

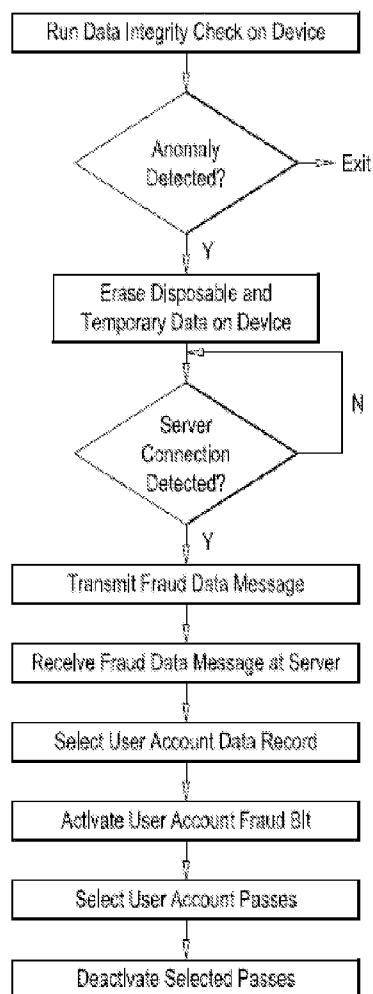


- (51) International Patent Classification:
G07B 11/02 (2006.01) *G06Q 10/02* (2012.01)
H04L 9/08 (2006.01)
- (21) International Application Number:
PCT/US2014/039393
- (22) International Filing Date:
23 May 2014 (23.05.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
13/901,243 23 May 2013 (23.05.2013) US
61/826,850 23 May 2013 (23.05.2013) US
- (71) Applicant: **BYTEMARK, INC.** [US/US]; 275 7th Ave, New York, NY 10001 (US).
- (72) Inventors: **BERGDALE, Micah**; c/o Bytemark, Inc., 275 7th Avenue, Suite 1501, New York, NY 10001 (US). **GRASSER, Matthew**; c/o Bytemark, Inc., 275 7th Avenue, Suite 1501, New York, NY 10001 (US). **IHM, Nicholas**; c/o Bytemark, Inc., 275 7th Avenue, Suite 1501, New York, NY 10001 (US). **REJKO, Kevin**; c/o Bytemark, Inc., 275 7th Avenue, Suite 1501, New York, NY 10001 (US).
- (74) Agent: **SABETY, Ted**; Sabety + Associates, PLLC, 8 West 40th St., 12th Fl., New York, NY 10018 (US).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH DATA INTEGRITY CHECKING

FIG. 22



(57) Abstract: This invention discloses a novel system and method for distributing electronic ticketing to mobile devices such that the ticket stored on the device is checked for its integrity from tampering and the device periodically reports on ticket usage with a central server.





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).

Published:

- with international search report (Art. 21(3))
- 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))

METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH DATA
INTEGRITY CHECKING.

[0001] This patent application claims priority to and incorporates by reference
provisional application U.S. Pat. App. No. 61/826850 filed on May 23, 2013. This patent
5 application claims priority to as a continuation in part and incorporates by reference: U.S. Pat.
App. No. 13/110,709 filed on May 18, 2011, U.S. Pat. App. No. 13/046,413 filed on March 11,
2011 and U.S. Pat. App. No. 13/901,243 filed on May 23, 2013.

FIELD OF INVENTION

10 [0002] This invention provides a mechanism whereby a venue or other facility that
meters usage by means of tickets can distribute tickets electronically and rely on data integrity
checking to confirm that a person holds a valid ticket.

BACKGROUND

15 [0003] Venues such as theaters, amusement parks and other facilities that use
tickets, for example airlines, ferries and other transportation have a need to use electronic
ticketing. Existing systems distribute information that can constitute a ticket, but the
verification problem is difficult. In one example of prior art, an electronic ticket is displayed as
a bar-code on the recipient's telephone display screen. The telephone is then placed on a scanner
20 that reads the bar-code in order to verify the ticket. The problem with these systems is that the
scanning process is fraught with error and the time taken to verify the electronic ticket far
exceeds that of the old system: looking at the paper ticket and tearing it in half. Barcode

scanners were not designed to read a lit LCD screen displaying a bar code. The reflectivity of the screen can defeat the scanning process. Therefore, there is a need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket. This invention provides for the distribution of an electronic ticket that also contains a
5 visual display that ticket takers can rely on as verification, without using a scanning device.

DESCRIPTION OF THE FIGURES

1. Basic architecture.
2. Flow chart for ticket purchase.
- 10 3. Flow chart for displaying the verifying visual object.
4. Example validating visual object.
5. Example validating visual object
6. Schematic of event database record.
7. Schematic of authorized user database record.
- 15 8. Flow chart for transfer of ticket.
9. Example user interface on user's device.
10. Example user interface showing activation selection screen.
11. Example user interface showing display of validating visual object and other ticketing information.
- 20 12. Flowchart for ticket activation process.
13. Protocol diagram for activation process.
14. Continued protocol diagram for activation process.

15. Flowchart for persistent channel.
16. Flowchart for persistent channel for purchase verification.
17. Choose Ticket Save Location
18. Details on Save Locations
- 5 19. Online Tickets List
20. Offline Tickets List
21. Ticket Save Location Settings
22. Data Integrity Flow Chart

10 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

[0004] The system operates on one or more computers, typically one or more file servers connected to the Internet and also on a customer's computing device. A customer's device can be a personal computer, mobile phone, mobile handheld device like a Blackberry™ or iPhone™ or
15 any other kind of computing device a user can use to send and receive data messages. The customer's device is used to display the validating visual object.

[0005] Conventional electronic tickets display a barcode or QR code on a user's telephone, typically a cellphone or other portable wireless device with a display screen. The
20 problem with this approach is that a barcode scanner has to be used by the ticket taker. Barcode scanners are not highly compatible with LCD screen displays of barcodes. The amount of time that it takes to process an electronic ticket is greater than that of a paper ticket. Sometimes the

LCD display does not scan at all and a passenger has to be sent away to get a paper printout of a ticket. Given the potential large crowds that often attend open venues, this is impractical.

[0006] In this invention, the ticket is procured electronically and stored on the user's
5 device. However, when the ticket is to be taken the verification is determined by a larger visual
object that a human can perceive without a machine scanning it. The particular validating visual
object chosen can be constantly changed so that the ticket taker does not have to be concerned
that a device displaying the designated validating visual object is invalid. There are many types
of visual objects that can be displayed that are easily recognized by a ticket taker. These can
10 include but are not limited to: Patterns of color change, Animations and Geometric patterns. In
one embodiment, the validating visual object that is transmitted can be computer code, that when
executed by the device, causes the user device to display the desired visual pattern. In another
embodiment, the validating visual object is a command that specifies what the visual pattern
should be. In that embodiment, the program operating on the user's device receives the command
15 instruction, decodes it, and determines what visual patterns to generate based on the data in the
command instruction. In another embodiment, the validating visual object is video or image
data transmitted directly from the server to the device for immediate display.

[0007] In one embodiment of the invention, the user purchases a ticket from an on-line
20 website. The website sends to the user's device a unique number, referred to as a token. The
token is also stored in the ticketing database. When the time comes to present the ticket, the
venue can select what visual indicator will be used as the designated validation visual object.

The user can then request the validation visual object. The user's device will have an application that launches a user interface. The user can select "validate" or some other equivalent command to cause the application to fetch and download from the ticketing system a data object referred to herein as a ticket payload, which includes a program to run on the user's device. In another
5 embodiment, the ticket payload can be pushed to the device by the venue. As a result, the application transmitted to the user's device is previously unknown to the user and not resident in the user's device. At that point the user's device can execute the program embodied in the ticket payload, which causes the validation visual object to be displayed on the user's device. The ticket taker knows what the validating visual object is, and simply looks to see that the user's
10 device is displaying the correct visual object.

[0008] Piracy is limited in several ways. First, the ticket holder and their device does not have access to the validating visual object until a time select to be close to the point in time where the ticket has to be presented. Second, the validating visual object is one of an very large
15 number of permutations and therefore cannot be guessed, selected or copied ahead of time. Third, the ticket payload can contain code that destroys the validating visual object in a pre-determined period of time after initial display or upon some pre-determined input event. Fourth, a number of security protocols can be utilized to ensure that a copy of the application that executes to display the validating visual object cannot be readily copied or reverse engineered.

20

Validating Visual Object Displays:

[0009] There many kinds of validation displays that can be utilized. The criterion for what constitutes a validating visual object is one that is readily recognizable from human observation, is encapsulated in such a way as to be transmitted to the customer's device with a minimum of network latency or download time, and that can be reasonably secured so as to avoid piracy.

Barcodes and similar codes like the QR code are not validating visual objects because a person looking at them cannot tell one apart from another. Instead, the person has to rely on a barcode scanner and computing device to verify the barcode.

[0010] In one embodiment, the period that a particular validating visual object may be used is automatically limited. Examples of validating visual objects include:

1. A color display on the device.
2. A color sequence.
3. An animation that is easily recognized.
4. Animations can include easily recognizable geometric patterns, for example an array of diamonds, or an array of rotating cubes.
5. A human recognizable image.
6. The customer's face as an image.
7. Combinations of the above.

[0011] In another embodiment, other images, for example, block letter, can be displayed so that additional information readily apparent to the ticket taker is displayed. For example, a letter can be designated for a Child ticket or a different letter for an Adult ticket.

5 [0012] Referring now to Figure 1, the customer uses their device (1) to purchase a ticket from the service operating the system server (2) and database (3).

[0013] In one embodiment, an authorized user associated with the venue, typically the box office manager, logs into the back-end system through a secure web-page. The authorized
10 user can enter the web-page by entering a username, password and venue identifier. The system maintains a database (3) that associates the venue identifier with a set of usernames and password pairs that are authorized to use the system on behalf of the venue. See Fig. 7. The system checks the database (3) to verify that the venue ID, username and password are consistent with each other. The authorized user can navigate through to a point in the system user interface
15 where a particular show may be selected for ticket taking. The user selects the upcoming show, and then selects from a display of possible validating visual objects. The validating visual object is transmitted to a device viewable by ticket taking staff at the entrances to the venue. The staff then can see the authorized object to accept for the upcoming show.

20 [0014] Ticket holders that have purchased tickets have a data record in the system database that contains the unique token associated with the ticket and other relevant information, including the venueID and an identifier identifying the specific show the ticket is for. See Fig. 6.

At the entrance, customers are requested to operate an application on their devices. This application fetches the stored ticket token and transmits that token to the system, preferably over a secure data channel. The database looks up the token to check that the token is valid for the upcoming show. If the token is valid, then the system transmits back to the device a ticket
5 payload. The ticket payload contains computer code that, when operated, displays the selected validating visual object.

[0015] The customer can navigate the user interface of the application in order to cause the application to request whether to display the validating visual object. As shown in Figure 9,
10 one or more available tickets can be displayed on the user interface, which provides the user the ability to select one of the tickets. When the customer properly actuates the user interface, for example, by actuating the "Activate Tickets" button (see Fig. 10), the validating visual object is displayed on the screen of the device. The animation can be presented along with other ticketing information (see Fig. 11). In one embodiment, the device transmits the ticket token to the system
15 with a command indicating that the ticket has been used. In another embodiment, the customer can operate the application and request that the application transmit to the database the condition that the ticket was used. In that embodiment, the user can input a numeric code or password that the application uses to verify that the customer is confirming use of the ticket. In yet another embodiment, after the validating visual object has been launched, a predetermined amount of
20 time later it can be deemed used. At that time, the application can cause the color of the object to be changed so that it indicates that there was a valid ticket, but the ticket was used. This

condition is useful in cases where the venue checks tickets during shows while letting customers move around the venue's facilities.

