US 20120091202A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2012/0091202 A1

(43) Pub. Date: Apr. 19, 2012

Cohen et al.

(54) **MOBILE APPLICATION BAR CODE IDENTIFICATION METHOD AND SYSTEM**

(75) Inventors: **Benjamin Charles Cohen**, Cedar Park, TX (US); **Andrew Michael Rosenbaum**, Mercer Island, WA (US)

(73) Assignee: **FLASH SEATS, LLC**, Cleveland, OH (US)

(21) Appl. No.: **13/340,200**

(22) Filed: **Dec. 29, 2011**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/320,287, filed on Dec. 16, 2002, now Pat. No. 8,131,572, which is a continuation of application No. 09/590,455, filed on Jun. 9, 2000, now Pat. No. 6,496,809.

(60) Provisional application No. 61/432,673, filed on Jan. 14, 2011.

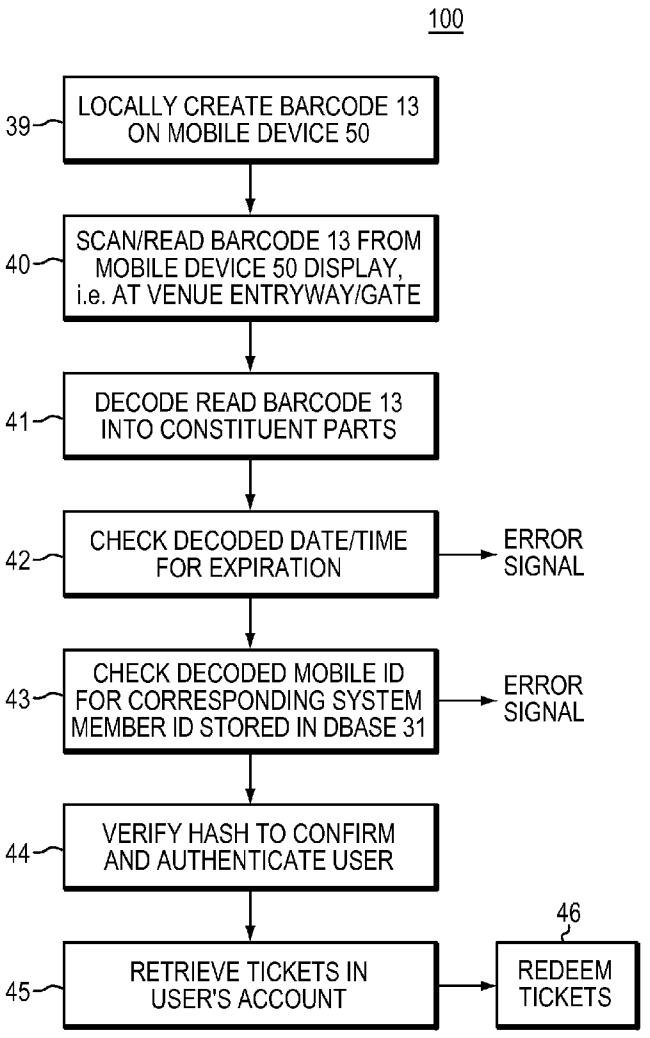
Publication Classification

(51) **Int. Cl.**
G06K 5/00 (2006.01)

(52) **U.S. Cl.** **235/382**

(57) **ABSTRACT**

Applicant's Smartphone application provides ticket-holding patrons an alternative, digital means of verifying personal identification at entry to a venue or event. The Smartphone application periodically generates a unique QR code (bar-code) that contains a unique identifier (i.e., mobile device ID) which prompts the venue/event entry system to recognize the patron. No barcode (serving as a ticket, or authentication/verification, or otherwise) is downloaded from the system server to the Smartphone/mobile device client in contrast to prior art systems.



