



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
27.12.2017 Bulletin 2017/52

(51) Int Cl.:
G07C 9/00 (2006.01)

(21) Application number: **14187825.6**

(22) Date of filing: **06.10.2014**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(72) Inventors:
• **Koblitz, Uwe**
82008 Unterhaching (DE)
• **Ben David, Meir**
43588 Israel (IL)

(71) Applicant: **G2K Holding S.A.**
4362 Esch-sur-Alzette (LU)

(74) Representative: **Wall, Natalie**
Wall & Kollegen
Karlsplatz 7
80335 München (DE)

(54) **Method and system for performing security control at, respectively, a departure point and a destination point**

(57) The invention relates to a method for performing security control at a destination point, comprising the steps of:
- obtaining (S8, S9) biometric data associated with the passengers expected to arrive at the destination point;

- obtaining (S14) live biometric data from the passenger at the destination point;
- matching (S15) the downloaded biometric data and the live biometric data.

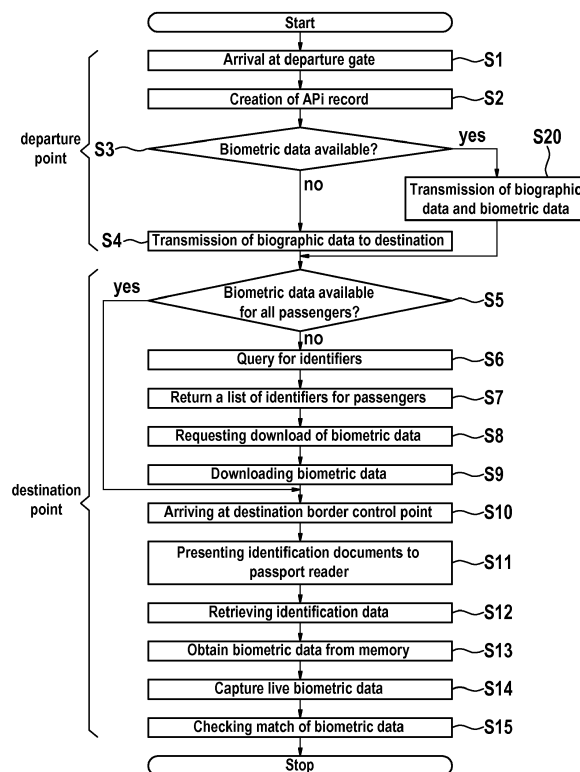


Fig. 2

Description

Technical field

[0001] The present invention relates to passenger control, particularly border-crossing checks of passengers at a destination point of a travel, particularly regarding air travel.

[0002] Part of the work leading to this invention has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° [312797].

Background of the invention

[0003] During air travel, passengers have to go through multiple checkpoints which are operated by the transportation company, the departure and destination facilities and/or governmental authorities. At the point of departure for air travel, for example, passengers will go to the check-in area first, they may then pass through passport control, and then they will finally proceed to the boarding area at which point the aircraft can be boarded. After they have reached their destination, the passengers have to pass through immigration, border control and customs.

[0004] Control requirements, particularly on the side of immigration, have risen in the last few years so that the effort required to check and verify the credentials of each traveler has increased greatly. On the other hand, the staffing and financial resources of governmental authorities, transportation companies and facility operators remain limited.

[0005] Document US 2008/0010464 A1 discloses an apparatus comprising a transit gate, a card-reading device configured to read identification data from an identification card to allow the transit gate to open, a biometry reading device located within a walk-through passage of the transit gate to obtain biometric data directly from the passing individual, and a server configured to compare the biometric data to biometric data read from the identification card by the card-reading device, and to compare the identity obtained from the identification card to a list of identities.

[0006] From document US 7,515,055 B2, a method and system for airport security is known wherein a security ID card carried by a person stores biometric information identifying the particular individual and is capable of communicating the biometric information to an external station. An identification collection device located at a checkpoint is provided to which the person presents the current biometric identification information wherein the security ID card additionally contains an electric circuit capable of providing information regarding the location of the ID pass with respect to the checkpoint.