[0016] In another embodiment, the purchase of the ticket causes the ticket payload to be
5 downloaded to the customer's device. Likewise, the authorized user for the venue will select a
validating visual object for a particular show well in advance of the show. In this case, because
a customer may possess the payload some time before its use, precautions must be taken to
secure the ticket payload from being hacked so that any similar device can display the validating
visual object. While this is a security tradeoff, the benefit is that the customer need not have an
10 Internet connection at a time close to the showtime of the venue.

[0017] The use of electronic ticketing provides opportunities that change how tickets can
be bought and sold,. For example a first customer can purchase a ticket and receive on their
device a ticket token. A second customer can purchase that ticket using the system. The first
15 customer can use the application to send a message to the system server indicating that the first
customer intends to the web-page indicating that it wants to buy that particular ticket. The
system can ask the first customer for a username and password to be associated with the first
customer's ticket. If the second customer identifies the first customer's username, the system
then can match the two together. At that point, the data record associated with the first
20 customer's ticket is modified so that the ticket token value is changed to a new value. That new
ticket token value is then transmitted to the second customer's device. At the same time, the
system can operate a typical on-line payment and credit system that secures payment from the

second customer and credits the first customer. In one embodiment, the system pays the first customer a discounted amount, retaining the balance as a fee.

[0018] In yet another embodiment, the first customer may be unknown to the second
5 customer. In that embodiment, the first customer simply may indicate to the system, through a message transmitted from the application operating on the device or directly through a web-page, that the first customer is not going to use the ticket and wishes to sell it. At that point, the system can mark the data record associated with the ticket as "available for sale." When the second customer makes a request to purchase a ticket for the same show, the system creates a new ticket
10 token for the second customer and updates the ticket token stored in the data record.

[0019] In a general admission type of scenario, the ticketing database is simple: each show has a venue ID, some identifier associated with the show itself, various time indicators, the selected validating visual object, and a list of valid ticket tokens. In a reserved seating
15 arrangement, the ticketing database has a data record associated with a show, as indicated by a show identifier, but each seat has a data record that has a unique show identifier and ticket token, which includes the identity of the seat itself.

[0020] In the preferred embodiment, the validating visual object is secured against
20 tampering. One threat model is that a customer who has received a ticket payload would then take the data file comprising the ticket payload and analyze it to detect the actual program code that when executed, produces the validating visual object on the display screen of the device.

Once that has been accomplished, the would-be pirate can then re-package the code without any security mechanism and readily distribute it to other device owners, or even cross-compile it to execute on other types of display devices. The preferred embodiment addresses this threat model in a number of ways.

5

[0021] First, the ticket payload can be secured in a region of the device under the control of the telecommunications provider. In this case, the customer cannot access the code comprising the ticket payload. In another embodiment, the ticket payload can be encrypted in such a way that the only decrypting key available is in the secure portion of the telecommunications device. In that embodiment, the key is only delivered when an application
10 running on the secure part of the device confirms that the ticket payload that is executing has not been tampered with, for example, by checking the checksum of its run-time image. At that point, the key can be delivered to the ticket payload process so that the validating visual object is displayed on the device.

15

[0022] Second, the selected animation is packaged for each device. That is, the code that operates to display the validating visual object itself operates certain security protocols. The phone transmits a ticket transaction request. The request includes a numeric value unique to the device, for example, an IMEI number. Other embodiments use the UDID or hardware serial
20 number of the device instead of or in combination with the IMEI number. The system server then generates the ticket token using the IMEI number and transmits that value to that device. In addition, the ticket payload is created such that it expects to read the correct IMEI number.

This is accomplished by the system server changing portions of the ticket payload so that the it is customized for each individual IMEI number associated with a ticket token. The animation code comprising the ticket payload is designed so that it has to obtain the correct IMEI number at run time. In another embodiment, at run-time, the animation code will read the particular ticket
5 token specific for the phone that instance of the animation was transmitted to. The code will then decode the token and check that it reflects the correct IMEI number for that device.

[0023] In another embodiment, the security protocol first requires the user to login to the server with a login username and password. The application also transmits the IMEI, UDID or
10 serial number of the device or any combination of them. When verified by the server, an authorization key (Authkey) is transmitted to the device. The Authkey is a random number. When the user's application transmits a request for a validating visual object, it transmits the Authkey and the IMEI, UDID or serial number (or combination) that is used for verification. This is checked by the server for validity in the database. On verification, the validating visual
15 object is encrypted using the Authkey and transmitted to the device. The application running on the device then uses the Authkey to decrypt and display the validating visual object. The Authkey is a one-time key. It is used once for each ticket payload. If a user buys a second ticket from the system, a different, second Authkey is associated with that second ticket payload. In one embodiment, the Authkey is unique to the ticket for a given event. In another embodiment,
20 the Authkey is unique to the ticket, device and the event. In other embodiments, the Authkey can be replaced with a key-pair in an assymetric encryption system. In that case, the validating

visual object is encrypted with a "public"key, and then each user is issued a private key as the "Authkey" to be used to decrypt the object.

[0024] In yet another embodiment, the Authkey can be encrypted on the server and transmitted to the device in encrypted form. Only when the application is operating can the Authkey be decrypted with the appropriate key. In yet another embodiment, the application that displays the validating visual object can request a PIN number or some other login password from the user, such that if the device is lost, the tickets cannot be used by someone who finds the device.

[0025] In another embodiment, the application running on the device can fetch a dynamic script, meaning a piece of code that has instructions arranged in a different order for subsets of devices that request it. The ticket payload is then modified so as to have the same number of versions that are compatible with a corresponding variation in the dynamic script. As a result, it is difficult to reverse engineer the application because the application will be altered at run time and the ticket payload customized for that alteration. One embodiment of the dynamic script would be expressed in Java(tm) computer language and rendered using OpenView. The ticket payload can be an HTML file called using Ajax.

[0026] Security can also be enhanced by actively destroying the validating visual object so that it resides in the device for a limited time. In one embodiment, the ticket payload has a time to kill parameter that provides the application with a count-down time to destroy the

validating visual object. In another embodiment, the validating visual object is displayed when the user holds down a literal or virtual button on the user interface of the device. When the button is released, the application destroys the validating visual object.

5 [0027] Security can also be enhanced by retaining as steganographic data embedded in the validating visual object, the IMEI, UDID, Serial number or phone number of the device. The application can be operated to recover that information and display it on the screen. This makes it possible for security personnel at a venue to view that information from a validly operating device. If the device is showing a pirated validating visual object, then the actual data associated
10 with the device will not match and it will be apparent from inspection of the device. This way, suspicious ticket holders can be subject to increased scrutiny, the presence of which deters piracy.

[0028] In another embodiment, the ticket payload can operate a sound sampling
15 application that requests the customer to speak in to the device. The application can then use that data to check whether the voice print of the speaker matches the expected voice print. In yet another embodiment, the device can take a picture of the customer's face, and then facial recognition code embedded in the ticket payload can operate to check whether the features of the face sufficiently match a pre-determined set of features, that is, of the customer's face at the time
20 the ticket was purchased. In yet another embodiment, the verification can be supplemented by being sure that the use of the ticket is during a pre-determined period of time. In yet another embodiment, the verification can be supplemented by the ticket payload operating to check that

the location of the venue where the ticket is being used is within a pre-determined range of tolerance to a GPS (Global Positioning System) location. In yet another embodiment, after a certain pre-determined number of downloads of ticket payloads for a specific show, the validating visual object is automatically changed. This last mechanism may be used for promotions, to select the first set of ticket buyers for special treatment at the venue. In yet another embodiment, two different validating visual objects may be used, which are selected based on the verified age of the customer. In this way, a venue can use the system to not only to verify ticket holders coming into the venue, but to verify their drinking age when alcoholic drinks are ordered.

[0029] In yet another embodiment, the system's servers control the ticket activation process. Fig. 12. In this embodiment, the token is generated randomly by the user's mobile computing device and then transmitted to and stored on the system server as a result of the user's request to activate the ticket. When the server receives a request to activate a ticket, the server checks whether there is already an activation token stored in its database that corresponds to that ticket. The token is stored in a data record associated with the user that is activating the ticket. The user logs into the account and then requests that a ticket be activated. If it is, then it checks whether the token received from the user's mobile device matches the stored token. That is, it authenticates against that stored token. If the user's request for activation is the first activation of the ticket, then the server stores the received token into the data record associated with the user's account and keeps it there for a predetermined period of time, in order to lock the ticket to that device for that period of time. This process locks a ticket to that unique token for that lock

period. Typically this will lock the ticket to the user's mobile computing device. If the stored token does not match the token received from the user's computing device, the ticket activation is denied.

5 [0030] The predetermined lock time permits a reusable ticket to be locked to a device for the predetermined lock time. This is useful in the event the user changes the mobile computing device that the user uses to the ticket. For example, a monthly train commuting ticket would be activated once each day, and would remain activated for the day of its activation. In this case, the user would validate the ticket once each day, and that activation would be locked to the
10 device for the day. The next day, the user would be able to activate the ticket using a different mobile computing device if the predetermined time locking the activation has expired, that is, if the data record associated with the ticket has been automatically reset into an deactivated state. The activation process also permits a user account to be shared within a family, for instance, but that each ticket sold to that account to be locked to one device.

15

[0031] As depicted in the protocol diagrams Fig. 13a and 13b, the user can use their mobile computing device to request that their ticket get activated for the first time. However, once that activation process has occurred, the server will store the unique token received from the activating user's computing device in the database in a manner that associates it with the
20 ticket and the user's account. If another user associated with the account attempts to use the ticket by activating it, a different random token will be transmitted to the server. Because these two tokens do not match, the second activation will be prohibited.

[0032] The activation process can also permit a ticket to be shared. In this embodiment, the user who has activated the ticket can submit to the server a request that the ticket be transferred to another user. For example, a data message can be transmitted from the user's device to the system that embodies a request to move the ticket to another user. In that case, the stored token is marked as blocked, or is equivalently considered not present. This is accomplished by storing a data flag in the database that corresponds to the ticket. One logic state encodes normal use and the opposite logic state encodes that the ticket has been shared. A data message may be transmitted to the second user indicating that the ticket is available for activation. The second user may submit a request to activate the ticket and a random token value is transmitted from the second user's device to the server. That second token value is checked to see if it's the first activation. Because the first user has activated the ticket, but then transferred it, the activation by the second user is not blocked. That is, the server detects that the first token is now cancelled or equivalently, the system has returned to the state where the first activation has not occurred and therefore permits the new activation to take place. The new activation can also have a predetermined time to live value stored in the database that is associated with it. In this case, the activation by the second user expires and the second user can be prevented from reactivating the ticket. At the same time, the flag setting that disables the first token can be reset, thereby setting the ticket up for reactivation by the first user. By this mechanism, it is possible for the electronic ticket to be lent from one user to another.