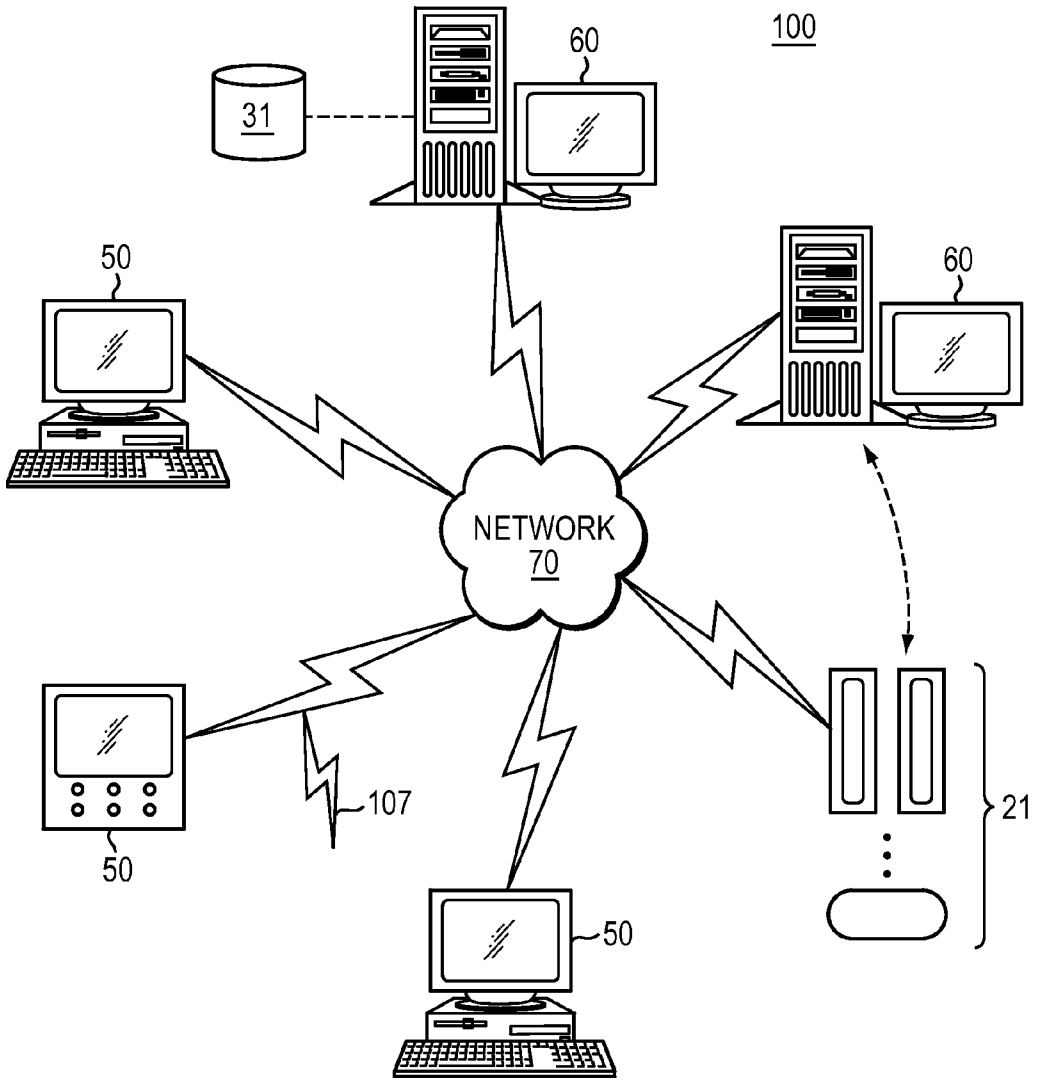


FIG. 1

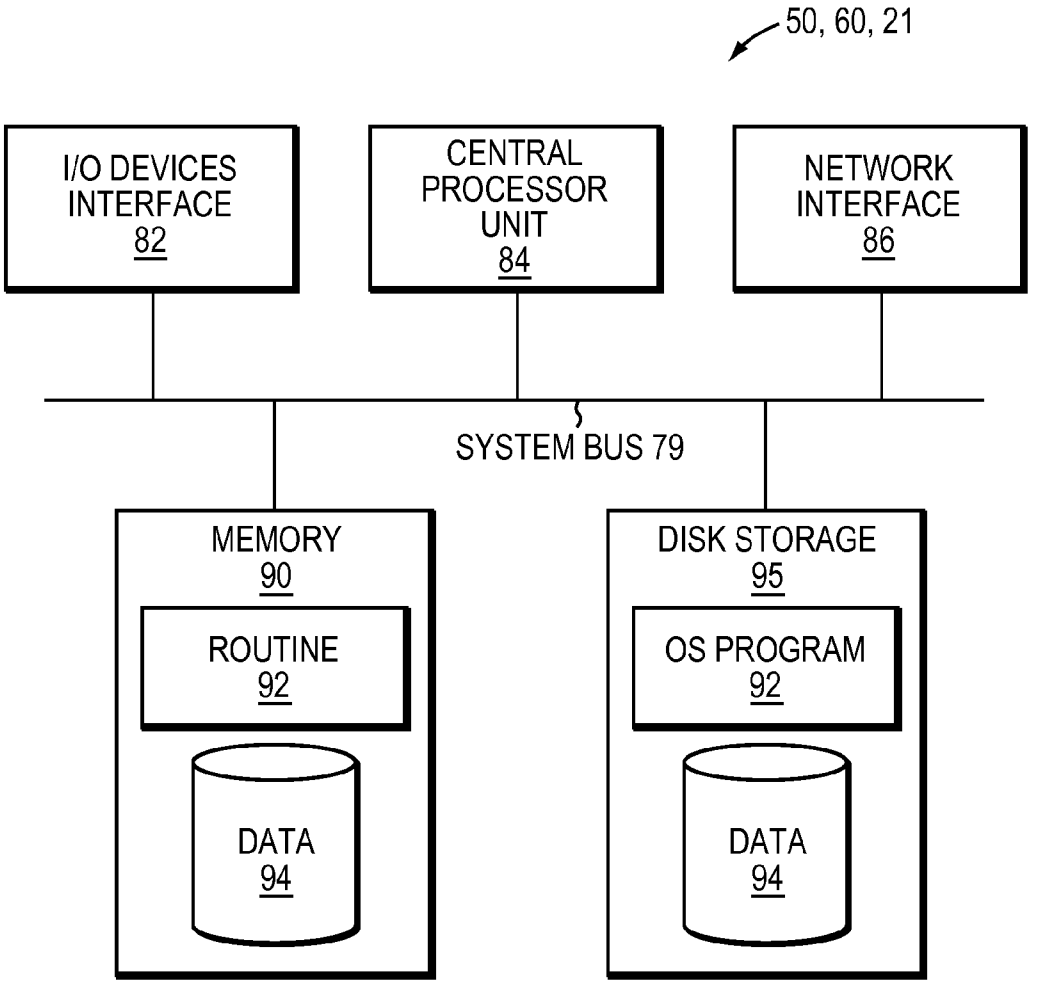

50, 60, 21
I/O DEVICES INTERFACE 82
CENTRAL PROCESSOR UNIT 84
NETWORK INTERFACE 86
SYSTEM BUS 79
MEMORY 90
ROUTINE 92
DATA 94
DISK STORAGE 95
OS PROGRAM 92
DATA 94

