 each gate in the gate array installed) and to be advised that an exception passenger has occurred. Intrusion alarms can be recorded by the BCU to a log file, and basic alarm and warning states can be shown on indicators or by audible alarm.

20 (2) Advance D-Point:

A D-Point could run on a PC (or multiple PCs) which allows the Immigration control officer to be fully informed as to the processing stages and to be able to control each of the gates in the gate array. Such an application could run on a PC with a touchscreen interface, and/or a keyboard/mouse to enter or select information. Control may be by touching a soft
25 switch on the touchscreen to select a specific gate, to drill down for information on the gate, and to review the biometric performance of previous transactions.

(3) Primary Line D-Point:

Primary line processing for exception processing can be performed on the same system.
30 This design of D-Point requires an updated Immigration Entry/Exit Authorisation system interface, an OCR reader and a electronic document reader.

Passenger Tracking System (PTS)

In a particular embodiment, the PTS utilises a series of active infra-red PE Beams and a dedicated microprocessor controller. Two rows of PE beams are installed horizontally on each wall of the immigration gate. The lower row is installed at a height low enough to detect a passenger's hand luggage as well as the lower portion of his/her legs. These lower PE's can also detect luggage which is inadvertently left behind by a passenger. The upper row's main function is to detect the torso. With these two rows combined with a thermal detector mounted overhead each lane it is possible to distinguish between multiple people and luggage.

10 The PTS accepts inputs via the series of upper and lower PE beams (for example between 20 to 28 beams dependant on requirements) together with the thermal detector and digitally filters the raw data. Data is then subjected to a comprehensive series of profile matching algorithms to ascertain the number of persons and/or luggage within the detection area.

15 The status of the PTS is constantly being polled by the biometric control unit application via either a high level serial or low level relay output to direct the operation of the various system elements. In a specific non-limiting form, the PTS may be a PTS system offered by Magnetic Automation Pty Ltd, of Australia.

20

Virtual Point (V-Point) Design

In this embodiment authentication/processing transactions are sought to be made intuitive by not requiring persons to stop at a fixed transaction point.

25 A V-Point comprises an arrangement of components of the various transaction points, system interfaces to other external systems, and a control application to track passengers moving through the pre-clearance terminal enclosure.

30 This aspect of the invention involves a secure and automated flow through subject identification and verification process that allows for relatively rapid processing of subjects without controlled gated areas, and the flexibility to allow an authorised authority to have as many Decision Points (D-Points) operating as required without taking up valuable floor space or resources.

The invention seeks to identify subjects in a tunnelled or restricted free format area and then to track subjects through a wide controlled area using a matrix array of coordinated infra-red sensors mounted throughout the controlled area. The system is able to reliably inform whether the subject approaching the Decision Point is the person identified in a manifest list within the threshold limits set by the system, or the system does not identify the subject.

The Passenger Tracking System makes appropriate decisions if the subject attempts to either knowingly or unknowingly change positions with another person by either de-identifying both persons are by re-acquiring their identities. The system can perform additional checks such as, is this person authorised to pass through the access line and so inform the authorised officer. The Passenger Tracking System can identify a mother and child in close proximity by the head heat signature of each person.

Other embodiments of the invention allow a person to be tracked through an entire building if so required, not just for access control.

V-Point is a security access control method and system allowing for the fully automated, rapid and secure identification and verification processing of subjects attempting to pass through a secure line (such as passengers crossing an immigration primary line at an airport or land-crossing), using personal identification technologies (such as a combination of tokens and biometric access control technologies and specifically biometric face recognition) thereby allowing subjects to be identified by non proximity readers (such as an array of roof mounted cameras to capture the subject's face image while they come down a channelled area prior to entering a larger area such as immigration clearance). The subject is processed and matched against a range of biometric enrolment identifiers provided on manifest lists that accommodate the subjects arrival in a group or individually (such as passenger flight manifest containing a biometric enrolment image or biometric template), such that subjects are identified prior to approaching the primary line. Subjects are then tracked by the system wherever they move prior to approaching an authorised officer provided with a computer system that can be used to identify the subject to the authorised officer for final visual confirmation of the subject for secure line processing. The Passenger Tracking System used can incorporate infra-red sensing technology.

A software application (herein referred to as V-Track), running on a hardware platform, co-ordinates and tracks the movements of passengers once they have been identified using an array of passenger tracking systems (known as tracking cells).

- 5 The PTS incorporates infrared sensing technology and is able to distinguish a mother with child by tracking a head heat signature for each person. In a specific non-limiting form, the PTS may be a PTS system offered by Magnetic Automation Pty Ltd, of Australia.

Features of V-Point include:

- 10 (1) A flight manifest/list (or watch list) of passengers including an ICAO compliant enrolment image of arriving passengers;
- (2) A predefined area (the identification area) where individual passengers can be identified by use of face recognition technology using 'face in a crowd' techniques referenced against the flight manifest;
- 15 (3) A predefined area (the tracking area) which represents the area limits in which a passenger can wander before being cleared on the primary line. A passenger cannot be allowed to wander outside of the tracking area if they are to be cleared by the V-Point system.
- (4) A D-Point, or multiple D-Points, that provide immediate and intuitive
- 20 information to a Immigration officer as passengers approach the D-Point, which allows the Immigration officer to direct the passenger appropriately to additional processing options relevant to the extent that the V-Point has processed each passenger.

- 25 The identification area and the tracking area should overlap and extend upto the D-Point.

(1) Flight List:

The flight list requires a systems interface to one or more of the following systems to provide the ICAO enrolment image to be attached to the watchlist with ETD details:

- (A) co-operating airlines who may use face recognition systems requiring a
- 30 passenger to present their ETD at the point of embarkation to ensure baggage and passenger have embarked;
- (B) port of departure immigration authorities control passing on the required information; or

(C) authorities preparing a watch list of citizens with an ETD from a centralised database.

(2) Identification Area:

5 The identification area includes an array of PTSs and a number of high quality PTZ cameras being ceiling or wall mounted. For practical sizing estimates, cells should overlap with each cell preferably covering a maximum 2500mm x 2000mm of floor area, which represents the nominal coverage of a PTS. The number of PTZ cameras required is dependent upon requirements, but might nominally be 5 in a tunnelled area. Lighting of
10 this area should also be optimised for face recognition purposes.

(3) Tracking Area:

The tracking area can include an array of PTS. The same maximum cell coverage should preferably apply as for the identification area.

15

As passengers are identified, the V-Track system places a request to the Immigration Entry/Exit Authorisation system for clearance. The Immigration Entry/Exit Authorisation system interface should not record a movement. The movement should be recorded by the Immigration officer at a D-Point after the passenger has been physically sighted and
20 directed to the clearance aisle.

25

V-Track has both face recognition components and tracking components, and cross checks and internal audit processes to validate watch list entries. V-Track also requires the Immigration officer to visually sight and confirm a passenger clearance.

The V-Point processing states that would be notified to the Immigration officer manning a D-Point could include:

(A) 'Cleared' – the V-Point has positively identified the passenger in the identification area and has been able to successfully request and receive an
30 immigration clearance for the passenger using a request to the Immigration Entry/Exit Authorisation system generated by information provided from the watch list for that person;

- 5 (B) 'Not Cleared' - the V-Point has positively identified the passenger in the identification area and has not been able to successfully request and receive an immigration clearance for the passenger using a request to the Immigration Entry/Exit Authorisation system generated by information provided from the watch list for that person;
- (C) Exception – the V-Point has not been able to either identify the passenger in the identification area, or the person has moved out of the bounds of the tracking area, or has been 'lost' by the PTS.