[0033] In yet another embodiment, the ticket activation process can open a persistent connection channel over the data network that links the server and the user's mobile computing device. In this embodiment, if the activation of the ticket and therefore the device is successful, the server can maintain a persistent data channel with a computer process running on the user's computing device. In this embodiment, the request for ticket activation causes the user computer device to open the persistent channel. In this embodiment, the server establishes a communication process operating on the server that receives data and then causes that data to be automatically routed to the user's computing device. The process on the user's mobile computing device can thereby automatically respond to that received data. In tandem, the computer process operating on the users computing device can send data directly to the server process associated with that user's session. For a server servicing many user devices, there will be one persistent channel established between the server and each mobile device that has an activated ticket.

[0034] The persistent channel between the server and the user's computer device can be used in a variety of ways. In the preferred embodiment, the persistent connection is designed so that that it maintains a bi-directional, full-duplex communications channel over a single TCP connection. The protocol provides a standardized way for the server to send content to the process operating on the user's computing device without being solicited by the user's device each time for that information, and allowing for messages to be passed back and forth while keeping the connection open. In this way a two-way (bi-direction) ongoing interaction can take place between a process operating on the user's computing device the server. By means of the

persistent channel, the server can control the activity of the user computer device. For each user computing device, there can be a distinct persistent connection.

[0035] In one embodiment, the persistent connection is established when the user
5 requests an activation of a ticket. See Fig. 14. In other embodiments, it can be used if the system is used to verify payment of a purchase price. In either case, the user computing device transmits a request message to the server. For each user computing device, there can be a distinct persistent channel. Each persistent channel has a label or channel name that can be used by the server to address the channel. In the case of ticketing, when the ticket is activated the data
10 representing the validating visual object can be transmitted in real time from the server to the user computing device and immediately displayed on the device. This provides an additional method of securing the visual ticketing process. In this case, when the ticket is activated and the persistent channel is created, the label of the channel is stored in the database in a data record associated with the user and the ticket. When the server transmits the validating visual object for
15 that ticket, it fetches from the database the label of the channel and then uses that label to route the transmission of the validating visual object. The use of the persistent channel causes the user computer device to immediately and automatically act on the validating visual object. In one embodiment, the receipt of the validating visual object causes the receiving process to immediately in response interpret the command and select and display the required visual
20 pattern. In another embodiment, the process receives a block of code that the process calls on to execute, and that code causes the visual pattern to be displayed. In yet another embodiment, the

process receives image or video data and the process passes that data on to the user device screen display functions for presentation on the user device screen.

[0036] In another embodiment, a validating visual object can be transmitted to the user's
5 computing device to be automatically displayed on the screen without the user having to input a command to cause the display. That visual object can be displayed by the user computing device. For additional security, the server can transmit to the user computing device a visual object that contains the channel name or a unique number that the server can map to the channel name. For clarity, this additional visual object is not necessarily used for visual verification by
10 ticket takers, as explained above. This visual object can be used by other machinery to confirm the ticket purchase transaction or even other transactions not directly related to the purchase of the ticket. The additional visual object can be in the form of a QR code, barcode or any other visual object that can be scanned, for example at a point of sale system, and from that scanned image, an embedded data payload extracted. In that visual object, data can be embedded that
15 uniquely identifies the source of the scanned object. The channel name of the persistent channel or a number uniquely mapped on the server to identify the channel can be embedded in that scanned object.

[0037] In one embodiment, as shown on Fig. 15, a merchant can use a point of sale
20 system operated by the merchant to scan the display screen of the user's computing device. That point of sale system can then capture from the scanned image the channel name or a unique number that is uniquely mapped on the server to the channel name. That information is

transmitted to the server as a challenge for verification. The received challenge data is checked to see if it matches the channel name or corresponding unique number used to transmit the visual object that the merchant scanned. If they match up, there is a verification of a transaction. This exchange provides verification that the user's device is present at the merchant location and that
5 a transaction with the merchant should be paid for.

[0038] In yet another embodiment, the persistent connection provides a means for the server to control the actions of the process operating on the user's computer device that is at the other end of the connection. In this embodiment, the server can automatically transmit a
10 command to the process on the user's computing device that automatically deletes the verifying visual object that has been transmitted to ensure that it cannot be reused or copied.

[0039] In one embodiment, the persistent connection is used to automatically transmit visual information to the user's mobile computing device and to cause that information to be
15 displayed on the screen of the device. The visual information can be the validating visual object or any other visual object that the server selects to transmit for display. In this embodiment, the persistent connection can be used by the server to transmit other information to the user's device. In this embodiment, the server transmits text, images, video or sound and in some cases in combination with other HTML data. In another embodiment, this material comprises
20 advertising that the server selects to display on the user's device. The selection process can utilize the GPS feature described above to determine the approximate location of the user's device and then based on that location, select advertising appropriate to be transmitted to that

device. In yet another embodiment, the server selects the advertising content by determining predetermined features of the validated ticket or purchasing transaction and then making a selection on the basis of those features. For example, a validation of a ticket to a baseball game played by a team specified in the data associated with the validated ticket may cause the
5 selection of an offer to purchase a ticket for the next baseball game of the same team. In yet another embodiment, the character of the transaction being verified can be used to cause the selection of advertising or the transmission of data comprising a discount offer related to the transaction.

10 [0040] In this embodiment, the server receives from the merchant the data that determines the persistent channel. The merchant, by relying on the system for payment will also transmit transaction details, for example, an amount of money and an identity of goods or services. When the channel name or unique number associated with the channel is matched for verification, the server can transmit data representing a confirmation display down to the user's
15 device using the persistent connection. This data is received by the user computing device and then automatically rendered by the process at the other end of the channel connection. In addition, the server can use the transaction information to determine one or more advertisements or discount offers to transmit to the user's computing device. The selection method can consist of one or more heuristics. In one example, the validation of the ticket for a baseball game can
20 trigger the display of advertising for food or drinks. Likewise, a transaction for purchasing a cup of coffee can trigger an advertisement for purchasing a newspaper.

Mobile ticket or pass management may be maintained securely by implementing protocols that check for pass data integrity and permit movement of passes between a user's device, their account on a server and to an alternative device. These methods and systems are applicable to mobile tickets or passes, whether using a visual validation display object or some other
5 validation technique when they are used.

[0041] Offline Passes.

In yet another embodiment, the mobile ticket is stored on the user's device. This is presented to the user as an option. At the time of purchase, the user may specify by input into a GUI, either
10 on the device or through a webpage displayed on their computer, whether any given mobile ticket (also referred to herein as a "pass") that they own is to be stored either "On This Device" or "In My Cloud Account." (See Figs. 17 and 18). When the user stored the pass to the current device, this allows for the full lifecycle of the pass to occur with no data connection between the device and the server operating the ticketing back-office. This means the customer can list the
15 pass on the device display, use the pass on the device, re-use the pass, and watch the pass expire, all without the need for a network connection to the device. In this embodiment, an accounting of the usage of the pass on the device is maintained on the back office server by means of a synchronization protocol executed between the device and the server when the next network or Internet connection becomes available to the device. A combination of fraud-prevention
20 features built into the software operating on the device and fraud-detection features built into the back-office server platform execute this process. In one example, the pass that has been stored

on one device cannot be accessed from the user's account on the server by another device without the first device "releasing" it to the user's Cloud Account.

[0042] Cloud Account. In one embodiment, the back office server maintains an account associated with the user. The server's database can store in a data structure data representing a ticket or pass and associate it with the user. When a customer elects to store a pass that is purchased in their Cloud Account, this means that the pass can be used from any device, provided that the user has

authenticated themselves as the owner of the Pass by logging in from a device and retrieving an authentication token, and that the Pass not already in use on another device. While this embodiment introduces the convenience of allowing any authenticated device to access a user's purchased ticket, the limitation here is that a pass stored to the user's Cloud Account can only be accessed by a device when there is connectivity between the device and the back-office server.

[0043] Listing Tickets. When the user's device has an online connection, all tickets, whether stored on the device or on the user's account in the cloud are displayed on the user's device, for example as presented in Fig. 19. Passes saved to another device are displayed with an indication that this is the case. When the pass is an "unlimited use", the GUI displays their expiration time, and other Passes are grouped by label for easy access.

As mentioned above, when the device has no network connectivity, the Cloud Account Passes will not be available for use. However, Passes saved “On This Device” will be displayed, and will be available for use (Fig. 20).

5 [0044] Using a Pass Effects Its Status. Regardless of where a pass is initially stored, whether on the user’s device or in the user’s cloud account, a data file representing the ticket will be cached locally on the device during the duration that the pass is active. For instance, if the rules set up via the back office system allow a pass to be reactivated for display for 30 minutes after initial activation, the pass will be cached locally on the device for those 30
10 minutes. When that time expires, a status value associated with that pass will revert to a value representing a use or expiration. If the pass is stored on the device, that status value is maintained on the device. If the pass is stored on the cloud, the device transmits a message to the server indicating the new status of the pass, and the server updates the data record associated with the pass to indicate the new status of the pass. This new status is then usable if the pass is
15 reused on a different device by the authenticated user.

[0045] In another embodiment, the GUI presented to by the back office server permits the user to change their mind about whether a purchased pass is stored on the user’s device or on the server in their cloud account. (See Fig. 21). The user can input a selection in order to
20 choose to save a pass currently stored in their Cloud Account to their device, or they can release a Pass currently stored on their device back to their Cloud account — provided logical conditions are satisfied that maintain the integrity of the ticket usage accounting. In this case, the locally

stored usage is transmitted to the server in order to update the pass data on the server to the most recent use of the pass.

[0046] Bytemark Offline Pass Schema

- 5 In order to effect an offline ticketing solution in a reliable and secure manner, the following schema was devised. It consists of four main classes of data – Permanent Data, Semi-Permanent Data, Temporary Data, and Disposable Data.

[0047] Permanent Data

- 10 The only Permanent Data is static hardware-based device identifier (eg. Vendor ID for iOS™, Android ID for Android™), and a hard-coded string in the software that is referred to as the Salt. These are used in specific sets of functionality in the other two Data classes.

[0048] Semi--Permanent Data

- 15 The Semi-Permanent Data includes any data that is critical for account management, namely any user detail information about the customer and any device- specific information.
- This class of data also includes a ticketing app software installation identifier (AII), and is unique to the particular install of the app on each specific device. It is critical to note that if a customer installs an app on 2 devices, the AII on each device will be distinct. Likewise,
- 20 installing 2 instances of the app on the same device produces 2 distinct identifiers. This Semi-Permanent Data is stored in a set of tables that is encrypted by the hardware-based identifier, and uniquely associated with the Salt data.

[0049] Temporary Data

The Temporary data is the data that is solely stored on the device in order to later interact with the back office server and synchronize data. It includes a list of cached uses for passes that were
5 used on the device when there was no network connection available. It also includes the Authentication Token that is stored by the local ticketing software after a successful sign-in, the time of this sign-in, and the last time the device was online and synced with the server. This Temporary Data is stored in a set of tables that is encrypted by the ticketing app, using the AII.

10 [0050] Disposable Data

The Disposable Data is the data that is temporarily cached on the device until the next online connection occurs. It is referred to as disposable because it can be completely recovered after deletion by simply regaining a network connection. The purpose of this data class is to store any pass, event, and visual validation display object data that is minimally necessary to maintain
15 the desired ticketing functionality on the device without a data connection. The Disposable Data is stored in a set of tables that is encrypted by the Authentication Token. This Disposable Data as a whole may optionally be set to expire after a set amount of time has passed with no network connection to the device. For instance, if a user's device has not synchronized with the server in within the expiration time, the software operating on the user's device erases Disposable Data.
20 As a result, the user has to log in again to sync with the server to obtain ticketing data. In embodiment, each element of the Disposable Data is associated with its own expiration rule, which may be specified by the back office server. For instance, a pass can be set to expire 30

minutes after the first use. As another example, a pass can be set to end at the end of the month. These rules are periodically run against the disposable data to ensure data integrity.