[0007] Document US 8,604,901 B2 discloses a method to ensure the provenance of passengers intending to depart on a vehicle from a transportation facility by providing biometric reading devices at both the check-in sta-

tion and the departure area station of the facility.

[0008] It is an object of the present invention to ease congestion and speed up passenger flow through security or other checkpoints while entering or leaving a country e.g. by any transportation means, such as an aircraft, ship, vehicle or the like.

Summary of the invention

[0009] This object has been achieved by the method for passenger control according to claim 1, the method for operating a checkpoint at a destination of passenger travel and a checkpoint apparatus according to the further independent claims.

[0010] Further embodiments are indicated in the depending subclaims.

[0011] According to a first aspect a method for performing security control at a destination point is provided, comprising the steps of:

- obtaining biometric data associated with the passengers expected to arrive at the destination point;
- obtaining live biometric data from the passenger at the destination point;
- matching the downloaded biometric data and the live biometric data.

[0012] Furthermore, for each passenger expected to arrive at the destination point, of which no biometric data is available, following steps are carried out:

- receiving a unique identifier associated to each individual passengers;
- downloading biometric data associated with the passengers' identifiers;

[0013] One idea of the above method is to provide information about passengers arriving at the destination point which has been collected at the departure point. Utilizing this information additional biometric data will be retrieved from a biometric data repository which can be located independent of/ remote from the destination point. So checking the identity of the passenger at the destination can be performed based on identification documents and biometric data.

[0014] It is proposed to actively transmit all necessary biographic data of the passengers provided at the departure point (Entry/exit point) for the travelling passengers expected to arrive at the destination point. The identifier is an anonymous unique reference to the passenger. The biographical data and the biometric data are both associated to one another but to the identifier. So the purpose of the identifier is, that the biographical data and the biometric data can be physically separated within the biometric data repository. The separation of biographical and biometric information is for enhancing data privacy protection.

[0015] The passengers' identifiers and further informa-

tion about the passengers may be received from a biometric data repository utilizing above biographic data for the query. The further information may refer to additional information about the traveller, what is also not known at the departure point. One example is a membership in a registered traveller programme of the destination region.

[0016] Furthermore, it is proposed to retrieve biometric data from a biometric data repository utilizing received passengers' identifiers for the query. This second query may involve a further database. Therefore at the time of arrival at the destination point, a full check of the arriving passengers can be carried out without waiting for biometric data to be retrieved from a remote location at the time of checking.

[0017] Moreover, depending on whether the collected biometric data matches, the passenger may be allowed to pass or they can be detained for further verification.

[0018] According to an embodiment the passengers' identifiers may be received from a biometric data repository according to a query based on passengers' biographic data.

[0019] It may be provided that the passengers' biographic data is provided at the departure point for the plurality of passengers.

[0020] Furthermore, the download/ data transfer of the biometric data may be immediately started after the query, or it may be scheduled to start so that all biometric data is fully downloaded at a time of arrival of the passengers at their destination. As usual, the collection of biometric and other identification data may add up to huge amounts of data which needs to be available and validated when checking the arriving passengers at their destination. So transmitting the necessary data at the time of departure of the passengers allows more time to complete a full check of their identities with respect to the security requirements, and the border control can be performed more thoroughly without reducing passenger flow through the check point at the destination.

[0021] According to an embodiment, depending on the passengers' identifier data received, at least one further database may be accessed. Additionally, further information about the passenger can be transmitted to the destination checkpoint prior to or during the arrival of the passengers at the destination point which allow the authorities to make a decision regarding each passenger's security clearance.

[0022] It may be provided that the live biometric data is obtained by means of a transit gate equipped with scanner for detecting biometric data.

[0023] The download from biometric data repository may be initiated by the destination point.

[0024] In alternative embodiment, the download may be initiated by the biometric data repository.

[0025] The download of the biometric data may include transmitting the biometric data of all passengers expected to arrive at the destination point. The passengers expected to arrive may be identified by a record generated or obtained at the departure point.