10 As a passenger approaches a D-Point, the D-Point may display either:

(A) A red ring meaning the passenger has been processed with an exception state. It would be expected that the passenger:

- (i) is directed for processing at an S-Point or F-Point if they have an ETD;
- 15 (ii) is directed to a manual processing point if they do not have an ETD;

(B) A green ring meaning the passenger has been identified but not cleared. They have been processed as 'not cleared'. It would be expected they would be referred to an S-Point or F-Point;

(C) The passenger's face from their ICAO enrolment image is displayed in which
20 case the Immigration officer would double click their finger on the touchscreen on the person's face confirming the movement of that passenger and directing them to the cleared aisle exiting the pre-clearance area.

Alternatively, as a subject approaches a D-Point, the D-Point can display the following
25 information if the system has been able to identify the subject:

- (1) The subjects biographical information;
- (2) an image (face if face recognition) of the enrolment record for the subject; and
- (3) a coloured ring around the subject's enrolment image, which may be:

(A) Red (or other configurable colour) indicates the subject does not have
30 appropriate security clearance. D-Points can be configured that red subjects must move away to the right or the left. If a subject moves in the wrong direction, an audible and/or visual alarm can activate warning the authorised Officer;

- 5 (B) Green (or other configurable colour) indicates that the subject has been identified by V-Point and has been authorised to proceed past the access line. The authorised officer would acknowledge that they have visually checked the subject's face (and token identification information) against the enrolment information providing on the D-Point screen and allow the subject to pass through the access line;
- 10 (C) No image or coloured ring indicating that V-Point has not been able to identify the subject. D-Points can be configured that unidentified subjects must move away to the right or the left. If a subject moves in the wrong direction, an audible and/or visual alarm can activate warning the authorised officer.

Software Architecture

Software services to support the aforementioned systems are illustrated in Fig. 7.

15

'FaceIV' as used herein is a set of libraries developed by Fieldware Pty Ltd, of Australia. These libraries provide system integrators with a framework to simplify the integration of facial biometric software (normally implemented in C++) into enterprise business systems (often implemented using J2EE). The libraries are can be implemented in Java, using J2EE standards, and provide support for live verification, manual verification, FIR creation and storage, similarity calculation, queuing of transactions and publishing of biometric events using JMS.

20

Figs. 8, 9, 10 and 11 illustrate flow charts for process control in an automated border control system, for example as previously discussed with reference to V-Point. These flowcharts detail specific logic steps that may be utilised and how exception passengers can be handled.

25

According to one particular, but non-limiting, embodiment of the present invention, the border control system adopts a component and modular based architecture. The system includes the major subsystems of a main capture system and a retrieval system. The main capture system can include registration, assessment, acknowledgment, verification and issuance. When a passport, or other electronic document is issued, the entire application

30

can be automatically moved to the a central host database for final completion of processing and archiving.

SmartGate system

- 5 According to a various embodiment of the present invention, the 'SmartGate' system supports biometric templates contained on, for example, a passport, as opposed to being stored in a database.

The physical architecture of the system (in terms of system nodes), can remain the same as
10 hereinbefore described, with the possible exception of separate servers to host a SQL server database application and other application services. That is, there are two main types of physical component: a SmartGate server and a verification station. Software services can be deployed in the following manner:

(A) SmartGate server

- 15 (1) SQL server 705
(2) J2EE (Java 2 Enterprise Edition) application server 710
(3) Transaction sink 715
(4) Transaction message queue 720
(5) Event topics 725
20 (6) Configuration server 730
(7) Event monitoring service 735
(8) Reporting service 740

(B) Verification Station

- (1) Verification service 745
25 (2) Face recognition processing engine 750
(3) J2EE application server 710
(4) SQL server 705 (eg. Desktop edition)
(5) Configuration service 755

30 The advantages of using J2EE and the FaceIV framework include:

- (1) Corporate - Common use of Java in enterprise business systems, providing availability, scalability and scope to be expandable;
(2) Standard - Use of standard protocols for messaging (avoiding the use proprietary mechanisms or direct database connections to perform data replication);

- (3) Security - The ability to force all communication between devices to go through an encrypted link. J2EE defines a standard for integration of a variety of common security frameworks and products, including SSL and PKI implementations;
- (4) Comparative Biometric Testing – FaceIV could allow comparison testing between vendors subject to licensing and uptake of other suppliers SDK;
- (5) Maintainable - Ease of software deployment and upgrades.

SQL Server 2000 Standard edition can be deployed on the SmartGate server. A J2EE application server could be hosted on the SmartGate server to provide enterprise-level, and standards-based services such as:

- (1) Message queuing
- (2) Web services
- (3) Event logging
- (4) Transaction processing
- (5) Security

Referring to Fig. 12, the application server could run other services required for the system as identified in the following sub-sections.

- (A) A transaction sink 1210 could be a J2EE-based application which stores transactions which have been put on the queue.

(B) A transaction message queue can be a JMS (Java Message Service – a J2EE standard for point-to-point and publish-and-subscribe messaging) -based message queue which allows the transactions to be delivered efficiently and transactionally to the server. JMS supports the point-to-point messaging concepts of guaranteed delivery and once-and-once-only delivery. The system could also support local storage of transactions (on the verification station) for the purpose of disaster recovery, allowing the system to “replay” transactions from a particular point in time if data corruption occurs. These transactions could be removed or archived from the verification systems at pre-defined intervals.

(C) An event topics service is a JMS-based service that supports the publish-and-subscribe mechanism of enterprise, distributed event handling. Verification stations could “publish” events to different topics, and various components of the event monitoring service could

“subscribe” to the various topics. These events could be configured to be stored in a variety of formats, including database, log files or a Windows event log.

5 (D) A configuration server could be a central point of management of verification stations, providing a database of locations and current status of devices. The interface could be web-based, such that those with appropriate security could configure various aspects of the system, including re-starting of individual stations, setting thresholds etc.

10 (E) An event monitoring service could monitor event/alarm topics and either forward on to another service and/or store the message either in the SQL server database, or as a text file in a particular format (for example XML). The “other service” could typically be an SNMP (Simple Network Management Protocol)-based service, allowing the system to be monitored by a COTS device monitoring product, such as HP OpenView. This would allow the network manager to have a graphical view of the system, being able to
15 view a high level diagram, and being able to “drill-down” to individual verification station details within, for example, an airport.

(F) A reporting system could be defined by a user, for example Immigration. With enterprise-level systems such as business objects, object-schemas could be created that
20 map to the physical database structure to allow intuitive creation of ad-hoc reports from SmartGate data. All data including transaction and event data can be reported. A data summarisation and archiving service could be designed to support data warehouse application.

25 (G) The verification service could contain additional processing of a biometric record obtained from, for example, a passport. A device preferably would include a computer operating system device driver. This is to primarily allow for reduced testing requirements, easier roll-out and the possibility of remote software upgrading of the verification stations.

30

(H) The face recognition processing engine could support the ability to accept an FIR or image from a smartcard on a passport, as opposed to a “token” (eg. the passport details), which requires a database lookup to obtain the FIR.

(I) The configuration service is a process running on each verification station which receives messages from the configuration server, running on the SmartGate Server. The configuration service controls the configurable parameters of a station, for example by having direct access to the physical device and manipulating text files. The service allows
5 remote management of the station.

