(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2014 (13.11.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/182157 Al

(51) International Patent Classification:
G06Q 10/02 (2012.01)

(21) International Application Number:
PCT/MY20 14/000085

(22) International Filing Date:
29 April 2014 (29.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2013001695 9 May 2013 (09.05.2013) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(72) Inventors: **BIN MUBARAK, Mohd, Faizal;** c/o Mimos Berhad, Technology Park Malaysia, Bukit Mil, 57000 Kuala Lumpur (MY). **BIN PARMAN, Mohd, Azuddin;** c/o Mimos Berhad, Technology Park Malaysia, Bukit Mil, 57000 Kuala Lumpur (MY). **BIN AB MANAN, Jamalul-Lail;** c/o Mimos Berhad, Technology Park Malaysia, Bukit Mil, 57000 Kuala Lumpur (MY).

(74) Agent: **HEMINGWAY, Christopher, Paul;** Marks & Clerk (Malaysia) Sdn Bhd, Lot 5B Level 5, Tower 2 Etiqa Twins, 11 Man Pinang, 50450 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

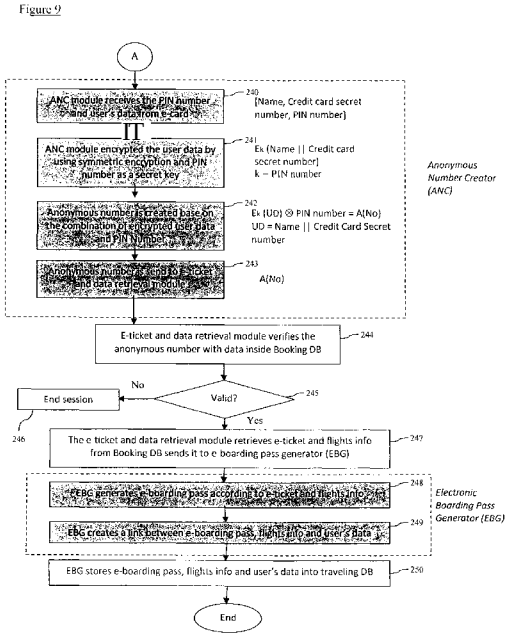
Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: ELECTRONIC TICKET BOOKING WITH IMPROVED PRIVACY

Figure 9



(57) Abstract: A method of booking a ticket comprising the steps of accessing (220) a ticket provider's website to book a ticket, reading (210) a user's details from an electronic smartcard (13) when a ticket booking is requested, encrypting (219) the user's details with a personal identification number (107) as a secret key, generating (220) an anonymous number based on the encrypted user details and personal identification number (107), and associating (226) the anonymous number with the ticket booking such that the user's details are private with regard to the ticket provider.

WO 2014/182157 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

ELECTRONIC TICKET BOOKING WITH IMPROVED PRIVACY

Field of Invention

The invention relates to a method of booking tickets electronically.

Background

Electronic tickets (e-tickets) are widely used in the ticketing systems of transportation services such as airlines, buses and trains. Current e-ticket systems are not fully secure because anybody, including an unauthorized person, who has the e-ticket and user data could easily access the boarding pass from an electronic kiosk (e-kiosk).

Moreover, current e-ticket systems do not provide any privacy protection in that user's data with flight or travelling information is exposed to the system administrator and/or operator of the service provider. As such, sensitive personal information may be available to the system operator, increasing the risk of identity theft by unscrupulous individuals.

An aim of the invention is to improve the security of such systems with respect to privacy of personal information.

Summary of Invention

In an aspect of the invention, there is provided a method of booking a ticket comprising the steps of:

accessing a ticket provider's website to book a ticket;

reading a user's details from an electronic smartcard when a ticket booking is requested,

setting a personal identification number for the ticket booking;

generating an anonymous number and associating it with the ticket booking;

storing said anonymous number such that the user can obtain the ticket by reading the smartcard at a ticket retrieval station;

characterised in that the user's details are encrypted with said personal identification number as a secret key.

Thus the ticket provider cannot view the user's private data as only the anonymous number is visible thereto, and only the user knows the personal identification number to allow the user's details to be retrieved. Advantageously if the smartcard was lost or stolen, or other details of the booking were obtained by a third party, the ticket would not be retrievable as the personal identification number would not be known to the third party.

In one embodiment the smartcard includes a physically unclonable function. Typically the smartcard is validated via a challenge-response session.

In one embodiment the personal identification number is stored on the smartcard. Typically the personal identification number is used in the challenge-response session.

Thus the smartcard validation and booking processes can use a common authentication procedure i.e. the same personal identification number, which has the advantage of being more user-friendly.

In one embodiment the ticket booking process proceeds if a user's details and payment are verified by a financial firm.

In one embodiment the anonymous number is generated based on the encrypted user's details and personal identification number.

In one embodiment a user obtains the ticket by using their smartcard and personal identification number at a ticket retrieval station. Typically the ticket retrieval station generates the anonymous number based on the encrypted user's details and personal identification number, and retrieves the details of the ticket booking.

Advantageously the personal identification number is required to book and retrieve the ticket, increasing security compared to systems where a user's input is only required for one of these actions.

In one embodiment the booking is for a travel ticket. Typically the travel ticket is a flight ticket.

In one embodiment the ticket retrieval station is capable of creating and/or printing a boarding pass. Typically the boarding pass is electronic and stored in a travelling database.

In a further aspect of the invention, there is provided a system for booking a ticket comprising:

a ticket provider's website configured for allowing a user to book a ticket;

a card reader for reading a user's details from an electronic smartcard when a ticket booking is requested;

input means for setting a personal identification number;

processing means for generating an anonymous number based on said user's details and associating the anonymous number with the ticket booking

storage means for storing said anonymous number; and

a ticket retrieval station for reading the smartcard and generating the anonymous number such that the user can obtain the ticket;

characterised in that the user's details are encrypted with said personal identification number as a secret key.