[0026] It may be provided that depending on the matching result the passenger is allowed to pass.

[0027] The identifiers may be received from a biometric data repository according to a query based on biographic data, wherein the biographic data is particularly obtained at a departure point of the passenger and transferred to the destination point of the passenger.

[0028] Furthermore, the biographic data may be provided at the destination point for the plurality of passengers scheduled to arrive at the destination point.

[0029] Depending on the received identifier at least one further database may be accessed.

[0030] Moreover, the live biometric data may be obtained by means of a transit gate equipped with a scanner for detecting biometric data.

[0031] According to a further aspect a method for performing security control at a departure point is disclosed, comprising the steps of:

- obtaining biographic data associated with the passenger's biographical and travel information;
- if access to prestored biometric data is made available by the passenger, obtaining the prestored biometric data;
- transferring biographic data to a destination point the passenger is scheduled to travel;
- if available, transferring biometric data of the passenger to a destination point the passenger is scheduled to travel.

[0032] According to a further aspect a system for performing security control at a destination point is provided, comprising:

- means for receiving identifiers associated with a plurality of passengers of travel;
- means for downloading biometric data associated with the passengers' identifiers;
- means for obtaining live biometric data from the passenger;
- means for matching the downloaded biometric data and the live biometric data.

[0033] According to a further aspect a system for performing security control at a departure point is provided, comprising:

- means for obtaining biographic data associated with the passenger's biographical and travel information;
- means for obtaining the prestored biometric data if access to prestored biometric data is made available by the passenger;
- means for transferring biographic data to a destination point the passenger is scheduled to travel;
- means for transferring biometric data of the passenger, if available, to a destination point the passenger is scheduled to travel.

Brief description of the drawings

[0034] Embodiments of the present invention are described in more detail in conjunction with the accompanying drawings, in which:

Figure 1 schematically shows the workflow for performing security control an airline passenger; and

Figure 2 shows a flowchart illustrating the method for performing the passenger checks during the time of travel of the passenger.

Description of embodiments

[0035] Figure 1 shows the arrangement 1 of stations a passenger must pass through during travel, such as air travel, in the following example. The flowchart of Figure 2 shows the steps to be carried out to achieve the workflow as shown in Figure 1.

[0036] In step S1, the passenger arrives the departure point at a departure gate 2. The departure gate 2 has a plurality of check-in counters 3 operating an electronic check-in system, where the passenger has to check-in/register for the flight. At the check-in counters 3 the passenger identifies him/herself by e.g. presenting an airline ticket and a government issued identification item, such as a passport, an identification card, an identification document or the like, as travel documents.

[0037] At the check-in, in step S2, the passenger further provides information for filling out an advance passenger information (API) record. The API system is known as an electronic data interchange system established to transfer biographic and travel-related data of a traveler to certain destinations as a prerequisite for entry at the departure point and for exit at a destination point. The API record hence contains specific biographical and travel information and referred herein as biographic data. Entering data into the API record might be done semi-automatically based on a passenger name record (PNR). The passenger name record may be provided as a record in the database of a computer reservation system in the travel industry that contains the itinerary for a passenger or a group of passengers travelling together. This record may be transmitted to the check-in system 31 operated at check-in counter 3.

[0038] In step S3 it is checked whether the passenger can additionally provide biometric data of him/herself stored in an individual biometric data source 8. The individual biometric data source 8 may be an electronic device, such as a mobile phone, a PDA, electronic passport, a token or the like carried by the passenger. Furthermore the individual biometric data source 8 may be an external database which can be accessed from the check-in counter 3 under assistance of the passenger checking-in. Biometric data retrieved from the individual biometric data source 8 is reliably stored and associated to the biograph-

ic data of the passenger. The biometric data may be preferably encrypted and can be made available to the check-in counter 3 under assistance of the passenger, e.g. by providing a password.

[0039] If it is found in step S3 that the passenger cannot provide biometric data (alternative: no), the process is continued with step S4. Otherwise (alternative: yes) the process is continued with step S20.