A mechanism for the delivery of transactions is to use JMS point-to-point messaging. Transactions from the verification stations 1240 could be stored locally in the SQL server 1230 database and queued locally 1250 to be sent to the SmartGate server. A service on
10 the verification station 1240 would remove the transactions from the local queue 1250 and send them to the SmartGate server via an encrypted queue. The purpose of the intermediate queue is to allow each verification station to be configured to queue transactions to the server at different intervals, and to cater for the situation when the communications to the SmartGate server is down.

15
In this case, transactions would not be put 1255 on the encrypted queue 1260 until the server is available. The standard may be no interval – that is, transactions are immediately sent to the SmartGate server, enabling accurate up-to-the-minute status reports. This mechanism is not believed to be a network traffic issue, and hence should not affect the
20 interrogation or “movement” of persons.

An electronic document, for example an e-passport, life cycle begins with the registration and enrolment process for all new applications. Applications may vary from the type of passport applied for and to whom it is issued. Generally there are three types, diplomatic,
25 official and general.

The following includes a list of possible business activities: Issue new passport for expired passport; Issue new passport for missing passport; Issue new passport for an invalid passport due to torn pages; Issue a temporary travel document; Registration approval for
30 rightful applicants; Personal and biometric information data entry; Payment processing and audit trail; Data page printing and chip personalization; Quality assurance after personalization with visual inspection; Passport delivery and issuance with biometric verification to determine biometric in the chip matches that of the legal holder's.

The invention may also be said to broadly consist in the parts, elements and features referred to or indicated herein, individually or collectively, in any or all combinations of two or more of the parts, elements or features, and where specific integers are mentioned herein which have known equivalents in the art to which the invention relates, such known
5 equivalents are deemed to be incorporated herein as if individually set forth.

Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions, and alterations can be made herein by one of ordinary skill in the art without departing from the scope of the present invention.

The claims:

1. A method of providing access control of a person attempting to move from a first area to a second area, the method including the steps of:
 - 5 (1) providing a walled passageway between the first area and the second area, the walled passageway including at least:
 - (A) an interface unit to obtain biometric information from the person; and,
 - (B) an exit gate;
 - 10 (2) allowing the person to enter the walled passageway from the first area;
 - (3) attempting to identify the person using at least the biometric information;
 - (4) verifying whether the person is authorised to enter the second area;
 - (5) opening the exit gate and allowing the person to proceed to a control gate, and dependent upon the results of the identification and
15 verification steps the control gate being set in one of the positions of:
 - (A) closed, thereby directing the person to enter the second area; or
 - (B) blocked, thereby directing the person to a holding area for further processing.
 - 20
2. The method as claimed in claim 1, wherein the control gate can be set in the position of open, thereby directing a person in the holding area to enter the second area.
- 25 3. The method as claimed in either claim 1 or 2, wherein the walled passageway includes a token reader, the token provided by the person.
4. The method as claimed in any one of the claims 1 to 3, wherein more than one walled passageway is provided in an array with adjacent walled passageways
30 associated with at least one common holding area.
5. The method as claimed in any one of the claims 1 to 4, wherein the person can be directed from the holding area to the first area via an access gate.

6. The method as claimed in claim 3, wherein the token is an electronically readable document.
7. The method as claimed in any one of the claims 1 to 6, wherein the person is a passenger and the first area and the second area are separated by an immigration line.
8. The method as claimed in any one of the claims 1 to 7, wherein the walled passageway includes an entry gate.
9. The method as claimed in any one of the claims 1 to 8, wherein each gate is controlled by software on a processing system.
10. The method as claimed in any one of the claims 1 to 9, wherein the walled passageway includes an array of sensors to determine whether the passageway is occupied or clear.
11. The method as claimed in any one of the claims 1 to 10, wherein the holding area is used to manually process a person.
12. The method as claimed in any one of the claims 1 to 11, wherein the person is directed to the holding area if:
- the person is not identified;
 - the person is not verified as having access to the second area; or,
 - the person does not have a valid token.
13. The method as claimed in any one of the claims 1 to 12, wherein the person must be identified or verified within a preset time limit or the person is directed to the holding area.
14. A system for providing access control of a person attempting to move from a first area to a second area, the system including:
- (1) a walled passageway between the first area and the second area, the walled passageway including at least:

-32-

- (A) an interface unit to obtain biometric information from the person; and,
(B) an exit gate;
- (2) an holding area;
- 5 (3) a control gate provided between the exit gate and the second area, the control gate able to be set in at least the positions of closed, thereby directing the person to enter the second area, or blocked, thereby directing the person to the holding area; and,
- 10 (4) a processing system adapted to attempt to identify the person using at least the biometric information and to verifying whether the person is authorised to enter the second area.
- 15 15. The system as claimed in claim 14, wherein the walled passageway includes a token reader.
16. The system as claimed in either claim 14 or 15, wherein more than one walled passageway is provided in an array, with adjacent walled passageways associated with at least one common holding area.
- 20 17. The system as claimed in any one of the claims 14 to 16, wherein the holding area is partially bounded by an access gate.
18. The system as claimed in any one of the claims 14 to 17, wherein the walled passageway includes an entry gate.
- 25 19. The system as claimed in any one of the claims 14 to 18, wherein the processing system automatically controls operation of the gates.
20. The system as claimed in any one of the claims 14 to 19, wherein the walled passageway includes a person tracking system.
- 30 21. The system as claimed in any one of the claims 14 to 20, wherein the interface unit obtains facial biometric information from the person.
22. The system as claimed in claim 21, wherein the interface unit automatically adjusts to a person's height.