Brief Description of Drawings

It will be convenient to further describe the present invention with respect to the accompanying drawings that illustrate possible arrangements of the invention. Other arrangements of the invention are possible, and consequently the particularity of the accompanying drawings is not to be understood as superseding the generality of the preceding description of the invention.

Figure 1 is a schematic overview of the apparatus used to book a ticket in accordance with an embodiment of the invention.

Figure 2 is a schematic overview of the apparatus used to retrieve a ticket in accordance with an embodiment of the invention.

Figure 3 is a diagram of the system used to book a ticket in accordance with an embodiment of the invention.

Figure 4 is a diagram of the system used to retrieve a ticket in accordance with an embodiment of the invention.

Figures 5-6 illustrate the method used to book a ticket in accordance with an embodiment of the invention.

Figures 7-9 illustrate the method used to retrieve a ticket in accordance with an embodiment of the invention.

Detailed Description

With reference to Figure 1, there is illustrated a schematic view of the apparatus used to book a ticket in accordance with an embodiment of the invention

A user accesses the website of a service provider such as an airline for booking an electronic ticket such as a flight by using a computer 10 or other platform. The website requests that the user selects which method should be used for the booking i.e. normal or electronic smartcard 13. For extra security the smartcard 13 is provided with a Physical Unclonable Function (PUF) 14 which requires a challenge-response for authentication. User's data is stored in the smartcard.

A card reader device 12 embedded with a PUF reader 11 can interact with the smartcard 13 and PUF 14 for authentication thereof. The airline website of also requests a personal identification **number** (PIN) from the user as another security features.

A privacy engine in the user's computer produces an anonymous number based on the combination of encrypted user's data and PIN number. This anonymous number is used to link to the electronic ticket at the booking phase, and stored inside a booking database, thereby protecting the privacy of the user's data.

With regard to Figure 2, there is illustrated a schematic view of the apparatus used to retrieve a ticket in the form of an e-kiosk 16. The e-kiosk 16 generates an electronic boarding pass according to the anonymous number and travelling information inside the booking database.

The e-kiosk 16 requests that the user selects which method should be used for the booking retrieval i.e. normal or electronic smartcard. A user can therefore insert their smartcard 13 in the card reader device 15' equipped with PUF reader 11'. The smartcard 13 is authenticated as before and the user then inserts their PIN so that the anonymous number can be recreated based on the combination of encrypted user's data and PIN number. The anonymous number is used to retrieve the electronic ticket and the electronic boarding pass is generated and stored with the user information inside a travelling database.

With further reference to Figures 3-9 the system used to book and retrieves a ticket is illustrated.

A customer accesses 200 the ticket provider's website to buy a transportation ticket such as a flight ticket through a secured channel such as https. After the user has accessed the ticket provider's webpage, the web client module 109 inside the customer's computer is connected with the web server module 104 at the ticket provider's application server.

After the user selects 201 to buy and book e-ticket by using a smartcard (also referred to as e-card) as a method of transaction or payment 202, the system requests input 203 from the e-card to verify 205 the user. If there is no e-card the system reverts 204 to the normal method. The e-card stores the user's details in a memory 113.

The customer puts 206 the e-card with an embedded physically unclonable function 114 into a card reader with PUF reader 110 capability. The PUF reader 110 transmits 112 a signal to start 207 a challenge-response session between PUF device 114 in the e-card 210. If the e-card is found 208 to be valid, the card reader reads the user's data in the e-card 210 and transmits 111 the same to the user's computer. If not the session is ended 209.

A secured **financial** firm **'s** website 102 **is** then **provided** for payment 211. The financial firm's website receives and validates 212 user's data for e-ticket payment

from the e-card. If the data is found 213 to be valid, the financial firm's website proceeds with the e-ticket booking process 215. If not the session is ended 214. The ticket provider's website requests 216 the user to set and insert 217 a PIN number 107 for another element of security.

An anonymous number creator (ANC) website plugin 108 receives 218 the PIN number from user input and user's data from the e-card. The ANC module encrypts 219 the user's data 106 by using symmetric encryption with the PIN number 107 as the secret key. The anonymous number is created 220 based on the combination of encrypted user's data and PIN number 107.

The anonymous number is then sent 221 to the web server module. The web server module 104 receives 222 the anonymous number and invokes 223 the e-ticket retrieval module 105 to retrieve 224 the e-ticket from a ticketing database 100. The webserver module 104 provides 225 e-ticket, flight information and anonymous number to the e-ticket and anonymous number linker (EAL) module 103.

The EAL module 103 creates 226 a link between the anonymous number and the e-ticket. The linking data between anonymous number and e-ticket, and flight information are stored 227 in the booking database 101. The booking process ends after all the related information is stored inside booking database 101.

The next step starts after a customer goes 228 to the e-kiosk of the ticket provider to generate a boarding pass. The system inside the e-kiosk needs the customer to select 229 the transaction method i.e. normal electronic or e-card. If the user selects 230 e-card, the system requests 232 input from the e-card to verify the user, otherwise the system reverts 231 to the normal method. The customer then puts 233 the e-card with PUF 114 into a card reader with PUF reader 119 capability.

The PUF reader 119 starts 234 a challenge-response session with the PUF device 114 in the e-card. If the e-card is found 235 to be valid, the card reader reads 237 the user's data in the e-card and transmits 118 the same to the kiosk. If not the session is ended 236. The subscriber's e-kiosk then requests 238 the user to insert 239 the PIN number 122 which was previously set by the user at the booking phase.