[0051] Data Integrity. Data integrity checking is to be sure that the pass data and the software managing that pass data on the user's device has not been altered improperly. For example, if the pass data or other data is unrecognized by the server or is inconsistent with a separate locally generated key on the device, there is an anomaly. When these anomalies are detected the tickets and user account are locked down to stop fraudulent activity. Behavioral Detection is focused on backend detection of usage of mobile ticketing and passes that do not match up with a consumer's typical usage habits. For example, the system detect a pass that is normally activated in the mornings going from Point A to Point B and then in the evening from Point B to Point A. If the system later detects that the ticket is activated for Point A to Point B say in the afternoon and there was a previous usage of a ticket from Point A to Point B without a return trip from Point B to Point A, it flags in the system that there is a behavioral anomaly and that there might be fraud or an attempt to share an account amongst multiple users. This detection technique is particularly helpful for monthly passes because they are the most likely to attempt to have repeated or fraudulent usage and are typically used by commuters. Whenever the ticketing software operating on the user's device determines that the disposable data has been maliciously altered, the session is cleared from the device, that is, the Temporary and Disposable Data is erased from the device. In one embodiment, the software operating on the user's device checks the data files representing the passes to see if a hash value for any of those files has changed or is invalid. In another embodiment, the software checks to see if the file has

been modified or stored with a time stamp that is later than the time that the pass was stored on the device. In yet another embodiment, the software checks for the condition where the AII is not properly decrypting pass data that is stored on the device. Any of these conditions are examples where the data integrity test fails.

5

[0052] As a result, the user will be forced to log in to the server again and authenticate themselves, which requires a network connection. At this point, the device will be able to synchronize with the server. The server can then determine if any fraudulent activity has taken place by inspection of the data transmitted by the device up to the server. Other data integrity tests can include transmitting the AII to the server to determine whether the device is using the proper AII. Other behavioral anomaly detection can be used. For example, if the same pass data is being used for multiple attempts to activate the same pass from different devices, this would indicate that the original purchaser may have maliciously distributed the ticket, or that their device was hacked and the ticket was maliciously obtained for further re-distribution.

15

If such suspicious activity is detected, the user account is flagged for further investigation if necessary, for example, by setting a status bit in a data record associated with the user to indicate a fraudulent transaction has occurred. When this logical condition is established, any passes that were previously locked to the device will no longer be available on any device. That is, the user's account data on the back office server is set so that each purchased pass has a status bit indicating that it is unavailable for use for security reasons.

20

[0053] In yet another embodiment, a user who has lost their device can recover their purchased tickets by having these bits set by an authorized user of the back office system, for example by means of a customer service call. In this situation, the authorized user can “unlock” passes stored on a lost device. When Passes are unlocked from a device, the device is
5 flagged as disabled, and any future activity that occurs on this device will be noted as fraudulent. On the next synchronization with the back office server, the software running on the device will erase the data associated with the user’s passes, including the Temporary and Disposable Data.

Operating Environment:

10 [0054] The system operates on one or more computers, typically one or more file servers connected to the Internet. The system is typically comprised of a central server that is connected by a data network to a user’s computer. The central server may be comprised of one or more computers connected to one or more mass storage devices. A website is a central server that is connected to the Internet. The typical website has one or more files, referred to as web-pages,
15 that are transmitted to a user’s computer so that the user’s computer displays an interface in dependence on the contents of the web-page file. The web-page file can contain HTML or other data that is rendered by a program operating on the user’s computer. That program, referred to as a browser, permits the user to actuate virtual buttons or controls that are displayed by the browser and to input alphanumeric data. The browser operating on the user’s computer then
20 transmits values associated with the buttons or other controls and any input alphanumeric strings to the website. The website then processes these inputs, in some cases transmitting back to the user’s computer additional data that is displayed by the browser. The precise architecture of the

central server does not limit the claimed invention. In addition, the data network may operate with several levels, such that the user's computer is connected through a fire wall to one server, which routes communications to another server that executes the disclosed methods. The precise details of the data network architecture does not limit the claimed invention. Further, the user's

5 computer may be a laptop or desktop type of personal computer. It can also be a cell phone, smart phone or other handheld device. The precise form factor of the user's computer does not limit the claimed invention. In one embodiment, the user's computer is omitted, and instead a separate computing functionality provided that works with the central server. This may be housed in the central server or operatively connected to it. In this case, an operator can take a

10 telephone call from a customer and input into the computing system the customer's data in accordance with the disclosed method. Further, the customer may receive from and transmit data to the central server by means of the Internet, whereby the customer accesses an account using an Internet web-browser and browser displays an interactive webpage operatively connected to the central server. The central server transmits and receives data in response to data and

15 commands transmitted from the browser in response to the customer's actuation of the browser user interface.

[0055] A server may be a computer comprised of a central processing unit with a mass storage device and a network connection. In addition a server can include multiple of such

20 computers connected together with a data network or other data transfer connection, or, multiple computers on a network with network accessed storage, in a manner that provides such functionality as a group. Practitioners of ordinary skill will recognize that functions that are

accomplished on one server may be partitioned and accomplished on multiple servers that are operatively connected by a computer network by means of appropriate inter process communication. In addition, the access of the website can be by means of an Internet browser accessing a secure or public page or by means of a client program running on a local computer
5 that is connected over a computer network to the server. A data message and data upload or download can be delivered over the Internet using typical protocols, including TCP/IP, HTTP, SMTP, RPC, FTP or other kinds of data communication protocols that permit processes running on two remote computers to exchange information by means of digital network communication. As a result a data message can be a data packet transmitted from or received by a computer
10 containing a destination network address, a destination process or application identifier, and data values that can be parsed at the destination computer located at the destination network address by the destination application in order that the relevant data values are extracted and used by the destination application.

15 [0056] It should be noted that the flow diagrams are used herein to demonstrate various aspects of the invention, and should not be construed to limit the present invention to any particular logic flow or logic implementation. The described logic may be partitioned into different logic blocks (e.g., programs, modules, functions, or subroutines) without changing the overall results or otherwise departing from the true scope of the invention. Oftentimes, logic
20 elements may be added, modified, omitted, performed in a different order, or implemented using different logic constructs (e.g., logic gates, looping primitives, conditional logic, and other logic

constructs) without changing the overall results or otherwise departing from the true scope of the invention.

[0057] The method described herein can be executed on a computer system, generally
5 comprised of a central processing unit (CPU) that is operatively connected to a memory device,
data input and output circuitry (IO) and computer data network communication circuitry.
Computer code executed by the CPU can take data received by the data communication circuitry
and store it in the memory device. In addition, the CPU can take data from the I/O circuitry and
store it in the memory device. Further, the CPU can take data from a memory device and output
10 it through the IO circuitry or the data communication circuitry. The data stored in memory may
be further recalled from the memory device, further processed or modified by the CPU in the
manner described herein and restored in the same memory device or a different memory device
operatively connected to the CPU including by means of the data network circuitry. The memory
device can be any kind of data storage circuit or magnetic storage or optical device, including a
15 hard disk, optical disk or solid state memory.

[0058] Examples of well known computing systems, environments, and/or configurations
that may be suitable for use with the invention include, but are not limited to, personal
computers, server computers, hand-held, laptop or mobile computer or communications devices
20 such as cell phones and PDA's, multiprocessor systems, microprocessor-based systems, set top
boxes, programmable consumer electronics, network PCs, minicomputers, mainframe

computers, distributed computing environments that include any of the above systems or devices, and the like.

[0059] Computer program logic implementing all or part of the functionality previously
5 described herein may be embodied in various forms, including, but in no way limited to, a source
code form, a computer executable form, and various intermediate forms (e.g., forms generated by
an assembler, compiler, linker, or locator.) Source code may include a series of computer
program instructions implemented in any of various programming languages (e.g., an object
code, an assembly language, or a high-level language such as FORTRAN, C, C++, JAVA, or
10 HTML) for use with various operating systems or operating environments. The source code may
define and use various data structures and communication messages. The source code may be in
a computer executable form (e.g., via an interpreter), or the source code may be converted (e.g.,
via a translator, assembler, or compiler) into a computer executable form.

15 [0060] The invention may be described in the general context of computer-executable
instructions, such as program modules, being executed by a computer. Generally, program
modules include routines, programs, objects, components, data structures, etc., that perform
particular tasks or implement particular abstract data types. The computer program and data may
be fixed in any form (e.g., source code form, computer executable form, or an intermediate form)
20 either permanently or transitorily in a tangible storage medium, such as a semiconductor memory
device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic
memory device (e.g., a diskette or fixed hard disk), an optical memory device (e.g., a CD-ROM

or DVD), a PC card (e.g., PCMCIA card), or other memory device. The computer program and data may be fixed in any form in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies, networking technologies, and internetworking technologies. The computer program and data may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software or a magnetic tape), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web.) It is appreciated that any of the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

[0061] The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices. Practitioners of ordinary skill will recognize that the invention may be executed on one or more computer processors that are linked using a data network, including, for example, the Internet. In another embodiment, different steps of the process can be executed by one or more computers and storage devices geographically separated by connected by a data network in a manner so that they operate together to execute the process steps. In one embodiment, a user's computer can run an

application that causes the user's computer to transmit a stream of one or more data packets across a data network to a second computer, referred to here as a server. The server, in turn, may be connected to one or more mass data storage devices where the database is stored. The server can execute a program that receives the transmitted packet and interpret the transmitted data
5 packets in order to extract database query information. The server can then execute the remaining steps of the invention by means of accessing the mass storage devices to derive the desired result of the query. Alternatively, the server can transmit the query information to another computer that is connected to the mass storage devices, and that computer can execute the invention to derive the desired result. The result can then be transmitted back to the user's
10 computer by means of another stream of one or more data packets appropriately addressed to the user's computer.

[0062] The described embodiments of the invention are intended to be exemplary and numerous variations and modifications will be apparent to those skilled in the art. All such
15 variations and modifications are intended to be within the scope of the present invention as defined in the appended claims. Although the present invention has been described and illustrated in detail, it is to be clearly understood that the same is by way of illustration and example only, and is not to be taken by way of limitation. It is appreciated that various features of the invention which are, for clarity, described in the context of separate embodiments may
20 also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable combination. It is appreciated that the particular

embodiment described in the specification is intended only to provide an extremely detailed disclosure of the present invention and is not intended to be limiting.

[0063] Modifications of the above disclosed apparatus and methods which fall within the
5 scope of the invention will be readily apparent to those of ordinary skill in the art. Accordingly, while the present invention has been disclosed in connection with exemplary embodiments thereof, it should be understood that other embodiments may fall within the spirit and scope of the invention, as defined by the following claims.

WHAT IS CLAIMED:

1. A mobile ticketing system comprising a server computer sub-system adapted to receive from a device via a data network, authentication data for a user account, and in dependence thereon, transmit to the device data embodying a pass; where the system is further adapted to determine the occurrence of fraudulent activity associated with the user account in connection with the ticketing system and in response thereto, store in a data record associated with the user a data value indicating the fraudulent activity.
2. The system of Claim 1 where the server sub-system is further adapted to detect fraudulent activity by detecting behavioral anomalies associated with the user's account.
3. The system of Claim 2 where the behavioral anomaly is the condition of one or more attempts to improperly use a pass originally associated with the user account.
4. The system of Claim 1 where the device is further adapted to check the integrity of the pass data stored on the device.
5. The system of claim 4 where the integrity check is to determine whether there is a mismatch of a hash value.
6. The system of Claim 4 where the integrity check is to determine whether a time stamp associated with stored pass data is inconsistent with other storage time stamp data.