FIGURE 1

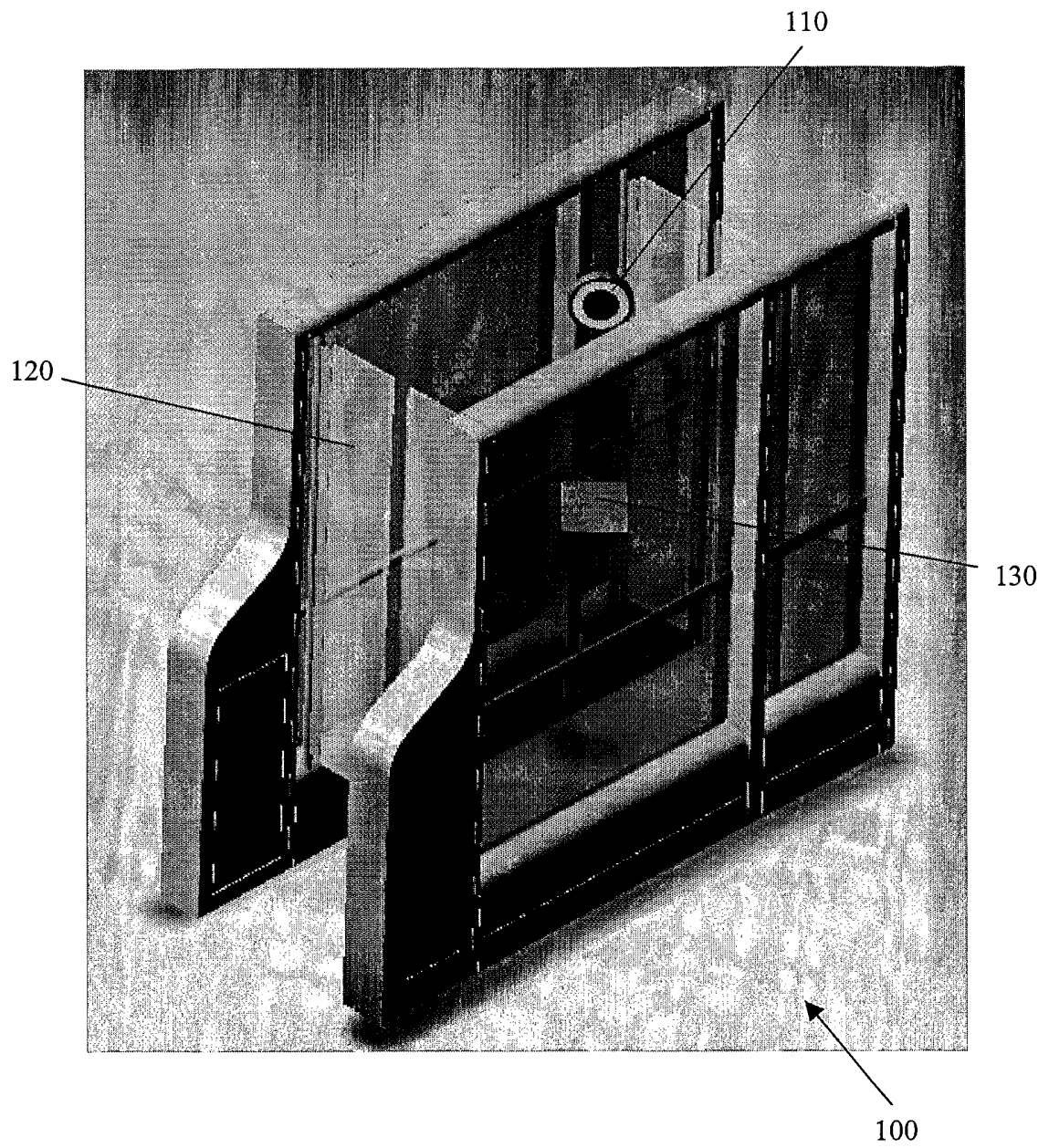


FIGURE 2

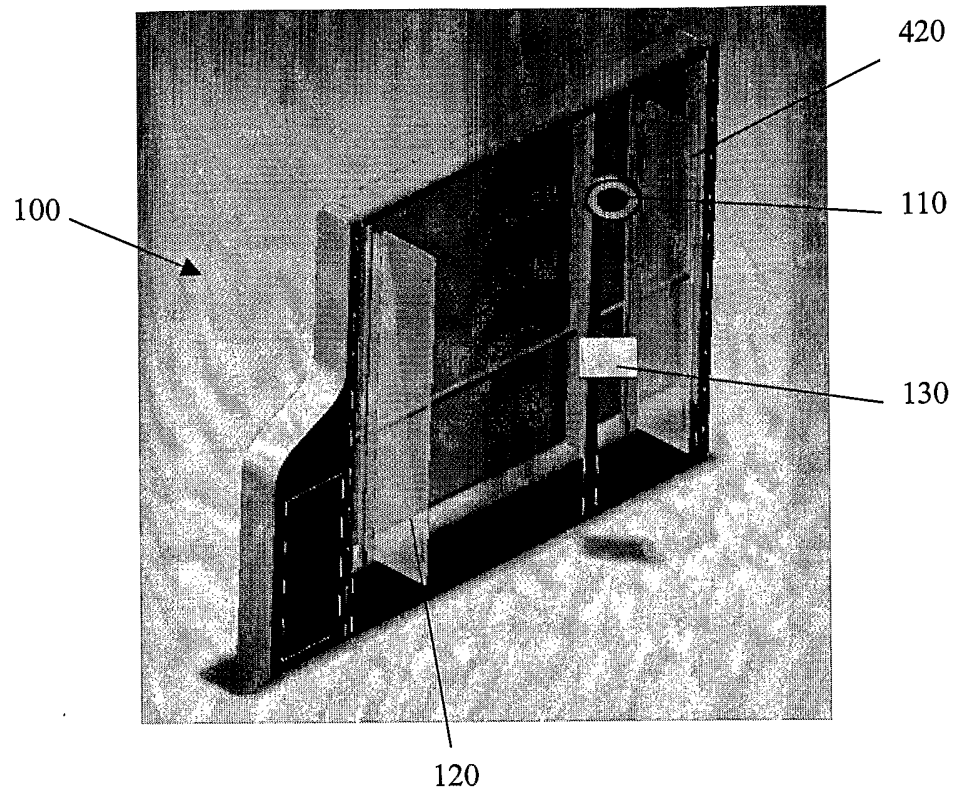


FIGURE 3