[0040] In step S4, the API records of checked-in passengers are collected by an electronic data system 4 connected to the check-in system 31 and forwarded therefrom as biographic data to a destination security control point 5. While the check-in counters 3 are operated by airlines, the electronic data system 4 may be operated by a transportation company, border police, airport facility or the like.

[0041] The electronic data system 4 is connected to the destination security control point 5 via a data communication path 7, e.g. internet-based or packet-based data connection, which allows to electronically transmit biographic data from the departure point to the destination point.

[0042] The destination security control point 5 includes an electronic security control system 51 including a memory 52. The transfer of the biographic data (consisting of or including API records) to the electronic security control system 51 may be initiated by push technology, i.e. the transfer of the biographic data is initiated by the electronic data system 4. For example time and kind of transfer of biographic data may be determined by the electronic data system 4.

[0043] In step S5 it is checked whether for the transferred biographic data for the passengers expected to arrive at the point of destination also the biometric data are available or have been received (transmitted via step S20). If it is found that for all respective passengers the biometric data are already available at the point of destination (alternative: yes) the method is continued with step S10. Otherwise (alternative: no) the process is continued with step S6.

[0044] In step S6, the passengers for which the biometric data is not available yet, identifiers need to be firstly obtained. As the identifiers are not known at the departure point, the biographic data of those passengers is used by the electronic security control system 51 to query a central biometric data repository 6 to obtain respective identifiers that match the biographical and travel information included in the biographic data.

[0045] In step S7, the central biometric data repository 6 returns a list of the identifiers that match the biographic data to the destination security control point 5 in response to the query. The identifiers provide identification information, e.g. a unique identification number associated to each individual, and may serve to retrieve biometric data associated with the passenger identified by the biographic data.

[0046] The identifiers correspond to anonymous unique references to the individual passengers. The pur-

pose of the identifiers is, that the biographical and travel information and the biometric data can be physically separated within the biometric data repository. The separation of biographical and biometric information is done to enhance data privacy protection.

[0047] In general, biometric data may be obtained by a face image scan, a fingerprint scan, a retinal scan of the eye, a hand scan, a palmprint, a finger length scan or any other unique identification means including DNA, voice or other means for positive identification.

[0048] Depending on the result of checking of step S3, in step S20, the API records of checked-in passengers are collected by the electronic data system 4 connected to the check-in system 31 together with the biometric data provided by the individual biometric data source 8 of the passenger and forwarded therefrom as biographic data and biometric data to the destination security control point 5. The process is then continued with step S11.

[0049] In step S8, the destination security control point 5, particularly the destination security control system 51, requests biometric data from the central biometric data repository 6 depending on the list of identifiers based on the API record, for each passenger which has not presented or could not present access to the individual biometric data source 8 at the departure point. The missing biometric data is downloaded in step S9 and cached locally in a memory 51 of the security control point 5 together with the biometric data received together with the biographic data in step S20.

[0050] In step S9, the biometric data is downloaded and stored in the memory 52 of the destination security control point 5.

[0051] Based on the identifiers and/or biographic data, additional databases such as a criminal database, law enforcement database, visa database or the like can also be queried so that corresponding data can be merged and evaluated along with the biometric data.

[0052] The download of the biometric data of the travelling passengers may be performed while the passengers are in-flight (or otherwise in transit from departure point to destination point) so that at the time of arrival the biometric data is fully downloaded and available in the memory 52. The download has to be started ahead of time as the huge data volume of biometric data of travelling passengers can place a significant load on the data communication path 7.

[0053] The biometric data allow authorities to perform a full check of the identity of the arriving passengers at the destination security control point 5. The biometric data associated with identification information of the passenger is readily available in the memory 52 and there is no longer a need to start retrieving such biometric data via a possibly heavily loaded data network at the time the passenger identifies him/herself at the destination security control point 5.

[0054] Thus, the data collected at the departure point can be immediately matched with biometric data captured at the destination security control point 5 at the time

each passenger is passing through.