7. The system of Claim 1 where the server sub-system is further adapted to receive a command to cause deactivation of a pass stored on the device, receive from the device usage data associated with the deactivated pass, update, using the received usage data, the pass usage data comprising a data record stored on the server system associated with the deactivated pass and in dependence on the updated usage data, transmit to a new device pass data for the same pass.

8. The system of Claim 1 where the server sub-system is further adapted to transmit to the device data representing purchased passes associated with the user account and the device is further adapted to combine the received data with pass data stored on the device in order to output on a graphical user interface operated by the device a list of all available passes.

9. The system of Claim 1 where the device is further adapted to receive from the server sub-system an expiration time value for an activated pass and, in dependence thereon, deactivate the pass when the device detects the condition that the time passed since activating the pass for use equals or exceeds the time value.

10. The system of Claim 9 where for a plurality of passes stored on the device, each expiration time is unique.

11. The system of Claim 1 where the device is further adapted to detect the condition that the device has not connected to the server system for a predetermined period of time and in dependence on such detection, erase the data associated with at least one pass stored on the device.

12. The system of Claim 1 where the detection of fraudulent activity occurs as the result of receiving a data message from the device representing the detection of fraudulent activity on the device.

13. The system of Claim 12 where the device is adapted to erase data stored on the device associated with the passes stored on the device when the condition of fraudulent activity has been detected.

14. The system of Claim 1 where the device is adapted to erase data stored on the device associated with the passes stored on the device when the condition of fraudulent activity has been detected by the device, and to transmit a data message to the server sub-system representing the detection of fraudulent activity on the device.

15. The system of Claim 1 where the server sub-system is adapted to receive a command to set a status bit associated with the user account to indicate fraudulent activity and the device is adapted to receive a data message representing the condition that the fraudulent activity bit is set, and in dependence thereon, disable the pass functionality on the device.

16. The system of Claim 15 where the device is further adapted to disable the pass functionality by erasing the pass data stored on the device.