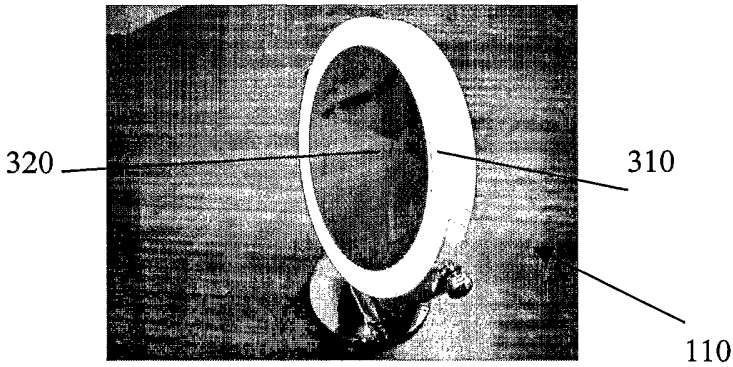


FIGURE 4

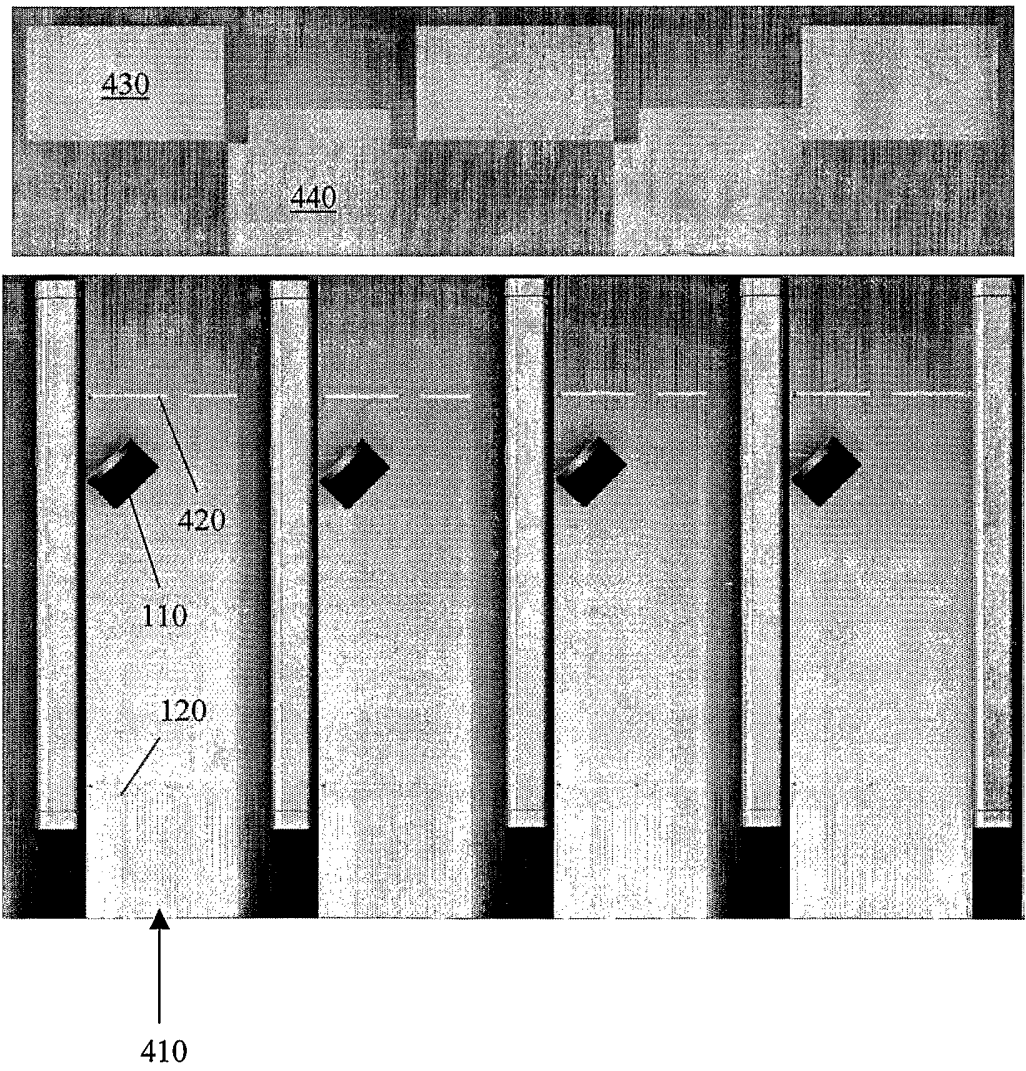
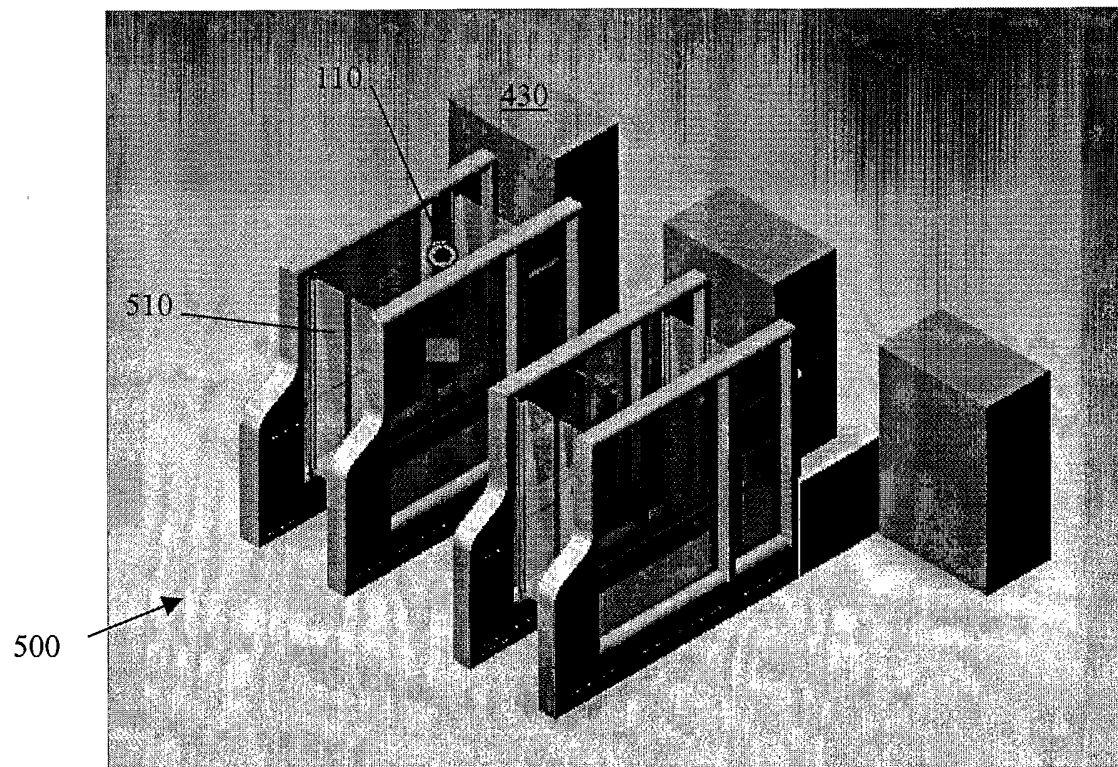