The anonymous number creator (ANC) application 121 receives 240 the PIN number 122 from the user input and user's data from the e-card. The ANC module encrypts 241 user's data 120 by using symmetric encryption and it uses the PIN number as the secret key 241. The same anonymous number as before is created 242 based on the combination of encrypted user's data and PIN number.

The anonymous number is then sent 243 to the e-ticket and data retrieval module 124 to **retrieve** and verify 244 the anonymous number with flight information inside the booking database 101. If the anonymous number is found 245 to be valid, the e-ticket

and data retrieval module 124 retrieves 247 e-ticket and flight information from the booking database 101 and sends it to the electronic boarding pass generator (EBG) 123. If not the session is ended 246.

The EBG 123 generates 248 an e-boarding pass according to e-ticket, flight information and user's data from the e-card. The EBG 123 then creates 249 link information between e-boarding pass, flight information and user's data. Finally, the EBG 123 stores 250 the e-boarding pass, flight information and user's data into a travelling database 125.

It will be appreciated by persons skilled in the art that the present invention may also include further additional modifications made to the device which does not affect the overall functioning of the device.

CLAIMS

1. A method of booking a ticket comprising the steps of:

accessing (200) a ticket provider's website to book a ticket;

reading (210) a user's details from an electronic smartcard (13) when a ticket booking is requested,

setting (217) a personal identification number (107) for the ticket booking;

generating (220) an anonymous number and associating it with the ticket booking;

storing (227) said anonymous number such that the user can obtain the ticket by reading the smartcard at a ticket retrieval station;

characterised in that the user's details are encrypted (219) with said personal identification number (107) as a secret key.

2. A method according to claim 1 wherein the anonymous number is generated (220) based on the encrypted user's details and personal identification number (107).

3. A method according to claim 1 wherein the smartcard (13) includes a physically unclonable function (14) which is validated via a challenge-response session.

4. A method according to claim 3 wherein the personal identification number (107) is used in the challenge-response session.

5. A method according to claim 1 wherein a user obtains the ticket by using their smartcard and personal identification number (107) at a ticket retrieval station (16).

6. A method according to claim 5 wherein the ticket retrieval station (16) generates (242) the anonymous number based on the encrypted user's details and personal identification number (107), and retrieves (247) the details of the ticket booking.

7. A system for booking a ticket comprising:

a ticket provider's website configured for allowing a user to book a ticket;

a card reader (15) for reading a user's details from an electronic smartcard (13) when a ticket booking is requested;

input means for setting a personal identification number (107);

processing means for generating (220) an anonymous number based on said user's details and associating the anonymous number with the ticket booking

storage means for storing (227) said anonymous number; and

a ticket retrieval station (16) for reading the smartcard (13) and generating the anonymous number such that the user can obtain the ticket;

characterised in that the user's details are encrypted with said personal identification number (107) as a secret key.

8. A system according to claim 7 wherein the ticket is for a flight or other means of transport.

9. A system according to claim 7 wherein the ticket retrieval station (16) is capable of creating and/or printing a boarding pass.

10. A system according to claim 7 wherein the anonymous number is generated (220) based on the encrypted user's details and personal identification number (107).