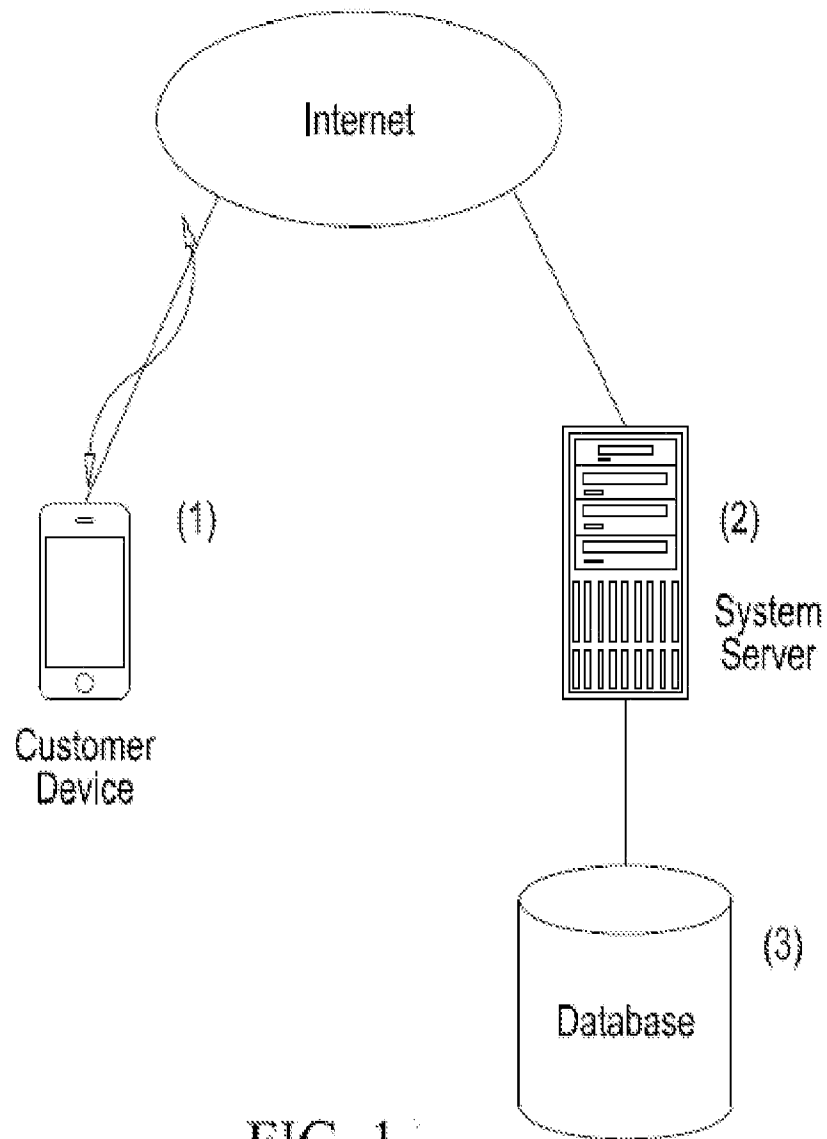


FIG. 1

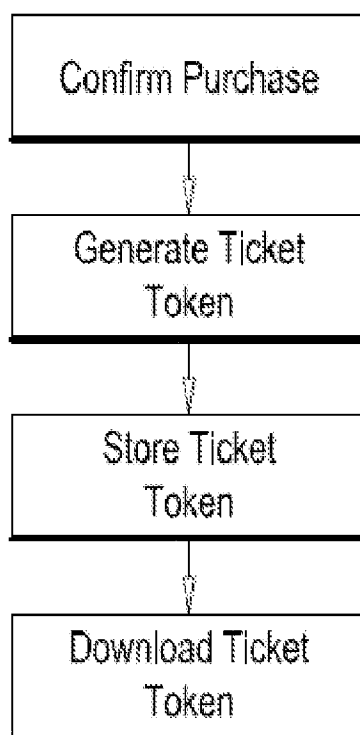


FIG. 2

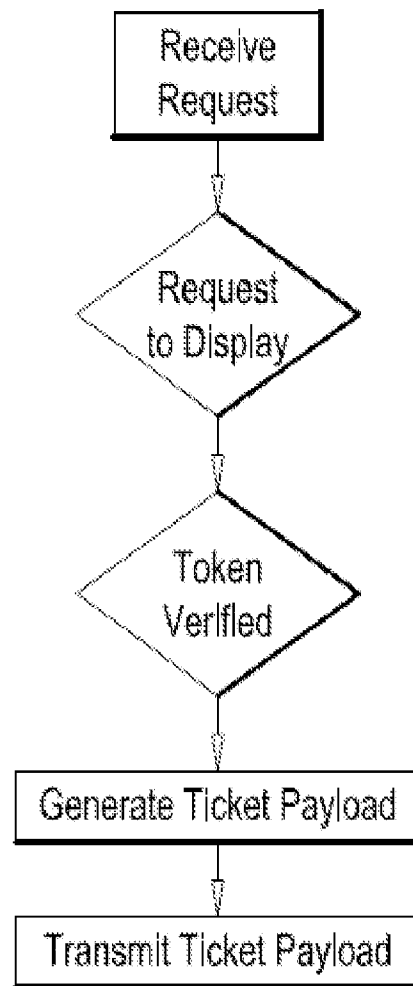


FIG. 3

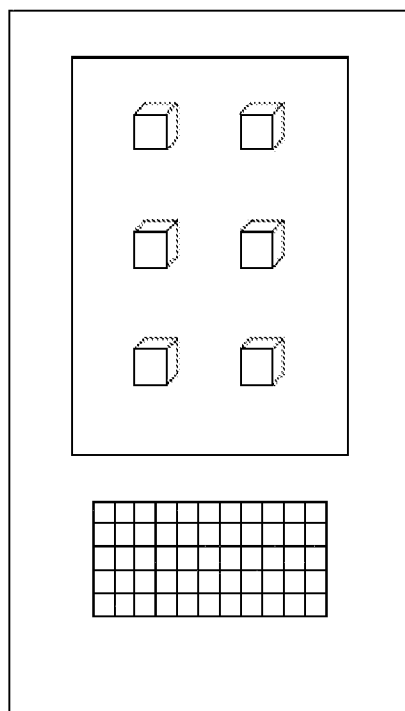


FIG. 4

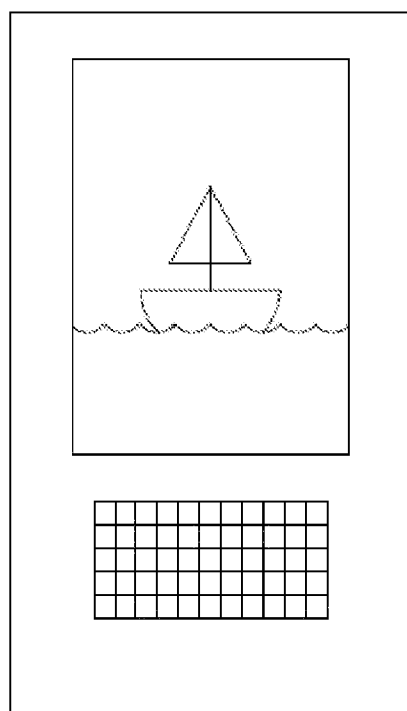


FIG. 5

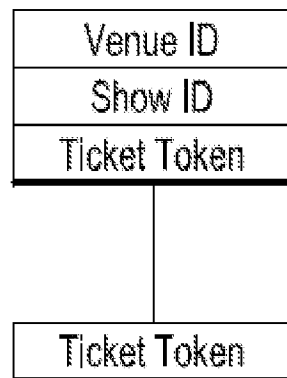


FIG. 6

Venue ID
Username
Password

FIG. 7

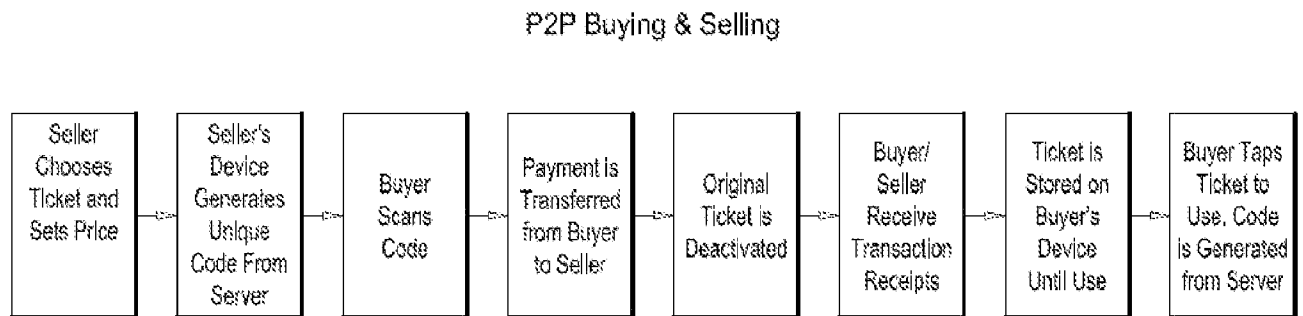


FIG. 8



FIG. 9

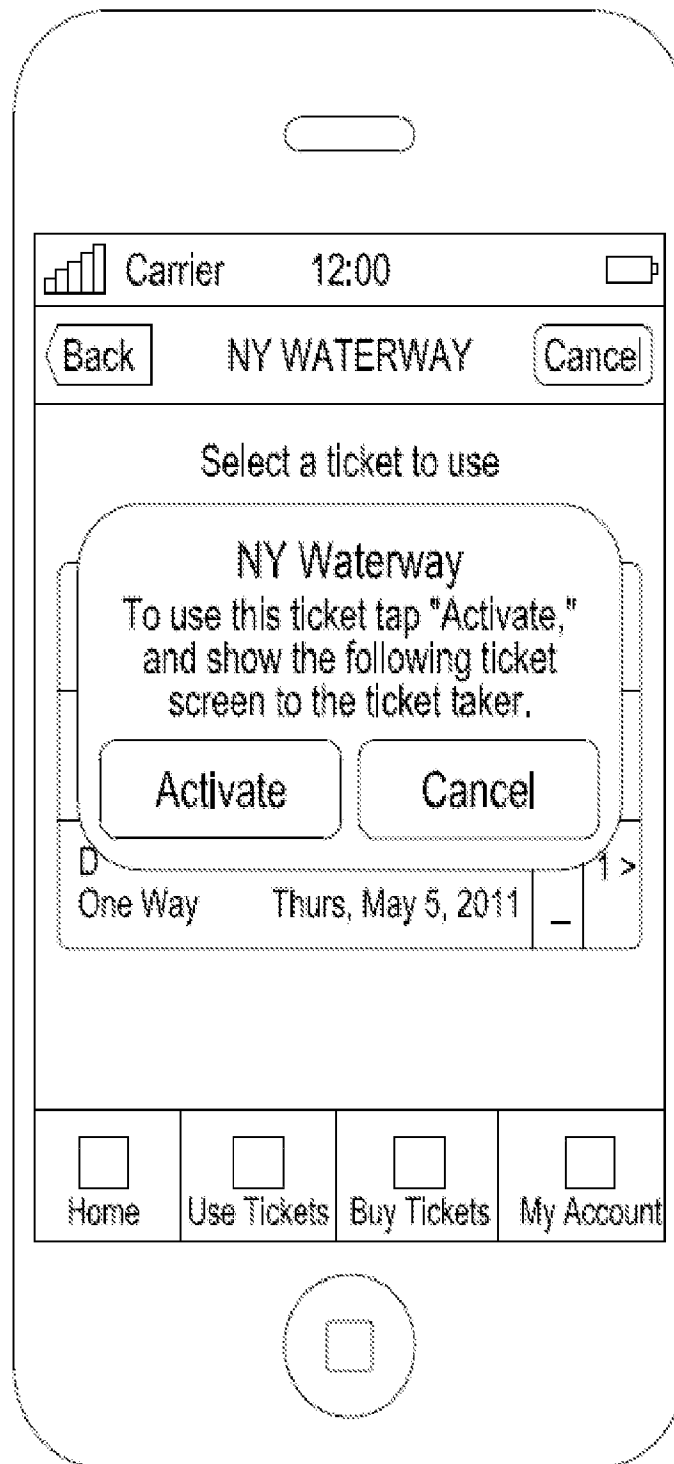


FIG. 10

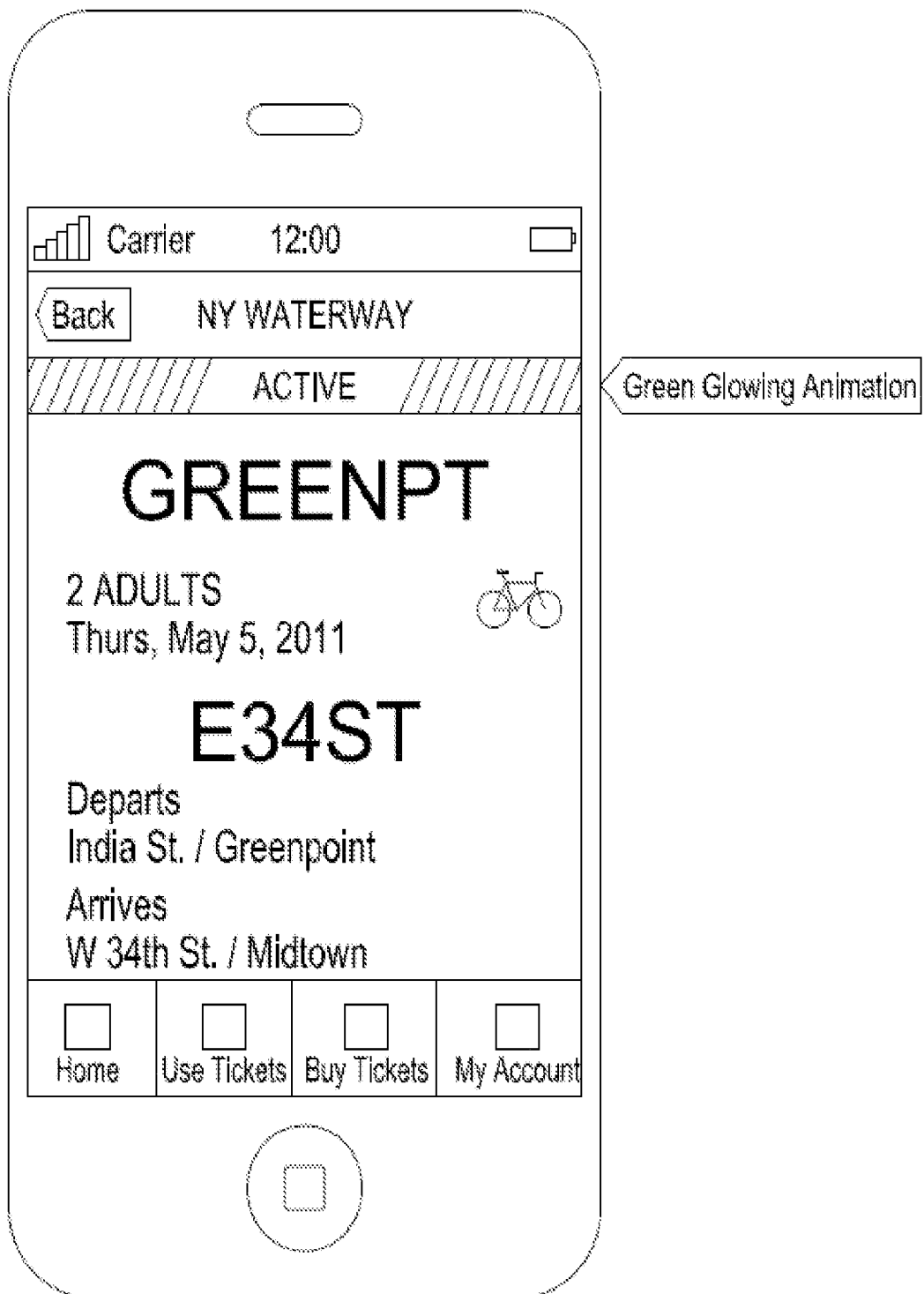


FIG. 11

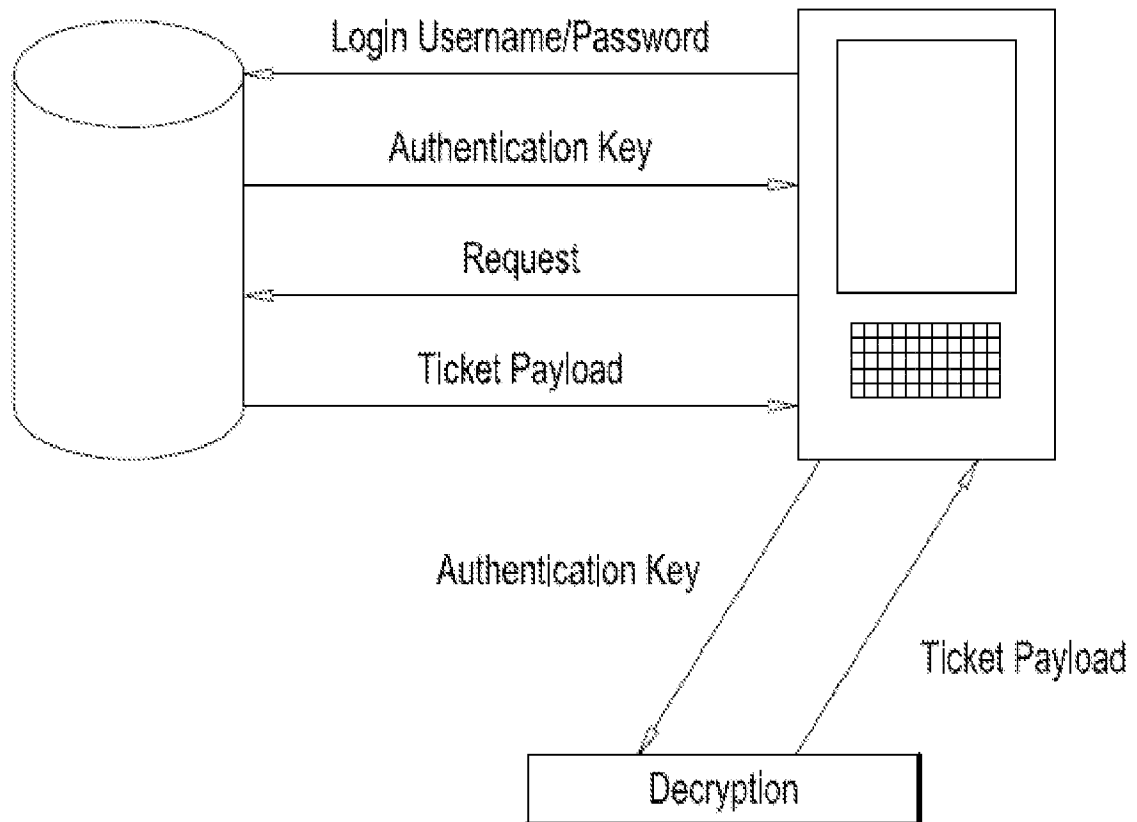


FIG. 12

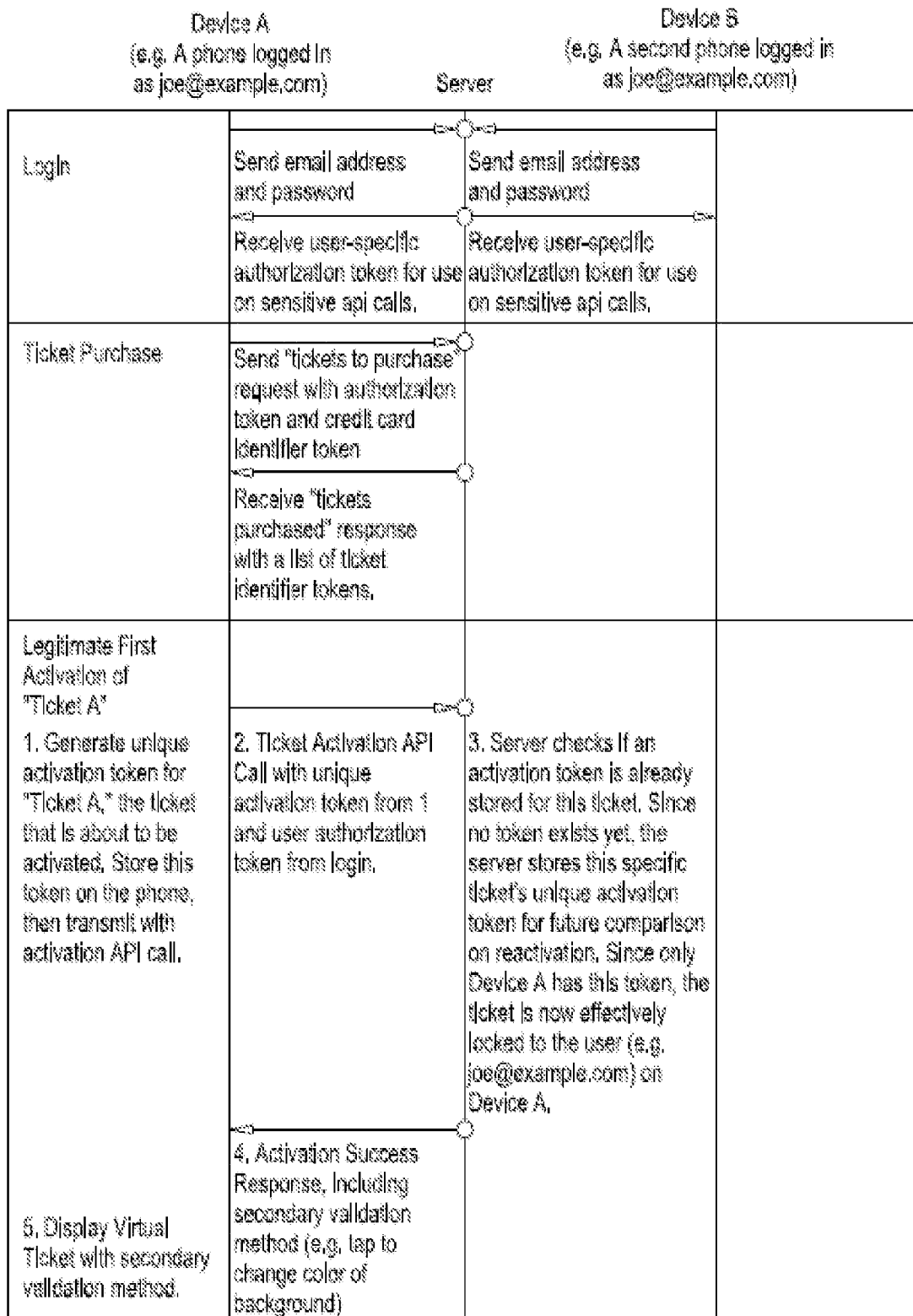


FIG. 13

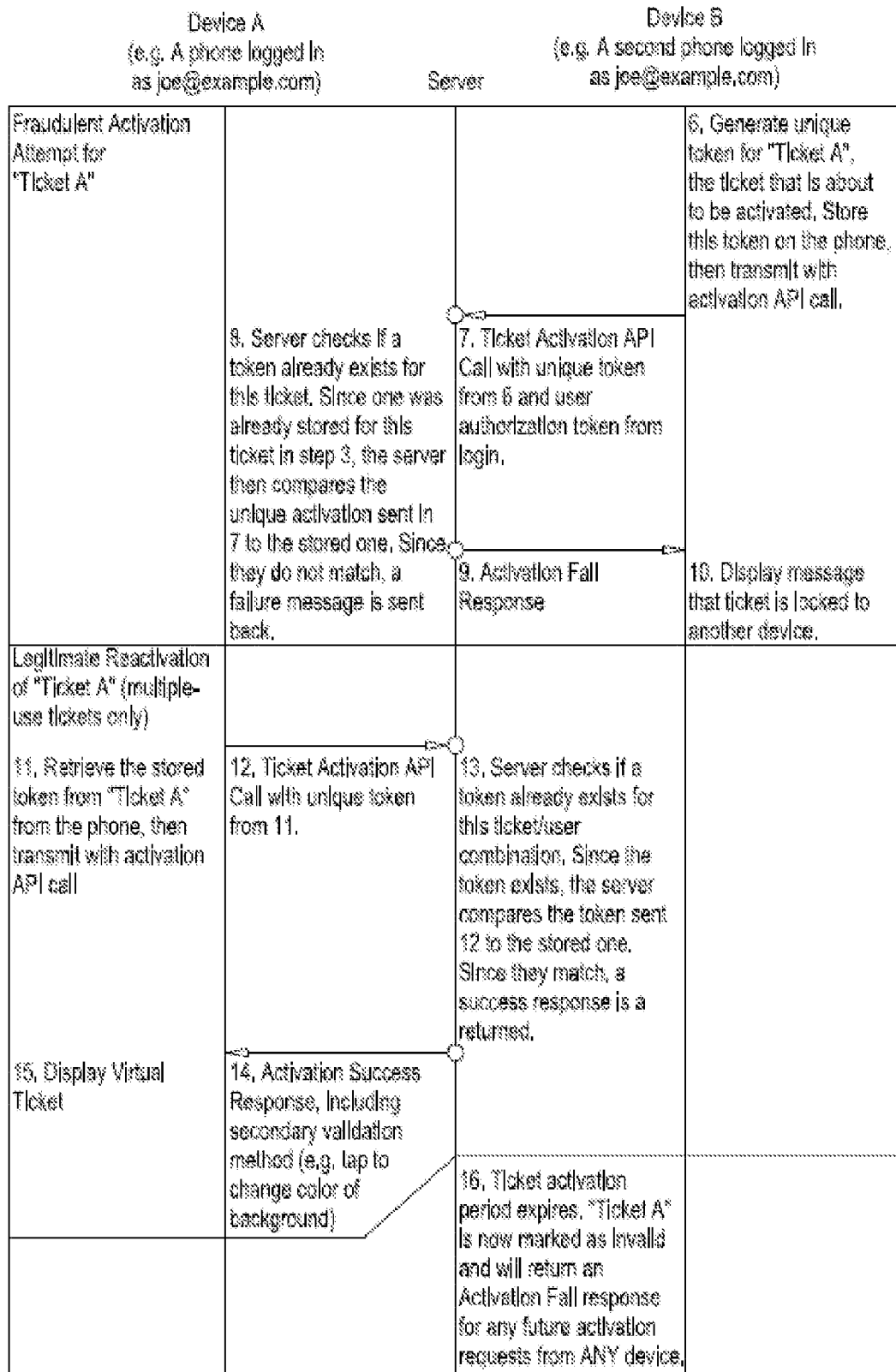


FIG. 14

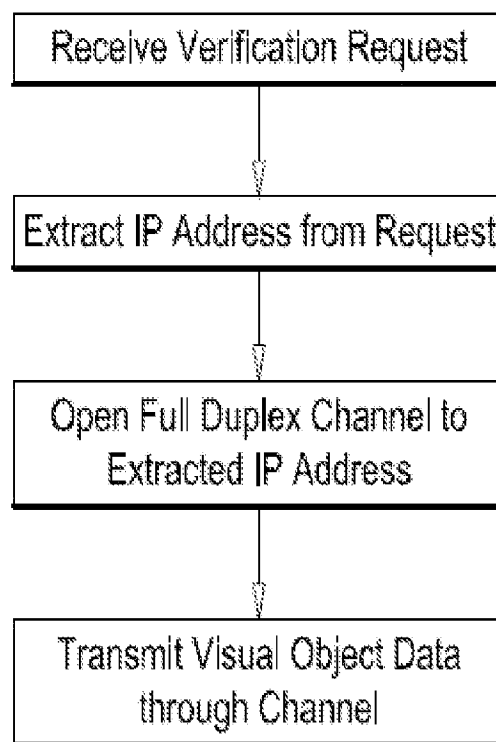


FIG. 15

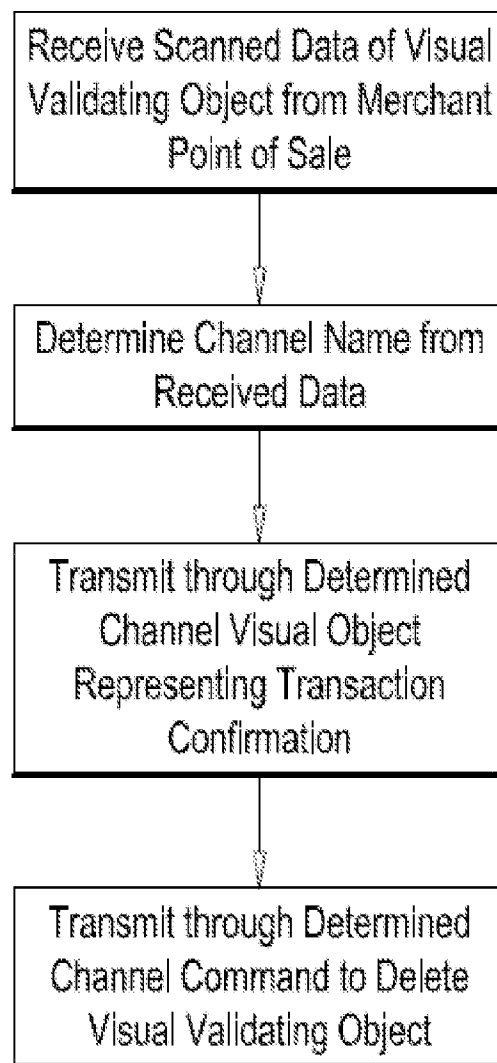


FIG. 16

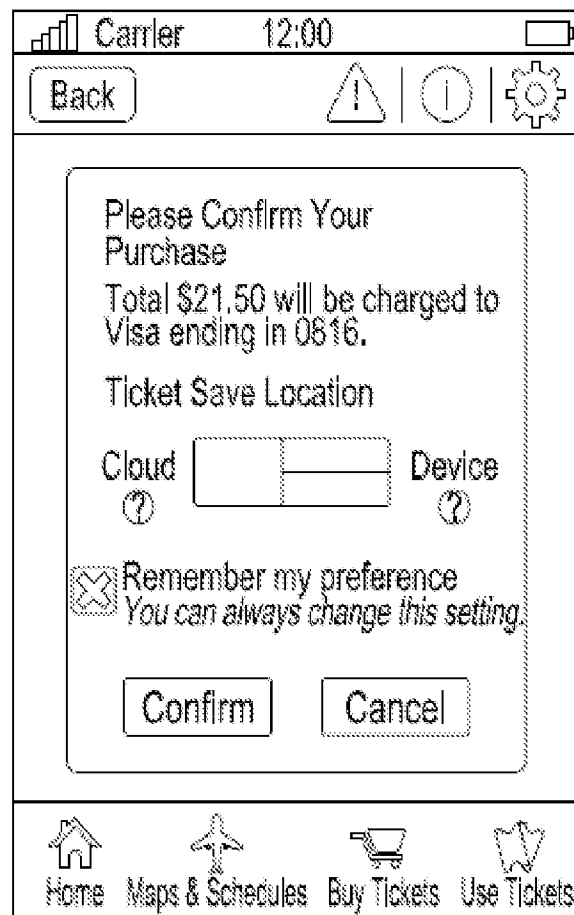


FIG. 17

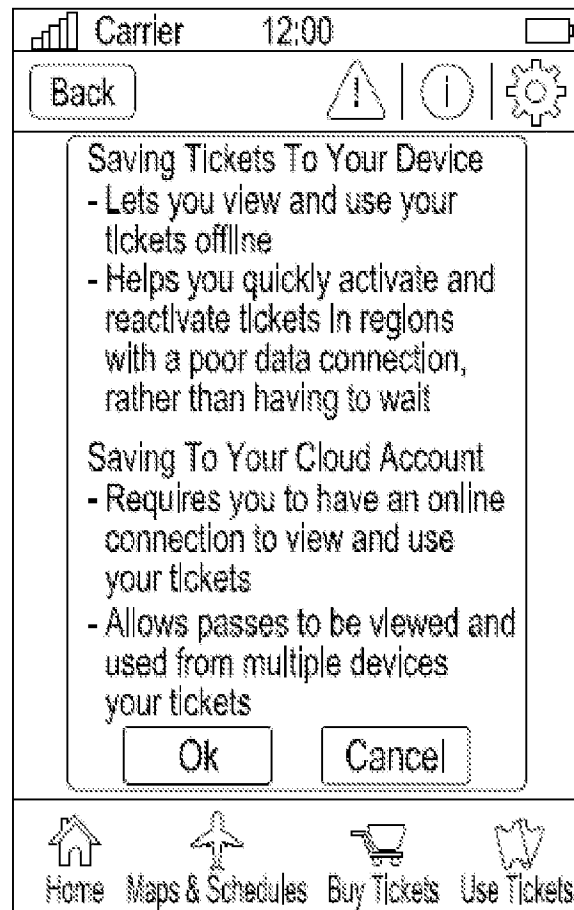


FIG. 18

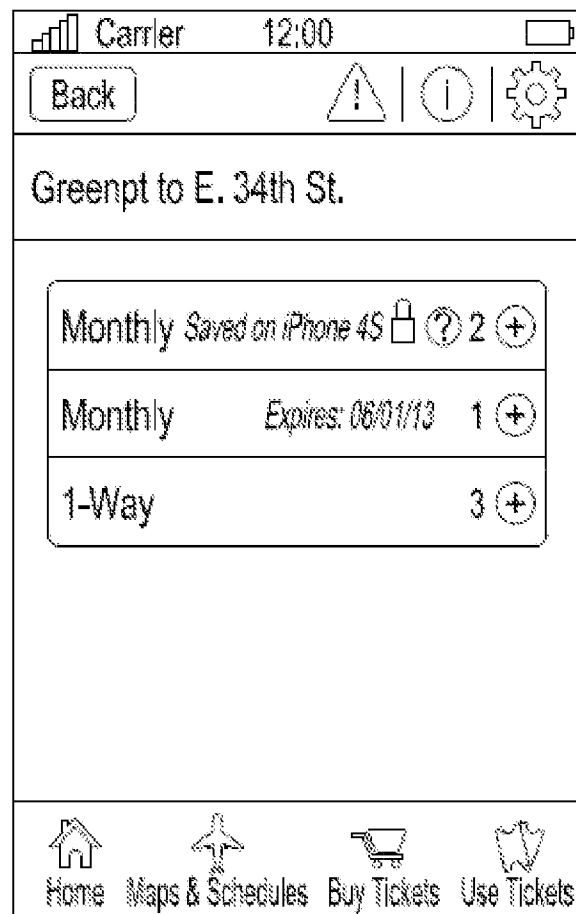


FIG. 19

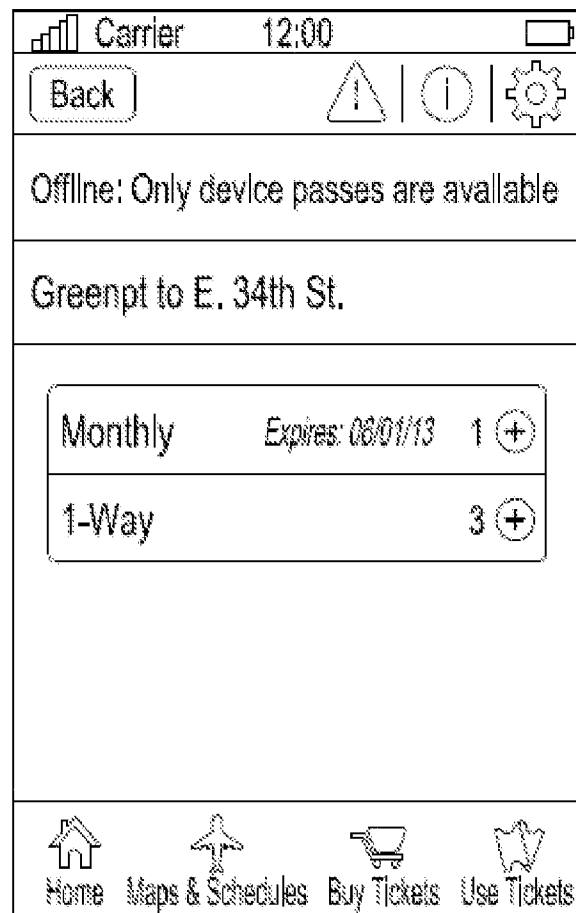


FIG. 20

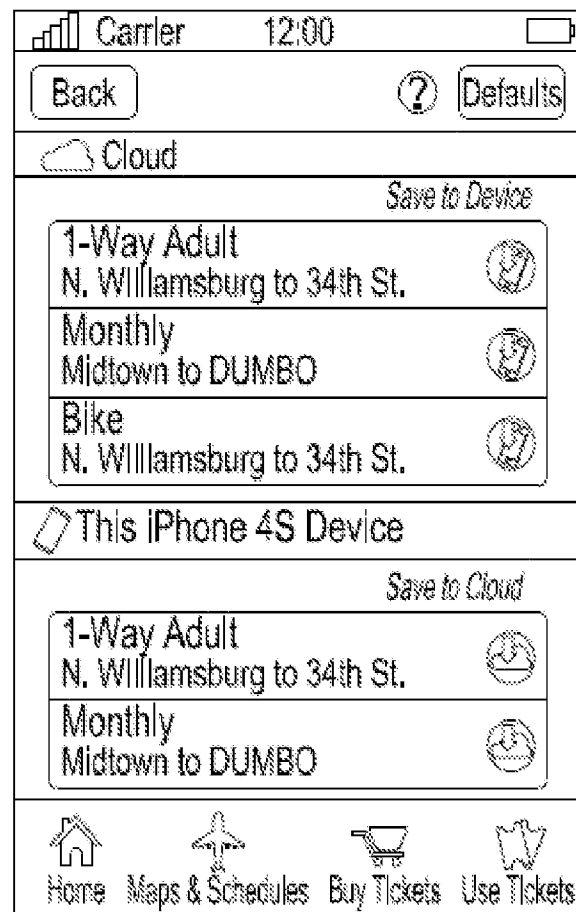