FIGURE 5



-5/11-

FIGURE 6

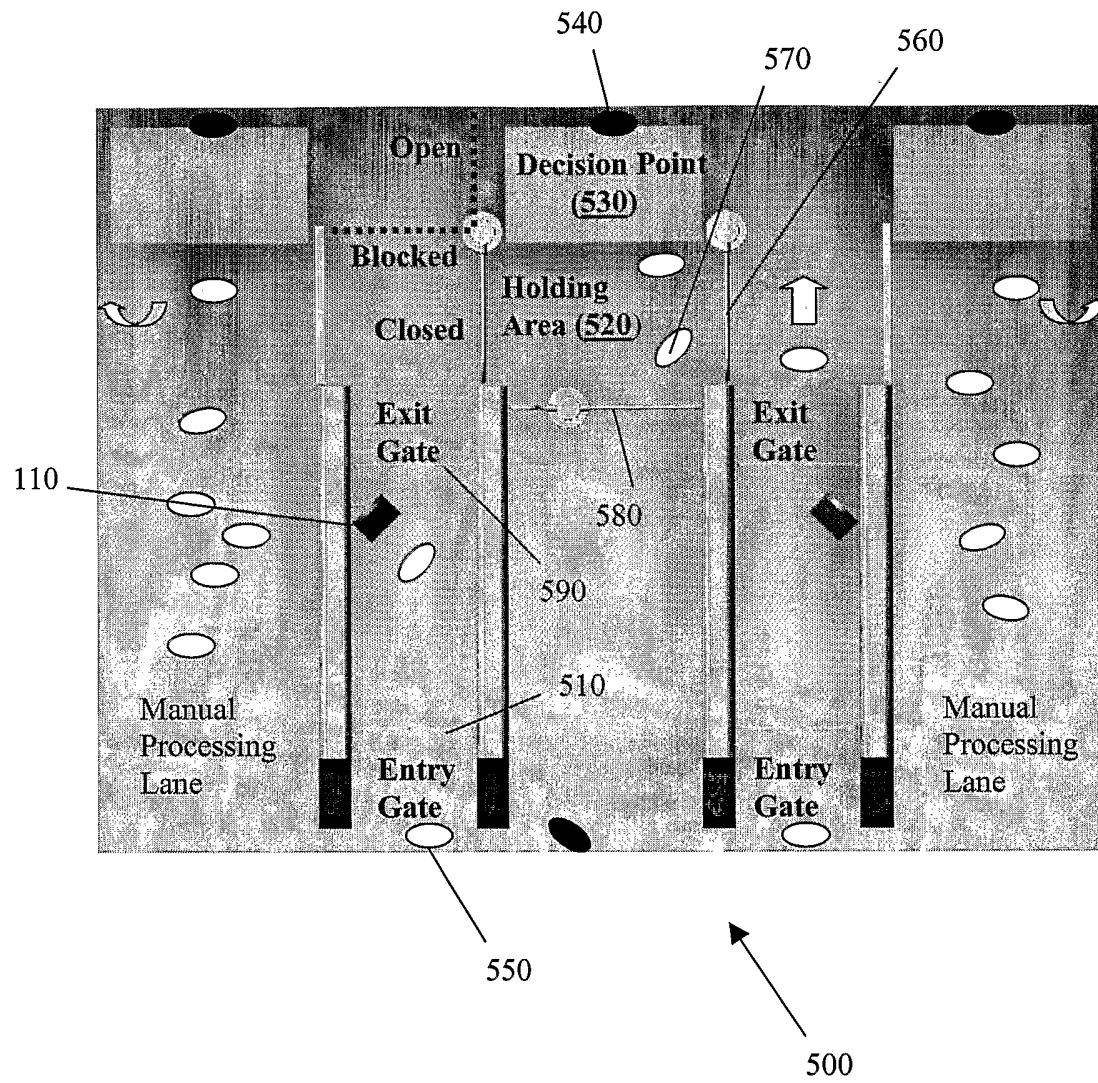
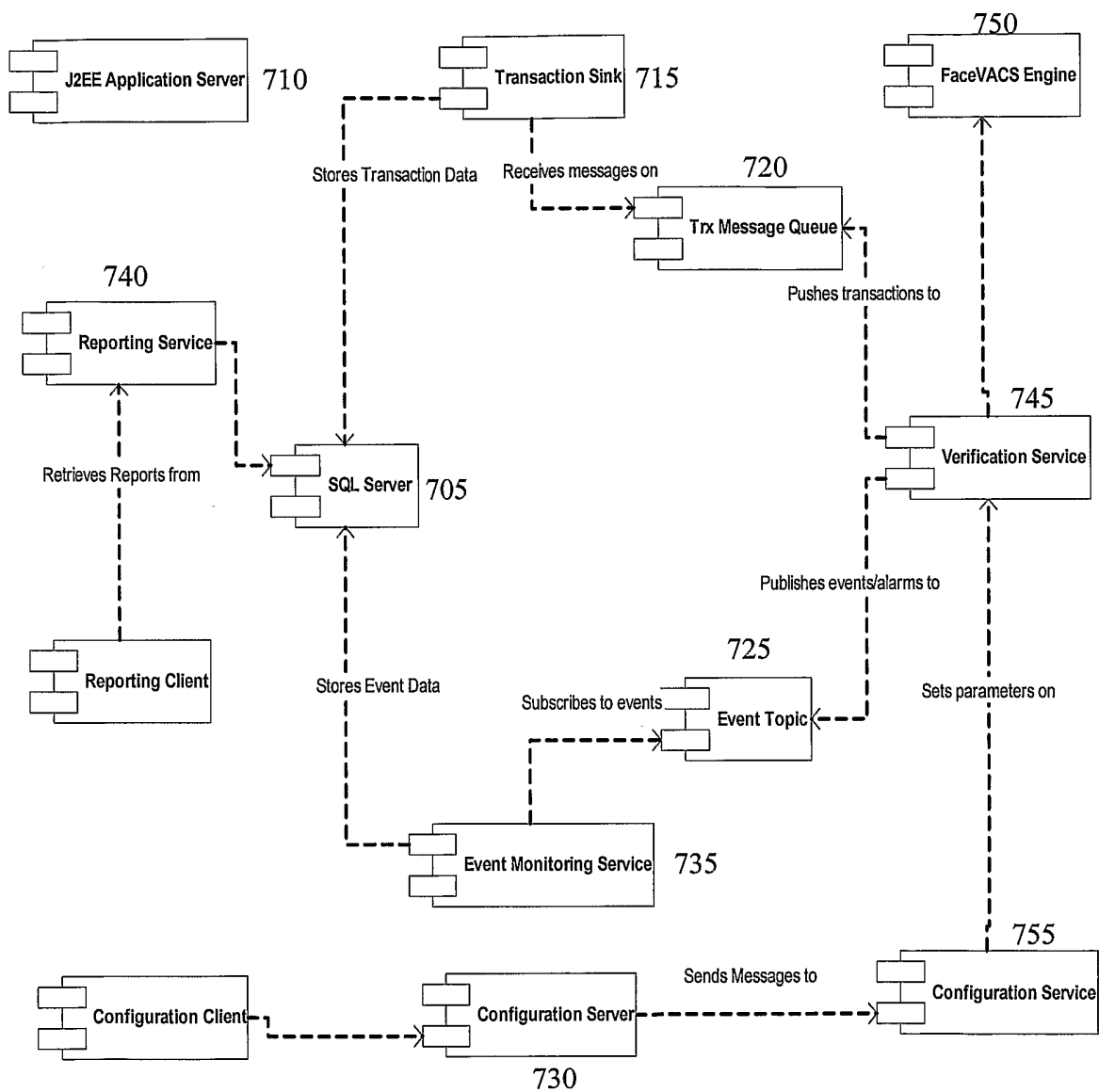