Figure 1

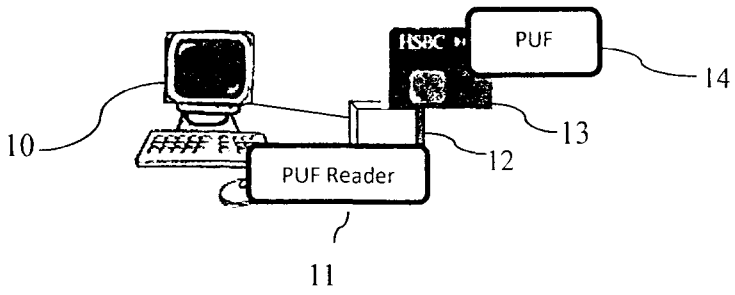


Figure 2

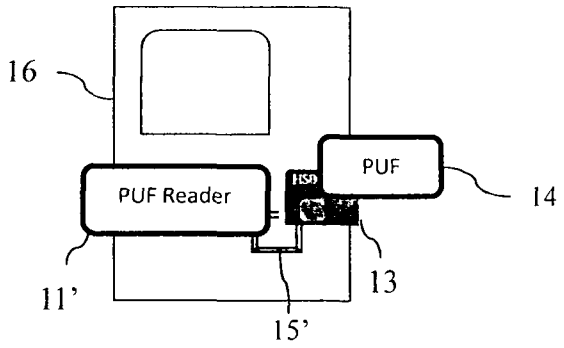


Figure 3

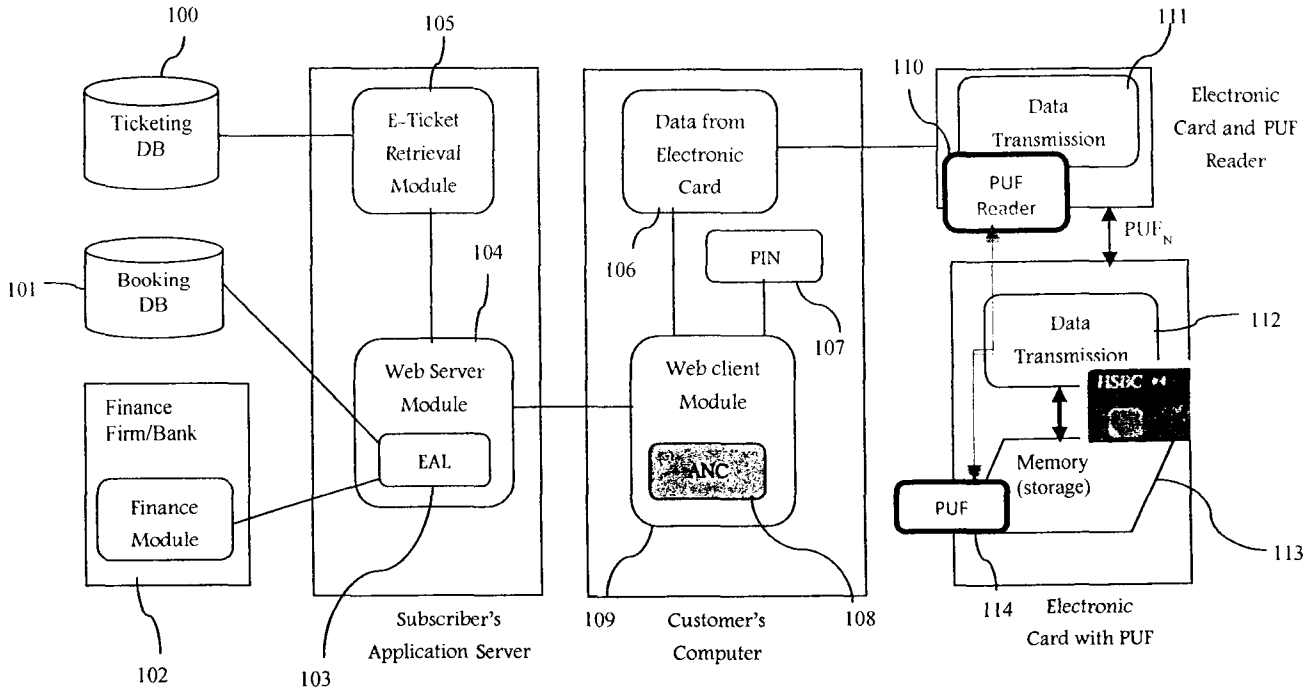


Figure 4

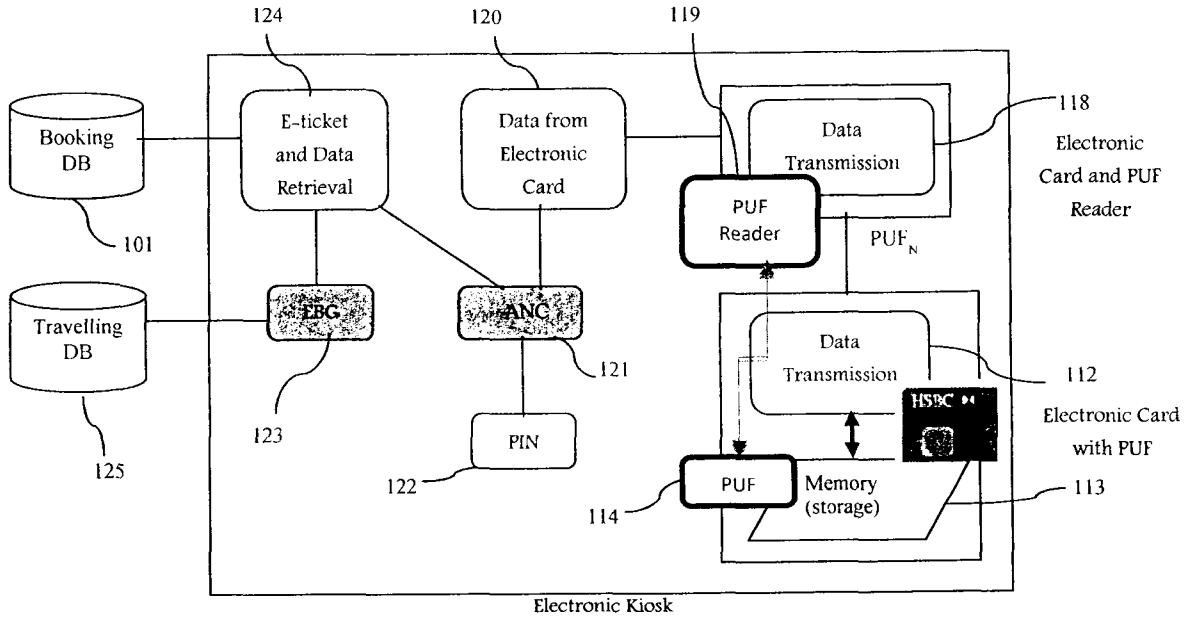


Figure 5

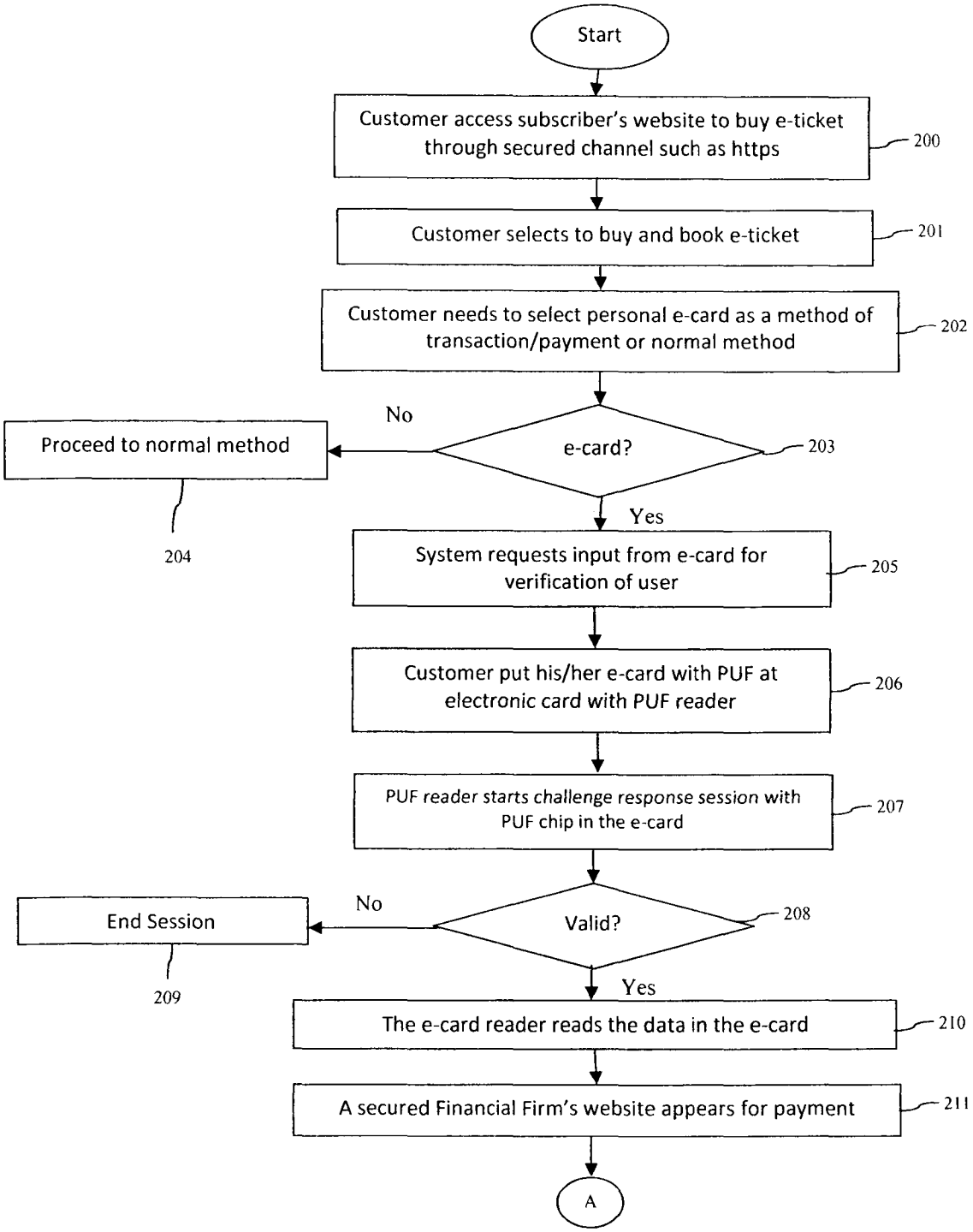

Start
Customer access subscriber's website to buy e-ticket through secured channel such as https
200
Customer selects to buy and book e-ticket
201
Customer needs to select personal e-card as a method of transaction/payment or normal method
202
No
Proceed to normal method
e-card?
203
204
Yes
System requests input from e-card for verification of user
205
Customer put his/her e-card with PUF at electronic card with PUF reader
206
PUF reader starts challenge response session with PUF chip in the e-card
207
No
End Session
Valid?
208
209
Yes
The e-card reader reads the data in the e-card
210
A secured Financial Firm's website appears for payment
211
A