FIG. 21

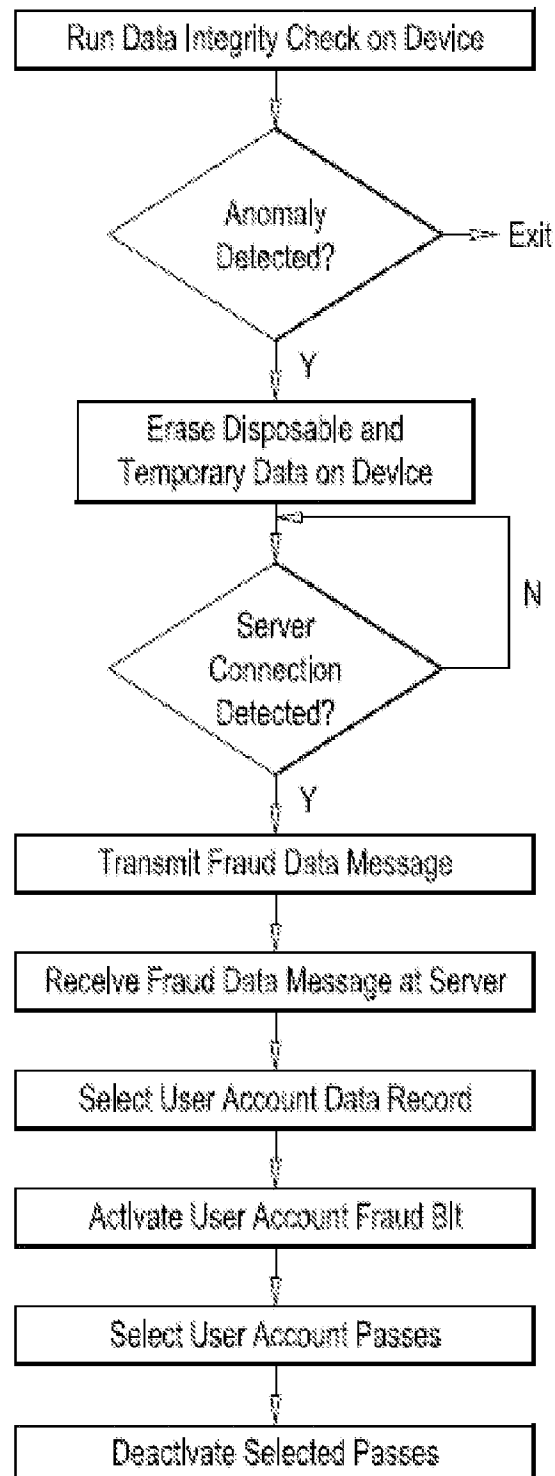


FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US14/39393

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G07B 11/02; H04L 9/08; G06Q 10/02 (2014.01)

CPC - H04W 12/04; H04L 9/32; G06Q 20/045

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)

IPC (8): G07B 11/02; H04L 9/08; G06Q 10/02; G06F 21/30; H04L 9/34; H04W 12/12; G06Q 20/32; G07B 11/11; G11C 16/14 (2014.01)

CPC: H04W 12/04; H04L 9/32; G06Q 20/045; H04L 63/083; H04L 9/06; USPC: 705/64,78; 380/277; 713/178

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)

MicroPatent(US-G US-A EP-A EP-B WO JP-bib, DE-G, DE-A, DE-T, DE-U, GB-A, FR-A); ProQuest; IEEE; Google Scholar;

KEYWORDS: secure, mobile, user, device, ticketing, eticket, authentication, detect, integrity, infraudulent, pass, password, account, transfer, erase, bit, flag

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2003/0229790 A1 (RUSSELL, WC) 11 December 2003; figure 1; paragraphs [0023], [0026], [0037], [0040]-[0044].	1-5 ----- 6-16
Y	US 5621797 A (ROSEN, S et al.) 15 April 1997; figures 2-4A, 5, 23, 25; column 6, lines 42-47; column 7, lines 50-60; column 8; lines 43-49; column 13, lines 1-21; column 14, lines 28-48; column 15, lines 1-27; column 18, lines 30-45; column 25, lines 17-40; column 26, lines 25-30.	6-16
Y	US 7263506 B2 (LEE, WW et al.) 28 August 2007; figures 2, 4; table 3; column 7, lines 60-65; column 8, lines 1-4; column 38, lines 54-60.	15-16
Y	US 2011/0040585 A1 (ROXBURGH, D et al.) 17 February 2011; paragraph [0010].	7
A	US 2004/0030658 A1 (CRUZ, CS) 12 February 2004, entire document.	1-16
A	US 2002/0040346 A1 (KWAN, KH) 04 April 2002, entire document.	1-16

☐ Further documents are listed in the continuation of Box C.

* 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

20 September 2014 (20.09.2014)

Date of mailing of the international search report

17 OCT 2014

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Shane Thomas

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774