[0055] In an alternative embodiment, the biographic data (API record) can be firstly transmitted to the central biometric data repository 6 including the information about the destination point. The transfer of the biometric data which is associated to the individual identified by the biographic data may then be initiated by the central biometric data repository 6 by means of push technology. Consequently, the destination security control point 5 may obtain all necessary data of the passengers expecting to arrive for performing a security check at the destination point without any further external database request.

[0056] In step S10, the passenger arrives at the destination security control point 5.

[0057] In step S11, the passenger presents the travel documents, particularly the identification item such as an electronic machine readable travel document (e-MRTD), an electronic device, such as a smartphone etc., having stored therein the passenger's identification information to an electronic identification item reader 53 of the destination security control point 5. The electronic identification item reader 53 is capable of electronically reading the identification items, and it provides the identification information to the security control system 51.

[0058] The identification item may further correspond to an ID card, a driver's license, a passport, e-MRTD, Visa, RT token or the like. The e-MRTD corresponds to an electronic machine-readable travel document which complies with ICAO's doc 9303 specifications (or any other authorized specifications) and which can be read by machines in automated border control stations and can be used by travellers internationally. The RT token (RT: Registered traveller) may correspond to a physical device by which the person who carries the RT token can identify themselves.

[0059] In step S12, the identification document is read out and corresponding identification data is provided to the security control system 51. The identification information may include a passport number of the identification document, visa number and/or an identifier assigned to a third country national (TCN). For example such an identifier of the TCN may be created from the data of a TCN passport using a hash technology. A third-country national (TCN) is any person who is not a citizen of the region/country of destination. The region of destination may be formed by multiple countries, such as the Schengen area. At the security control point 5 it is verified whether the data read out from the identification item matches with the identifier provided in step S5.

[0060] The security control system 51 obtains in step S13 the biometric data from the passenger's e-MRTD and from the memory 52 based on the identification data of the identification document.

[0061] The security control point 5 may comprise an e-gate 54 (transit gate) which is commonly known in the art and which is configured to capture live biometric data of the passenger as they pass through. Particularly, the

e-gate 54 can be equipped with at least one of a fingerprint scanner, a retinal scanner, a DNA scanner, a hand scanner, a palmprint scanner, a finger length scanner, voice verification scanner or any other means allowing positive identification of an individual. The e-gate can be further equipped with a camera to support face recognition. Furthermore, the e-gate is configured to allow or to disallow a passenger to pass through.

[0062] The live biometric data is obtained in step S14 and provided to the destination security control system 51.

[0063] In step S15 it is checked whether or not the live biometric data corresponds to the biometric data downloaded from the biometric data repository 6 and associated to the identification information obtained from the electronic identification item reader 53.

[0064] If the live biometric data matches the retrieved biometric data the passenger could be successfully identified and the passenger is allowed to pass the e-gate. Otherwise authorities may be alerted.

Claims

1. Method for performing security control at a destination point, comprising the steps of:

- obtaining (S8, S9) biometric data associated with the passengers expected to arrive at the destination point;
- obtaining (S14) live biometric data from the passenger at the destination point;
- matching (S15) the downloaded biometric data and the live biometric data.

2. Method according to claim 1, wherein for each passenger expected to arrive at the destination point, of which no biometric data is available, following steps are performed:

- receiving (S7) a unique identifier associated to each individual passengers;
- downloading (S9) biometric data associated with the passengers' identifiers;

3. Method according to claim 2, wherein the downloading is immediately started after the query or is scheduled to start so that all biometric data is fully downloaded at a time of arrival of the passengers at the point of destination.

4. Method according to any of the claims 2 to 3, wherein the download is initiated from the destination point.

5. Method according to any of the claims 2 to 3, wherein the download is initiated by a biometric data repository (6).

6. Method according to any of the claims 2 to 5, wherein the download of the biometric data includes transferring the biometric data of all passengers expected to arrive at the point of destination.

7. Method according to any of the claims 1 to 6, wherein depending on the matching result the passenger is allowed to pass.