Figure 6

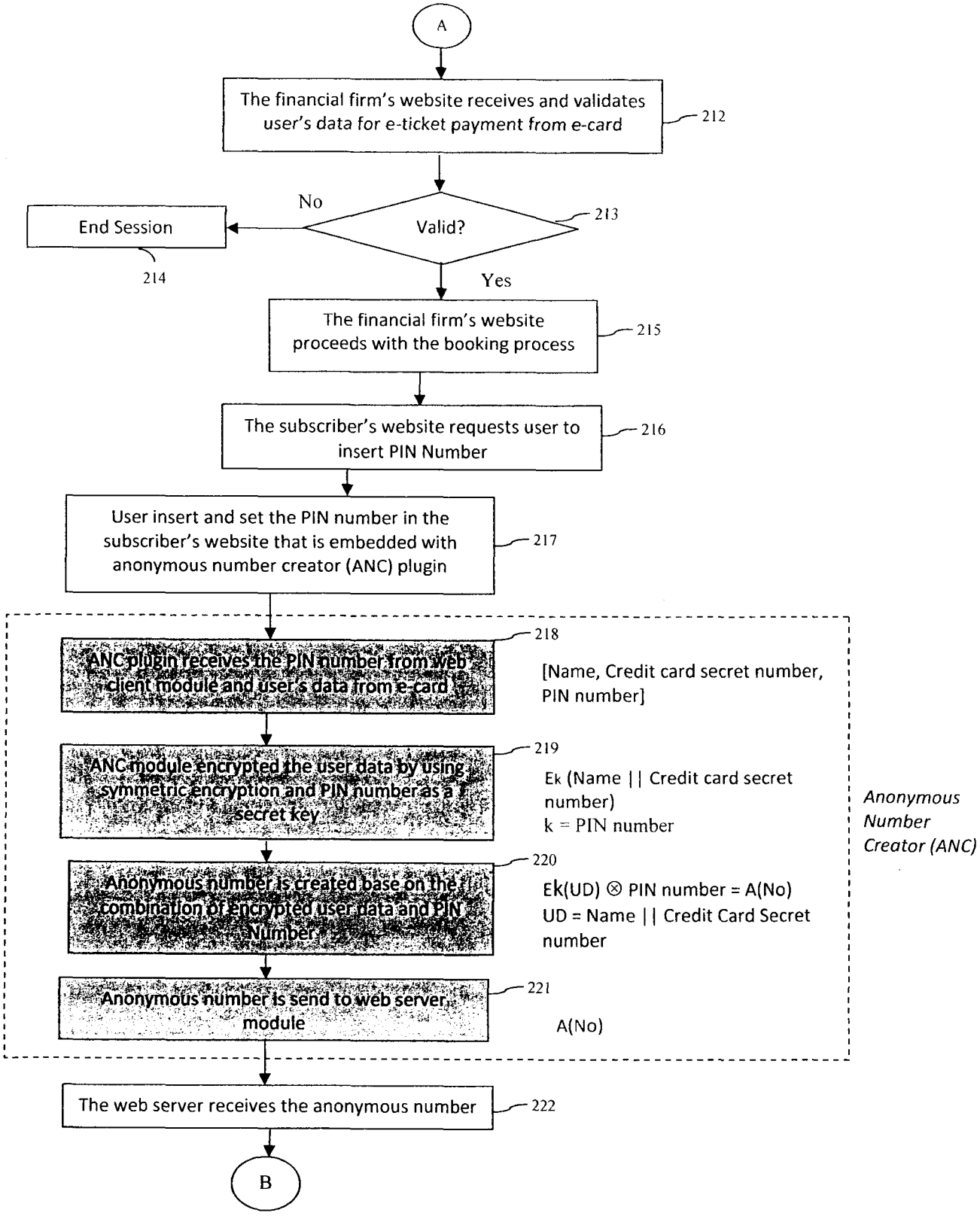

A
The financial firm's website receives and validates user's data for e-ticket payment from e-card
212
No
Valid?
213
End Session
214
Yes
The financial firm's website proceeds with the booking process
215
The subscriber's website requests user to insert PIN Number
216
User insert and set the PIN number in the subscriber's website that is embedded with anonymous number creator (ANC) plugin
217
ANC plugin receives the PIN number from web client module and user's data from e-card
218
[Name, Credit card secret number, PIN number]
ANC module encrypted the user data by using symmetric encryption and PIN number as a secret key
219
Ek (Name || Credit card secret number)
k = PIN number
Anonymous number is created base on the combination of encrypted user data and PIN Number
220
Ek(UD) ⊗ PIN number = A(No)
UD = Name || Credit Card Secret number
Anonymous number is send to web server module
221
A(No)
Anonymous Number Creator (ANC)
The web server receives the anonymous number
222
B

Figure 7

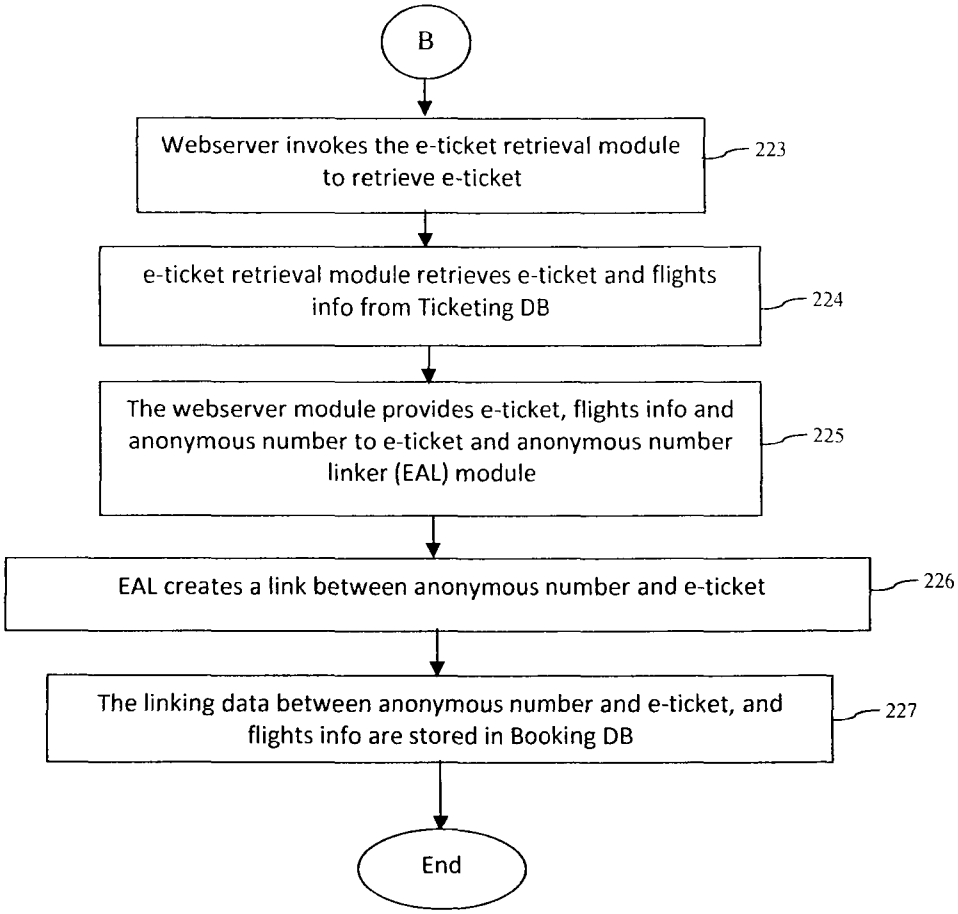

B
Webserver invokes the e-ticket retrieval module to retrieve e-ticket
223
e-ticket retrieval module retrieves e-ticket and flights info from Ticketing DB
224
The webserver module provides e-ticket, flights info and anonymous number to e-ticket and anonymous number linker (EAL) module
225
EAL creates a link between anonymous number and e-ticket
226
The linking data between anonymous number and e-ticket, and flights info are stored in Booking DB
227
End