FIGURE 7



-7/11-

FIGURE 8

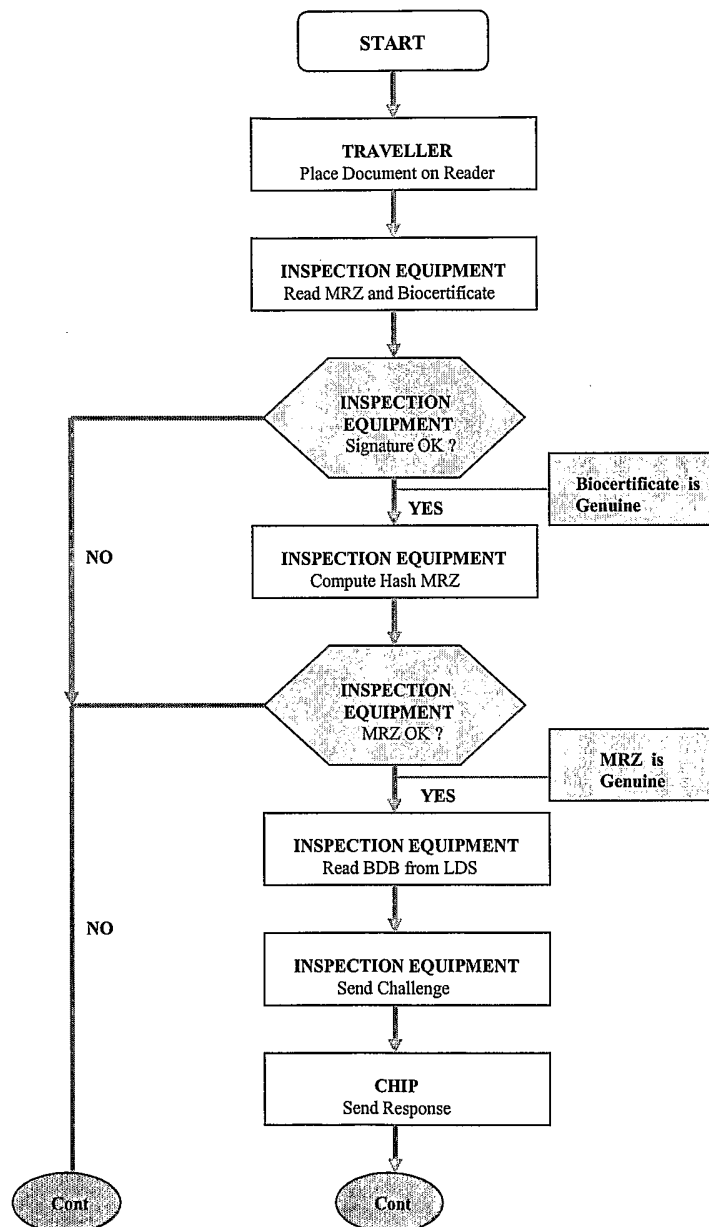


FIGURE 9

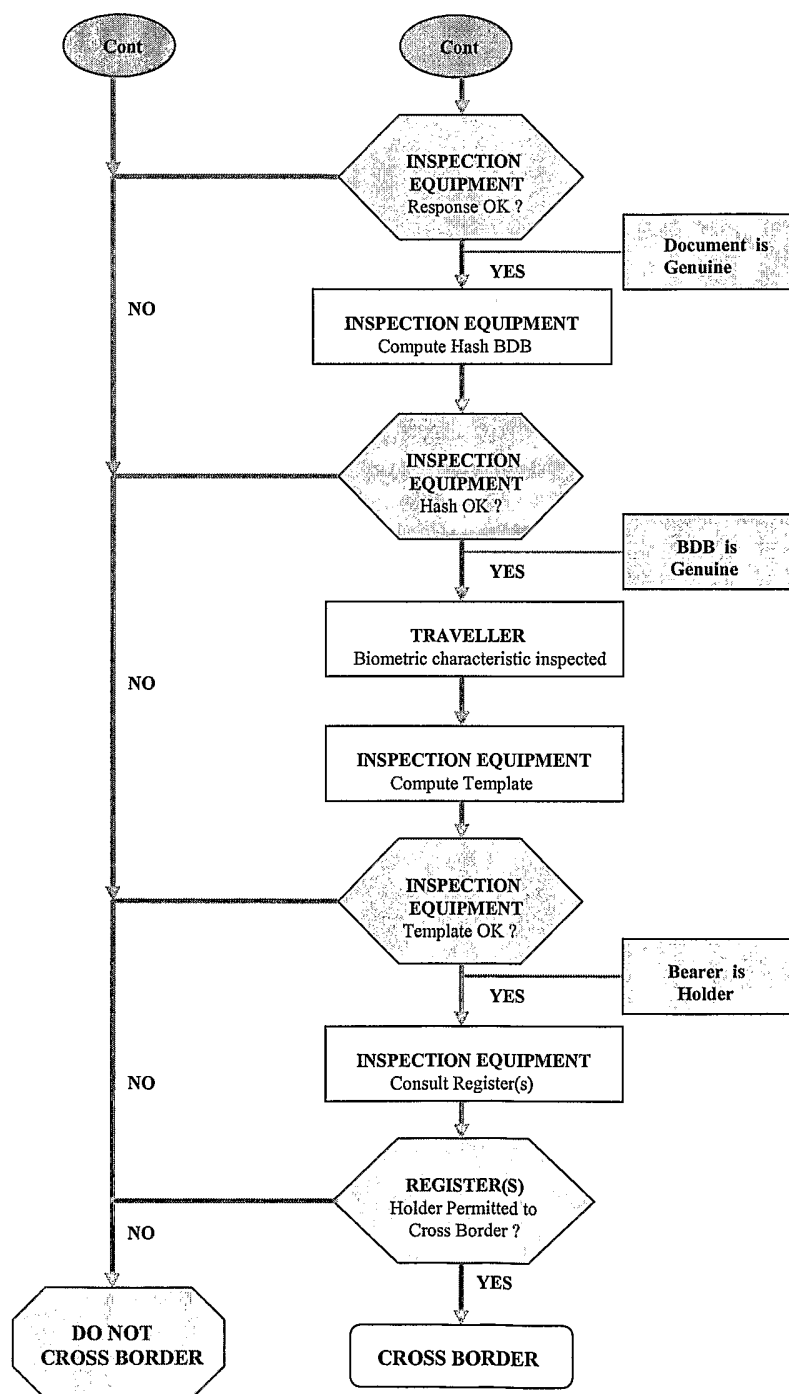
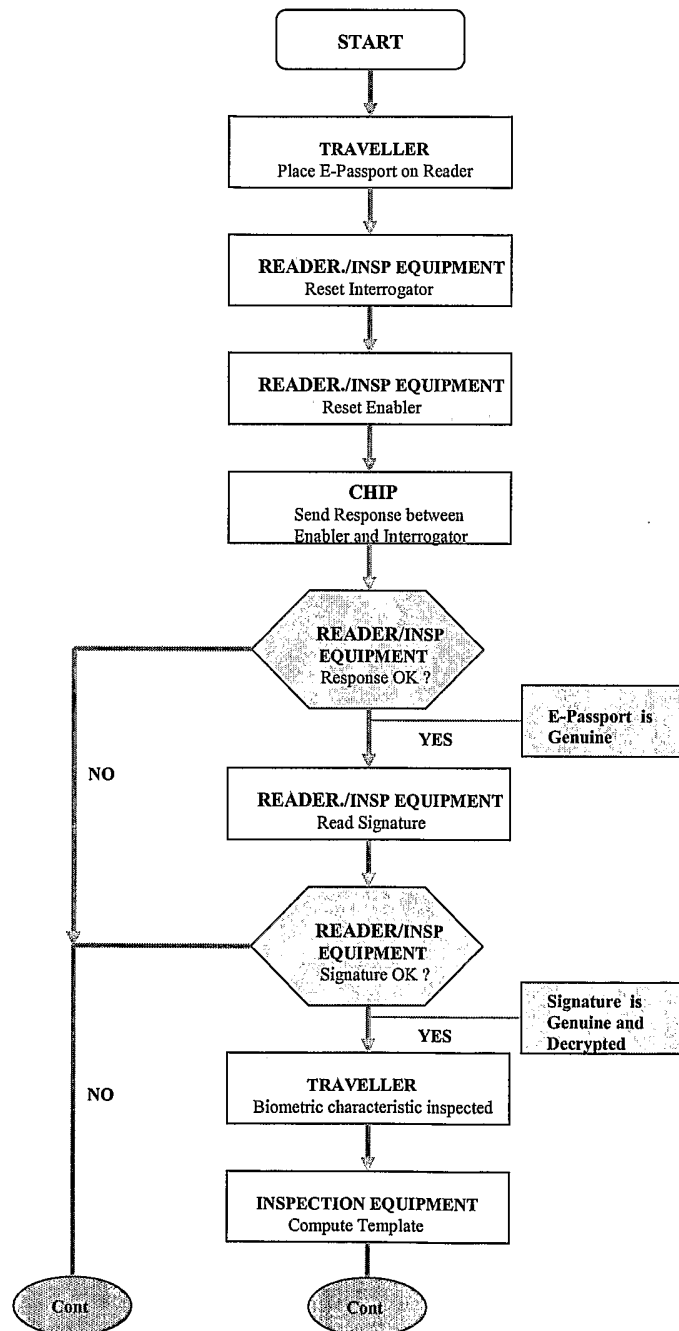