8. Method according to any of the claims 1 to 7, wherein the identifiers are received (S7) from a biometric data repository according to a query based on biographic data, wherein the biographic data is particularly obtained at a departure point of the passenger and transferred to the destination point of the passenger.

9. Method according to claim 8, wherein the biographic data is provided at the destination point for the plurality of passengers scheduled to arrive at the destination point.

10. Method according to any of the claims 1 to 9, wherein depending on the received identifier at least one further database is accessed.

11. Method according to any of the claims 1 to 9, wherein the live biometric data is obtained by means of a transit gate (54) equipped with a scanner for detecting biometric data.

12. Method for performing security control at a departure point, comprising the steps of:

- obtaining biographic data associated with the passenger's biographical and travel information;
- if access to prestored biometric data is made available by the passenger, obtaining the prestored biometric data;
- transferring (S4, S20) biographic data to a destination point the passenger is scheduled to travel;
- if available, transferring (S20) biometric data of the passenger to a destination point the passenger is scheduled to travel.

13. System for performing security control at a destination point, comprising:

- means for receiving identifiers associated with a plurality of passengers of travel;
- means for downloading biometric data associated with the passengers' identifiers;
- means (54) for obtaining live biometric data from the passenger;
- means (51) for matching the downloaded biometric data and the live biometric data.

14. System for performing security control at a departure point, comprising:

- means for obtaining biographic data associated with the passenger's biographical and travel information; 5
- means for obtaining the prestored biometric data if access to prestored biometric data is made available by the passenger;
- means for transferring biographic data to a destination point the passenger is scheduled to travel; 10
- means for transferring biometric data of the passenger, if available, to a destination point the passenger is scheduled to travel. 15