Figure 8

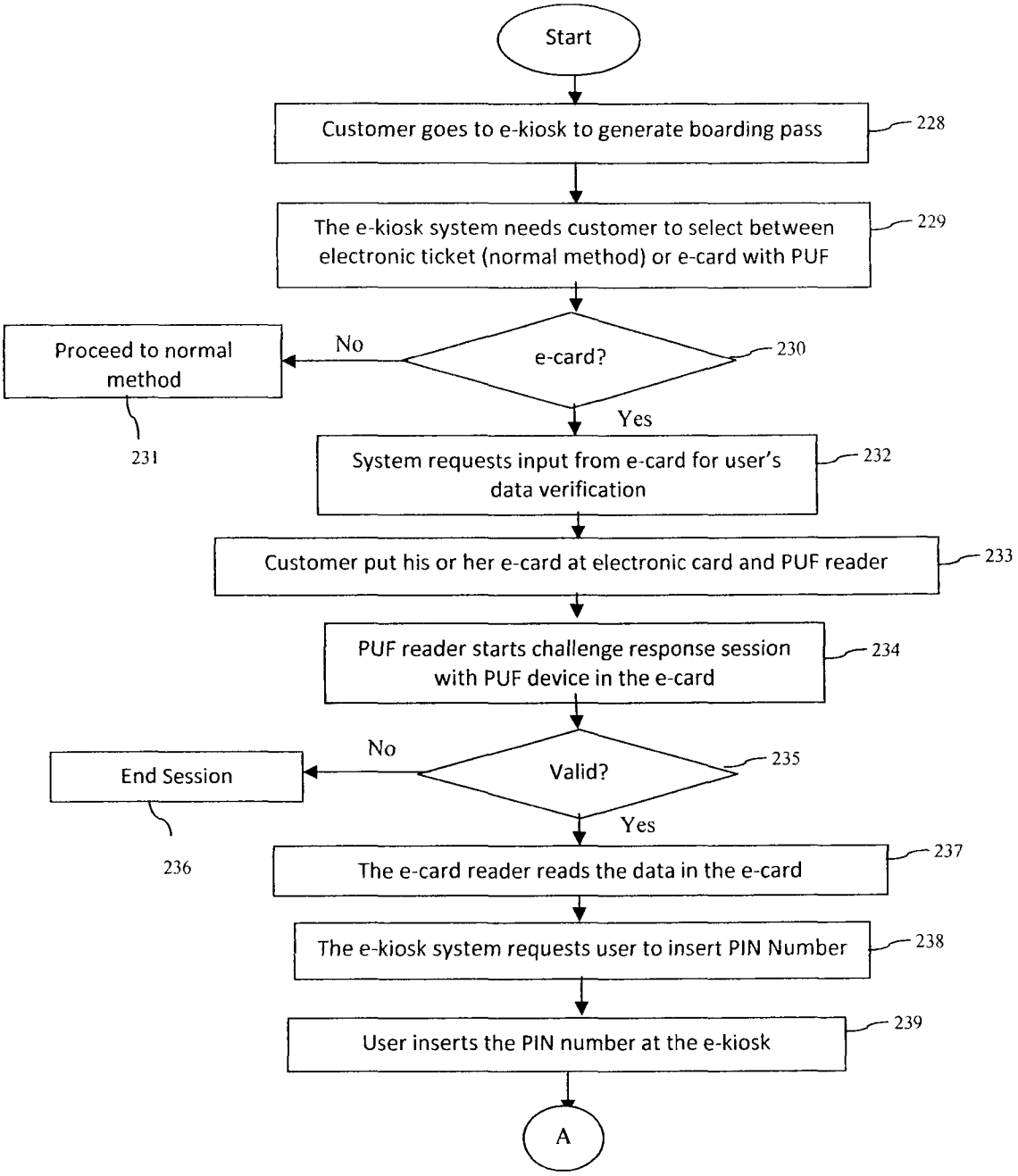
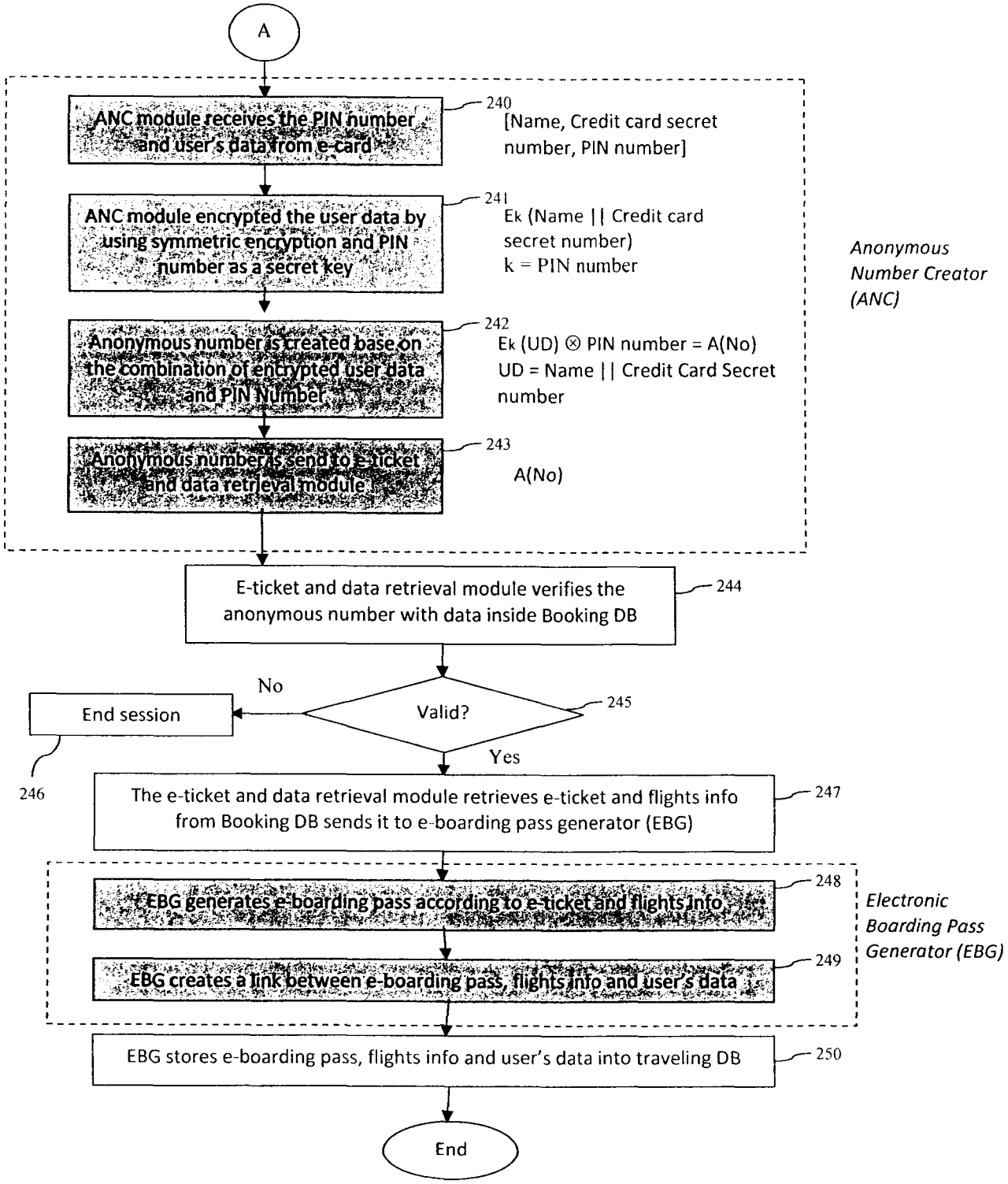