FIGURE 10



-10/11-

FIGURE 11

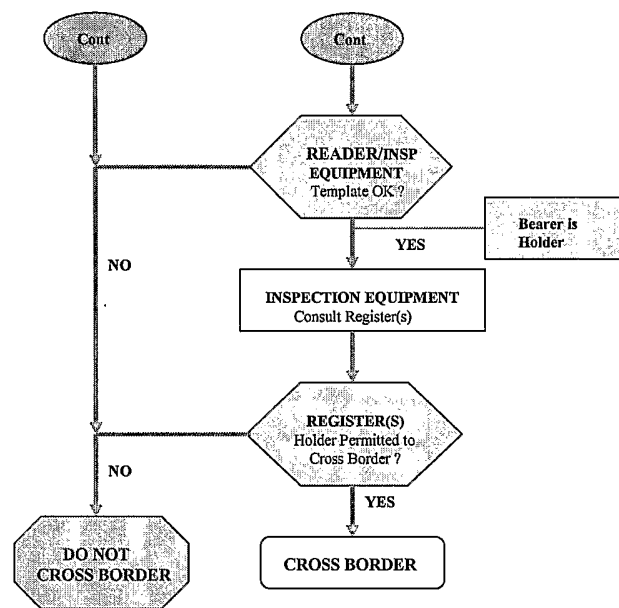
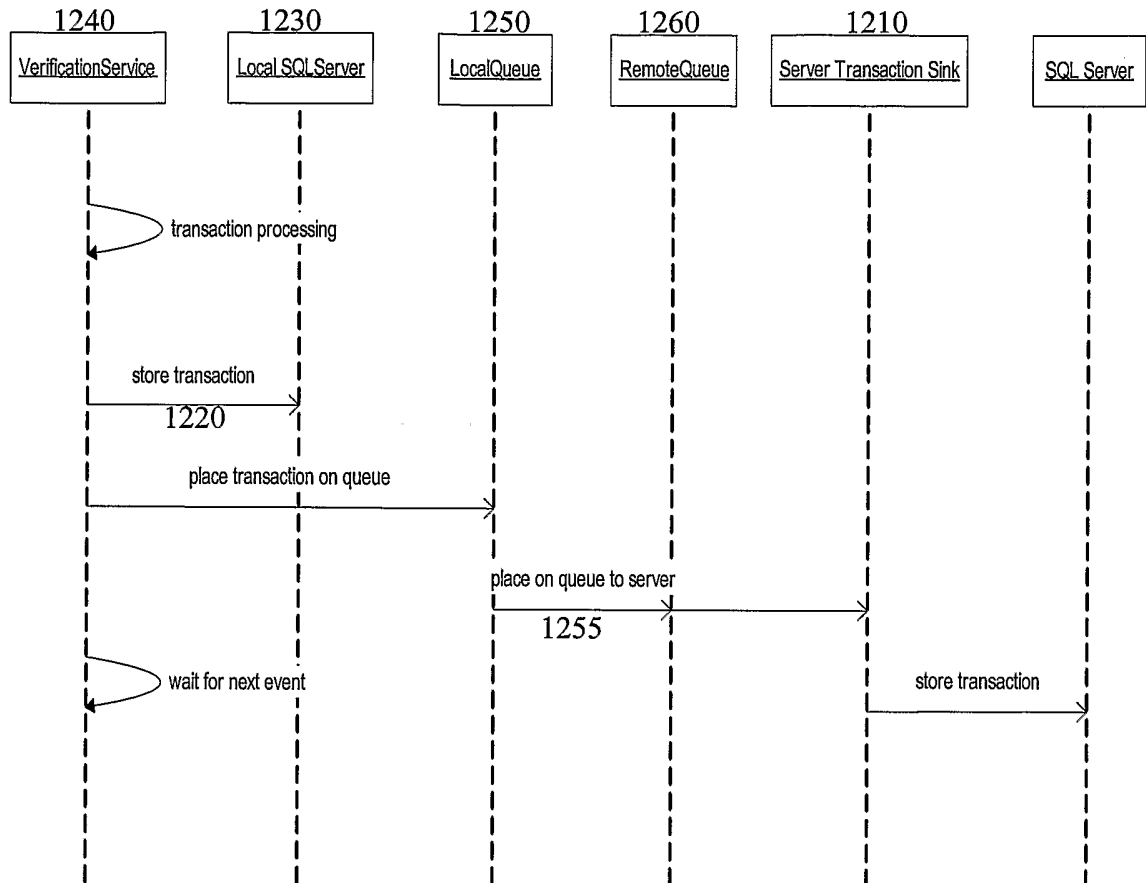


FIGURE 12



INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2004/001208

| | | | | | |
|--|--|---|--|--|--|
| A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. ⁷ : G07C 9/00, E06B 11/00 According to International Patent Classification (IPC) or to both national classification and IPC | | | | | |
| B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPPATENT; (G07C 9/00B6D/EC or G07C 9/00C2D/EC), (hold+, wait+, detention, isolation, exit+, depart+ leav+ etc) DWPI, JAPIO; (person, traveller, tourist, user etc), (passport, access+, entry immigration, G07C-009/IC, etc), (biometric, (face, facial, voice, iris etc)(w)(recognition, identification), (authori+, permit+, approv+, clear+ etc), (detention, close, hold+, wait+ etc), (exit+, leav+, pass, depart+ leav+ etc), (gate, barrier, turnstile, door etc), (zone, area, room etc) | | | | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | | | | |
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. | | | |
| X | US 2003/0133597 A1 (MOORE et al) 17 July 2003 See the abstract | 1-22 | | | |
| A | CA 2392264 A1 (ACCENTURE GMBH) 31 May 2001 See the abstract | | | | |
| P,A | US 2004/0064453 A1 (RUIZ et al) 1 April 2004 See the abstract | | | | |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex | | | | | |
| <table style="width: 100%; border: none;"> <tr> <td style="width: 33%; vertical-align: top;"> * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed </td> <td style="width: 33%; vertical-align: top;"> "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family </td> <td style="width: 33%;"></td> </tr> </table> | | | * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family | |
| * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family | | | | |
| Date of the actual completion of the international search 5 November 2004 | | Date of mailing of the international search report 10 NOV 2004 | | | |
| Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. (02) 6285 3929 | | Authorized officer I.A.BARRETT Telephone No : (02) 6283 2189 | | | |

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2004/001208

| C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|---|--|-----------------------|
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| A | US 6119096 A (MANN et al) 12 September 2000 See the abstract | |
| A | EP 1170705 A2 (KABUSHIKI KAISHA TOSHIBA) 9 January 2002 See the abstract | |
| A | Patent Abstracts of Japan, JP 2001-243515 A (NIPPON SIGNAL CO LTD) 7 September 2001 See the abstract | |
| A | Patent Abstracts of Japan, JP 11-185087 A (OKI ELECTRIC IND CO LTD) 9 July 1999 See the abstract | |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2004/001208

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

| Patent Document Cited in Search Report | | Patent Family Member | | | |
|---|------------|----------------------|----------|----|------------|
| US | 2003133597 | WO | 03063102 | | |
| CA | 2392264 | AU | 25025/01 | DE | 19961403 |
| | | WO | 0139133 | | EP 1102216 |
| US | 2004064453 | | | | |
| US | 6119096 | AU | 71231/98 | AU | 87633/98 |
| | | CA | 2302277 | EP | 1029298 |
| | | WO | 9906901 | WO | 9906928 |
| EP | 1170705 | CA | 2349933 | JP | 2002008070 |
| | | | | US | 2001054951 |
| JP | 2001243515 | | | | |
| JP | 11185087 | | | | |
| Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001. | | | | | |
| END OF ANNEX | | | | | |