20

25

30

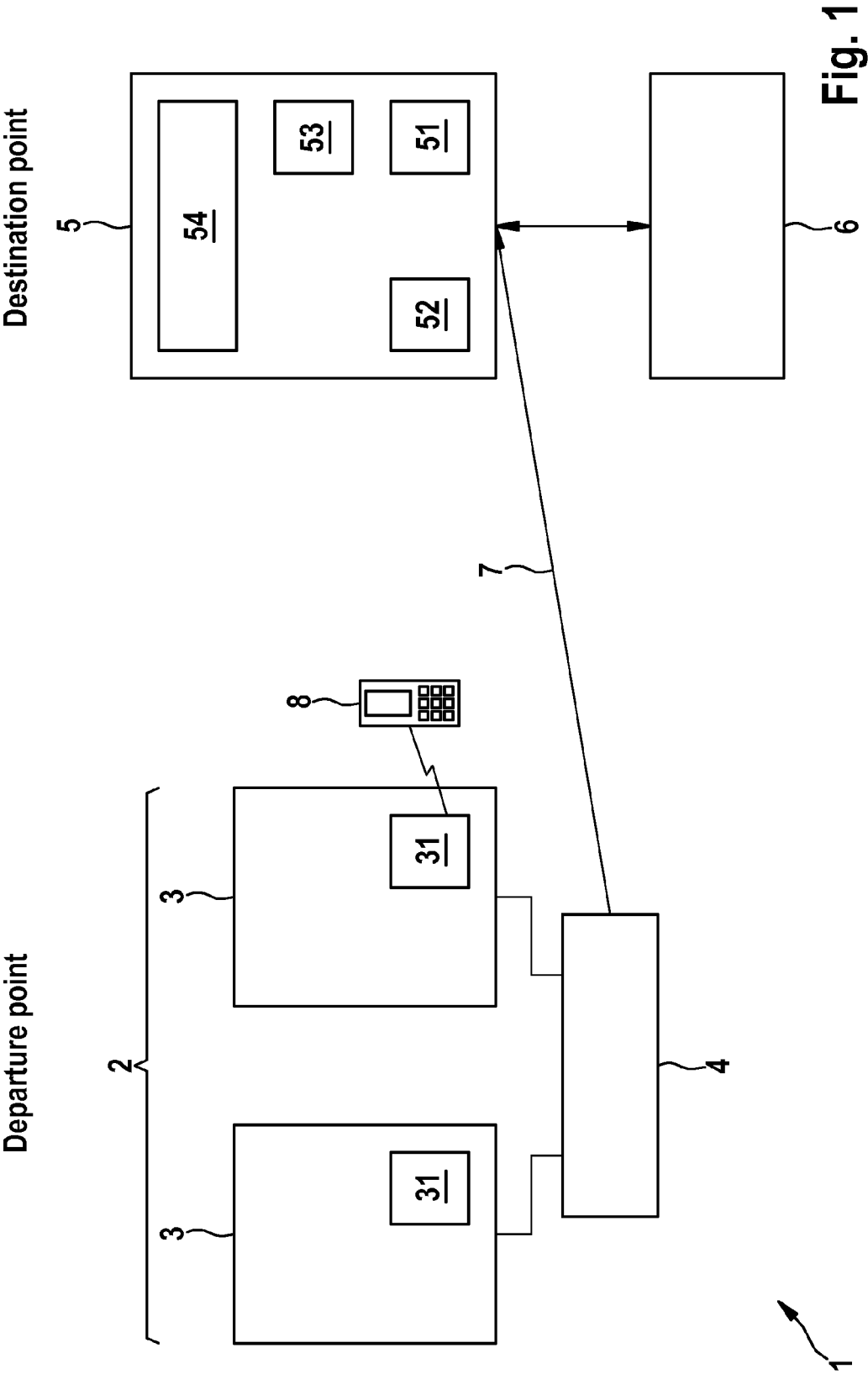
35

40

45

50

55



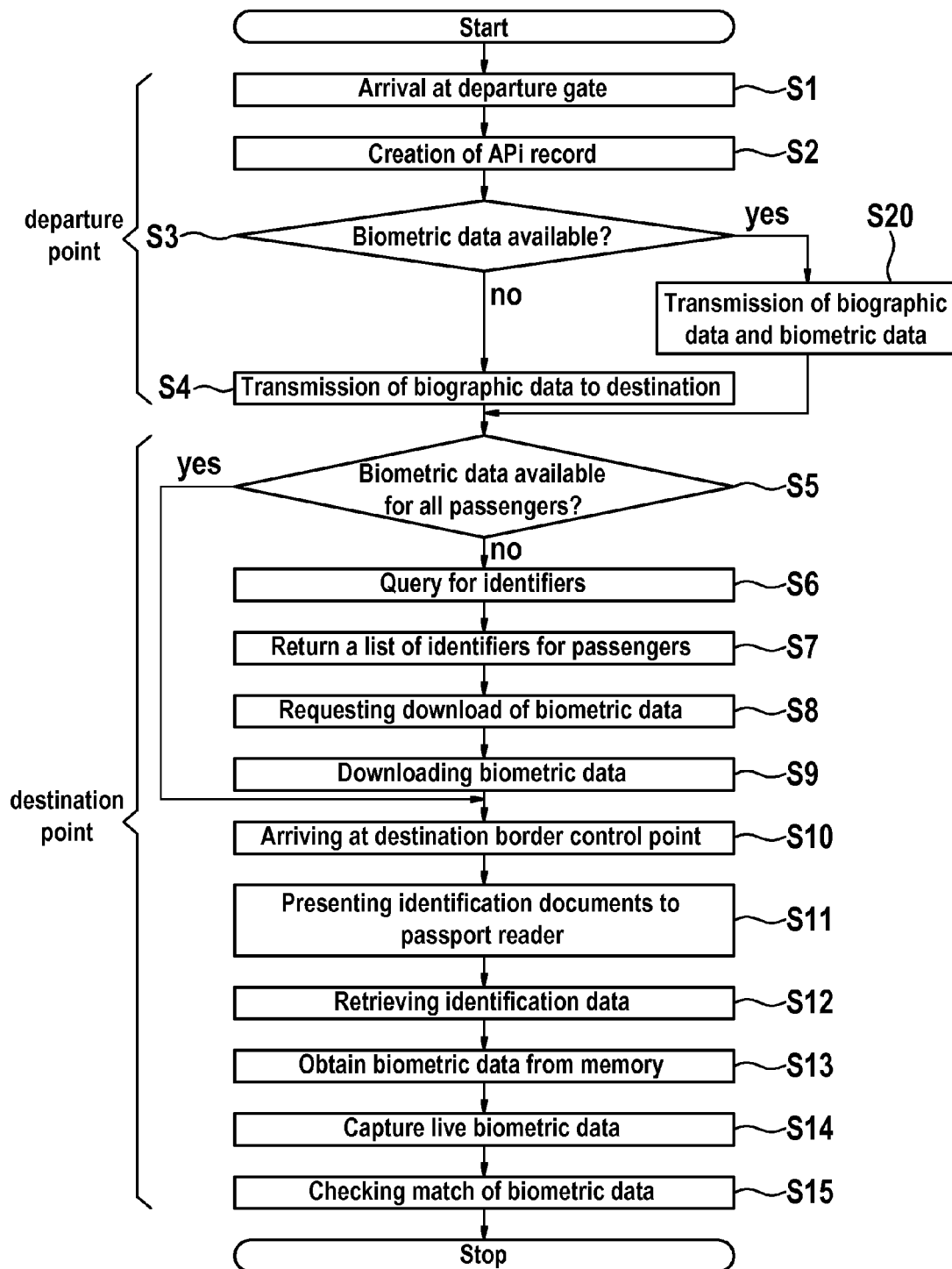


Fig. 2



EUROPEAN SEARCH REPORT

Application Number
EP 14 18 7825

5

10

15

20

25

30

35

40

45

50

55

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 1 318 482 A2 (HITACHI LTD [JP]) 11 June 2003 (2003-06-11) * column 1, line 7 - line 14 * * column 6, line 37 - column 7, line 4 * * column 8, line 43 - column 18, line 13 * * figures *	1-14	INV. G07C9/00
X	----- WO 2005/027023 A1 (STRATECH SYSTEMS LTD [SG]; CHEW DAVID KHIEN MEOW [SG]) 24 March 2005 (2005-03-24) * page 2, line 3 - page 4, line 32 * * page 5, line 28 - page 8, line 30 * * figures 1,2 *	1-14	
X	----- WO 2004/114074 A2 (UNISYS CORP [US]) 29 December 2004 (2004-12-29) * page 4, line 16 - page 8, line 4 * * page 11, line 2 - page 17, line 12 * * page 23, line 5 - page 33, line 15 * * figures 1,3-6 *	1-14	
	-----		TECHNICAL FIELDS SEARCHED (IPC)
			G07C
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 3 March 2015	Examiner Van der Haegen, D
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03/82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 14 18 7825

5 This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

03-03-2015

10

15

20

25

30

35

40

45

50

55

ORM P0459

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1318482 A2	11-06-2003	CN 1426015 A	25-06-2003
		EP 1318482 A2	11-06-2003
		JP 3938303 B2	27-06-2007
		JP 2003178346 A	27-06-2003
		KR 20030047796 A	18-06-2003
		KR 20050102598 A	26-10-2005
		TW 1282516 B	11-06-2007
		US 2003107472 A1	12-06-2003

WO 2005027023 A1	24-03-2005	EP 1683070 A1	26-07-2006
		JP 4937743 B2	23-05-2012
		JP 2007506159 A	15-03-2007
		MY 140501 A	31-12-2009
		TW 1409705 B	21-09-2013
		US 2006055512 A1	16-03-2006
		WO 2005027023 A1	24-03-2005

WO 2004114074 A2	29-12-2004	AU 2004250643 A1	29-12-2004
		CA 2529398 A1	29-12-2004
		EP 1639736 A2	29-03-2006
		US 2004078335 A1	22-04-2004
		WO 2004114074 A2	29-12-2004

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20080010464 A1 [0005]
- US 7515055 B2 [0006]
- US 8604901 B2 [0007]