Start
Customer goes to e-kiosk to generate boarding pass
228
The e-kiosk system needs customer to select between electronic ticket (normal method) or e-card with PUF
229
e-card?
230
No
Proceed to normal method
231
Yes
System requests input from e-card for user's data verification
232
Customer put his or her e-card at electronic card and PUF reader
233
PUF reader starts challenge response session with PUF device in the e-card
234
Valid?
235
No
End Session
236
Yes
The e-card reader reads the data in the e-card
237
The e-kiosk system requests user to insert PIN Number
238
User inserts the PIN number at the e-kiosk
239
A

Figure 9


A
ANC module receives the PIN number and user's data from e-card
240
[Name, Credit card secret number, PIN number]
ANC module encrypted the user data by using symmetric encryption and PIN number as a secret key
241
Ek (Name || Credit card secret number)
k = PIN number
Anonymous number is created base on the combination of encrypted user data and PIN Number
242
Ek (UD) ⊗ PIN number = A(No)
UD = Name || Credit Card Secret number
Anonymous number is send to e-ticket and data retrieval module
243
A(No)
Anonymous Number Creator (ANC)
E-ticket and data retrieval module verifies the anonymous number with data inside Booking DB
244
Valid?
245
No
End session
246
Yes
The e-ticket and data retrieval module retrieves e-ticket and flights info from Booking DB sends it to e-boarding pass generator (EBG)
247
EBG generates e-boarding pass according to e-ticket and flights info
248
EBG creates a link between e-boarding pass, flights info and user's data
249
Electronic Boarding Pass Generator (EBG)
EBG stores e-boarding pass, flights info and user's data into traveling DB
250
End

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000085

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q10/02
ADD.

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)
G06Q

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)
EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/111837 A1 (AUPPERLE BRYAN E [US]) 15 August 2002 (2002-08-15) abstract paragraphs [0011] - [0016] paragraphs [0020] - [0021]; figure 1 paragraphs [0023] - [0027]; figure 2 paragraph [0029] paragraph [0031] paragraph [0033]; figure 3	1-10
A	US 2002/111909 A1 (LEE J0NGH0 [KR]) 15 August 2002 (2002-08-15) abstract paragraph [0020]; figure 1 paragraphs [0026] - [0030]; figure 2 paragraphs [0034] - [0044]; figures 3-6	1-10

-/-

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* 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" documentwhich may throw doubts on priority claim(s) orwhich 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	Date of mailing of the international search report
3 September 2014	12/09/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frederic

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000085

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/03040 A1 (ZEBRAPASS INC [US]) 11 January 2001 (2001-01-11) abstract page 33, lines 4-16; figure 15 page 39, line 16 - page 43, line 15; figures 19-22	1-10
A	US 6 101 477 A (HOHLE WILLIAM [US] ET AL) 8 August 2000 (2000-08-08) abstract column 5, lines 1-36 column 8, lines 48-62; figure 5 column 21, line 43 - column 22, line 67	1,3,4,7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2014/000085

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002111837 A1	15-08-2002	NONE	
US 2002111909 A1	15-08-2002	KR 20010035419 A	07-05-2001
		KR 20010113609 A	28-12-2001
		US 2002111909 A1	15-08-2002
WO 0103040 A1	11-01-2001	AU 6069200 A	22-01-2001
		EP 1208504 A1	29-05-2002
		WO 0103040 A1	11-01-2001
US 6101477 A	08-08-2000	AT 298119 T	15-07-2005
		AU 744984 B2	07-03-2002
		AU 2336299 A	09-08-1999
		DE 69925810 D1	21-07-2005
		DE 69925810 T2	04-05-2006
		EP 1050027 A1	08-11-2000
		GB 2333630 A	28-07-1999
		JP 2002501267 A	15-01-2002
		JP 2005100464 A	14-04-2005
		NZ 506167 A	26-11-2002
		US 6101477 A	08-08-2000
		WO 9938129 A1	29-07-1999