FIG. 2

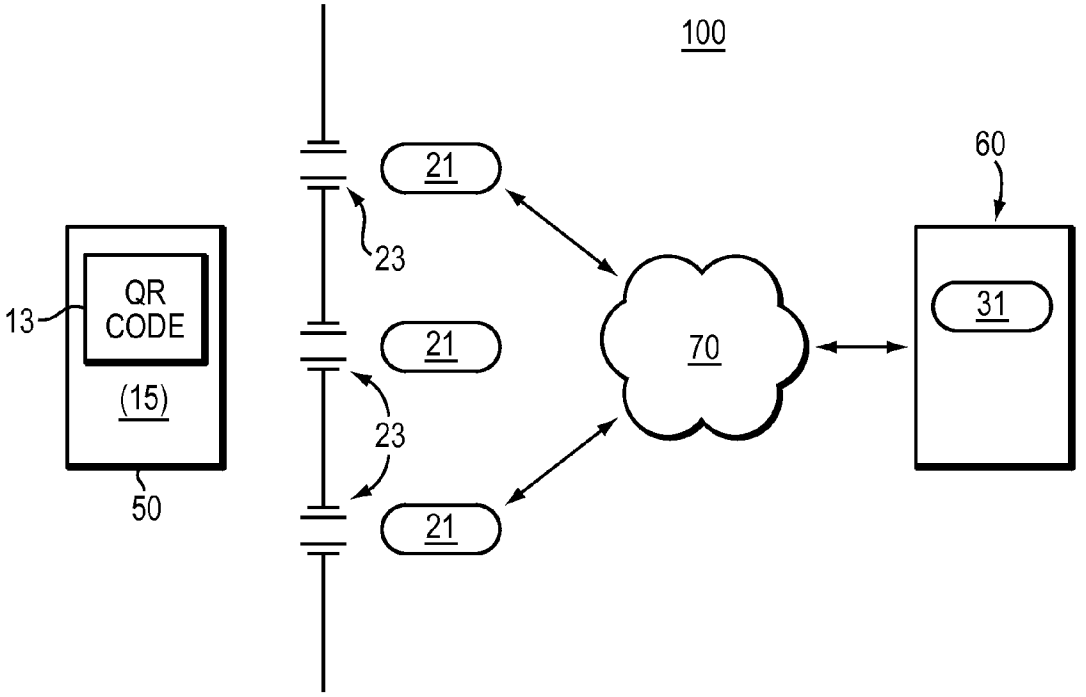


FIG. 3

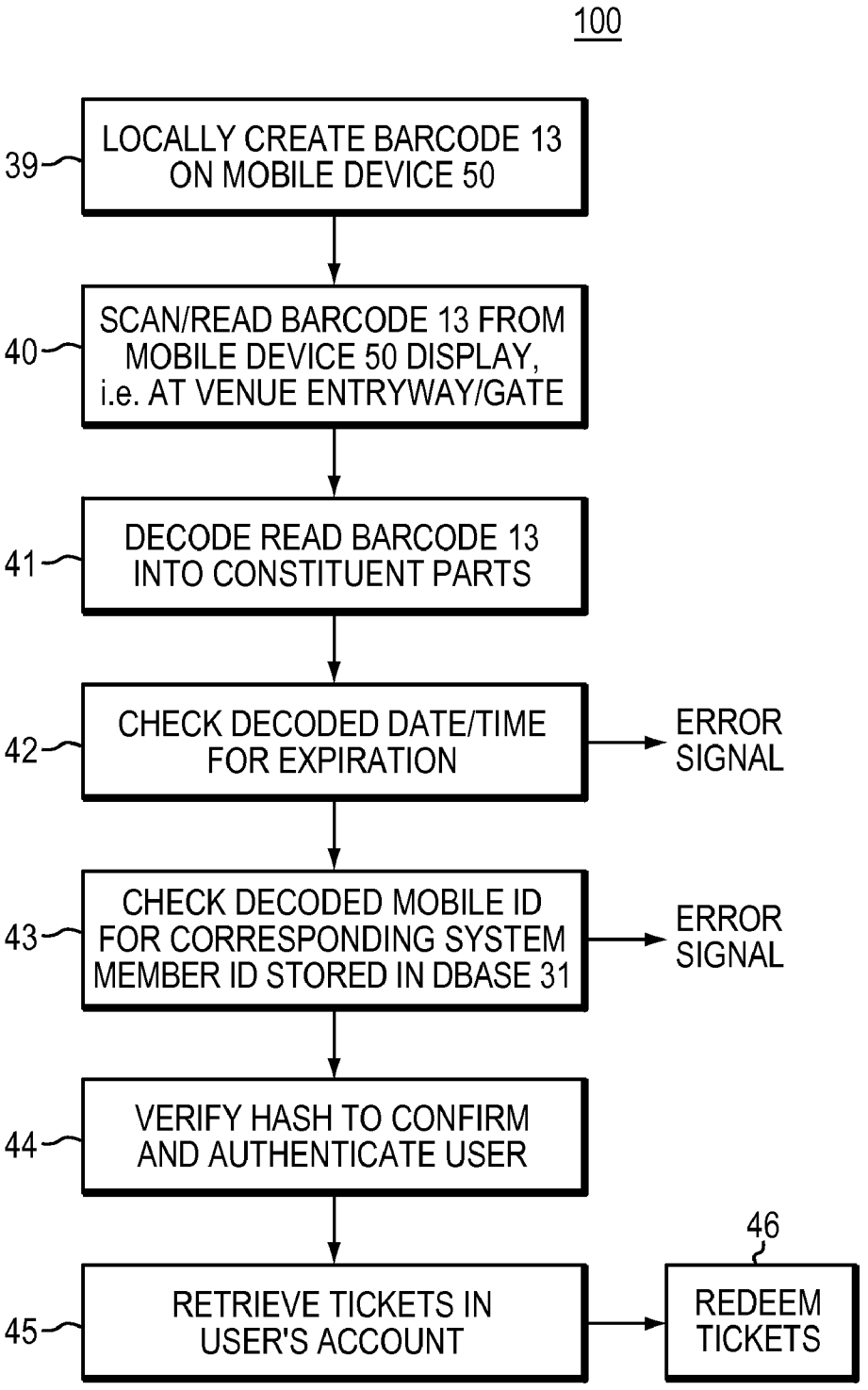

100
39
LOCALLY CREATE BARCODE 13 ON MOBILE DEVICE 50
40
SCAN/READ BARCODE 13 FROM MOBILE DEVICE 50 DISPLAY, i.e. AT VENUE ENTRYWAY/GATE
41
DECODE READ BARCODE 13 INTO CONSTITUENT PARTS
42
CHECK DECODED DATE/TIME FOR EXPIRATION
ERROR SIGNAL
43
CHECK DECODED MOBILE ID FOR CORRESPONDING SYSTEM MEMBER ID STORED IN DBASE 31
ERROR SIGNAL
44
VERIFY HASH TO CONFIRM AND AUTHENTICATE USER
45
RETRIEVE TICKETS IN USER'S ACCOUNT
46
REDEEM TICKETS

FIG. 4

MOBILE APPLICATION BAR CODE IDENTIFICATION METHOD AND SYSTEM

RELATED APPLICATIONS

[0001] The following claims the benefit of U.S. Provisional Application No. 61/432,673 filed Jan. 14, 2011. The following is also a continuation-in-part application of U.S. patent application Ser. No. 10/320,287 filed on Dec. 16, 2002 which is a continuation of U.S. patent application Ser. No. 09/590,455 filed Jun. 9, 2000 (now U.S. Pat. No. 6,496,809 issued Dec. 17, 2002).

[0002] The teachings of these prior applications are herein incorporated in their entireties.

BACKGROUND OF THE INVENTION

[0003] Common barcode technology is based on a laser emitting diode emitting a laser onto a subject barcode pattern and a reader reading the resulting reflected wave. This technology is unable to read barcodes displayed on PDA/mobile device screens or other liquid crystal displays. See Wu, et al., U.S. Patent Application Publication No. 2004/0035925, published Feb. 26, 2004 providing an image processing system for reading barcodes scanned from PDA/cell phone screens.

[0004] Yet other systems deliver barcodes to and render the downloaded bar codes on display units of mobile devices. Examples include:

[0005] U.S. Pat. No. 6,685,093 to Challa, et al for "System, Method and Apparatus for Communicating Information Between a Mobile Communications Device and a Bar Code Reader";

[0006] U.S. Pat. No. 7,693,744 to Forbes for "Optimised Messages Containing Barcode Information for Mobile Receiving Devices"; and

[0007] U.S. Patent Application Publication No. 2003/0047613 by Funamoto, et al. for "Identification Barcode Assigning Method, Identity Verifying Method, Identification Barcode Assigning Device, Identity Verifying Device and Portable Terminal Device" which generates an identification barcode of a customer per store or event (i.e., serves as a concert/event ticket).

SUMMARY OF THE INVENTION

[0008] With the present invention, Applicant's provide improvements and advantages over the prior art. In embodiments, the present invention locally creates, i.e., generates anew, at the mobile device a barcode display uniquely identifying a person (the holder/bearer of the mobile device).

[0009] The mobile device may be any of a personal digital assistant (PDA), mobile phone, or other hand held digital processing and/or communications device. In a preferred embodiment, the mobile device is a so called smartphone by way of example and not limitation.

[0010] Applicant's smartphone application provides ticket-holding patrons an alternative, digital means of verifying personal identification at entry to a venue or event. The smartphone application periodically generates a unique QR code (barcode) that contains a unique identifier (i.e., mobile device ID) which prompts the venue/event entry system to recognize the patron. No barcode (serving as a ticket, or otherwise) is downloaded from the system server to the smartphone/mobile device client in contrast to prior art systems.

[0011] In a preferred embodiment, a computer-based method electronically authenticates a person (e.g., patron) at a venue or event entry, or otherwise. The person may be a patron, especially an account holding patron. To that end the method electronically verifies a person as an account holding patron/customer and electronically accesses patron account. The preferred method includes electronically storing in a database an indication of a mobile device user and an indication of a certain mobile device for that user.

[0012] The database is operatively coupled to venue or event entry subsystem. The subsystem may include turnstiles and/or gates, especially those that are electronically controlled and operated.

[0013] Next in the preferred embodiment, the method executes a code generating program on the certain mobile device. In turn, the mobile device locally creates and displays a bar code unique to the mobile device user. The bar code is not based on data solely driven by the venue or event such as, location name, address, event title, performance name, event session/showing, etc. In this way, the bar code is independent of venue data and event data.

[0014] At the venue or event entry subsystem, the mobile device user displays the locally created bar code on the certain mobile device. In response, the method: (a) electronically reads the bar code from the certain mobile device, (b) electronically decodes the bar code into a first indicator portion indicating mobile device user and a second indicator portion indicating mobile device, and (c) electronically accesses the database and compares the decoded first indicator portion to the database stored indication of the mobile device user and compares the decoded second indicator portion to the database stored indication of the certain mobile device. Where the comparing results in a match of the first indicator portion to the database stored indication of the mobile device user and a match of the second indicator portion to the database stored indication of the certain mobile device, the method automatically positively authenticates the mobile device user at the venue or event entry. This may include opening, unlocking or otherwise allowing the mobile device user to pass through the gate or turnstile of the venue or event entry subsystem.

[0015] In some embodiments, the database also stores user account information. For each user account, the database stores an indication of one mobile device of (associated with) the person (user) holding the account. Restated, per user account, an indication of the mobile device user (person holding the account) is associated with an indication of his certain mobile device in the database. Also in embodiments, the database per user account, stores ticket information of one or more tickets owned by the mobile device user (person who holds account). However, the venue or event entry subsystem authenticates identity of the mobile device user as an individual at the venue or event entry separate from and independent of authenticating him as a specific ticket holder (having tickets to a specific event).

[0016] The locally created bar code uniquely identifies the mobile device user that is the account holding person/patron/customer. The bar code is not based on data solely driven by the venue or event such as location name, location address, event title, performer name, event session or showing and the like. Instead the bar code is independent of event data and venue data.

[0017] After positively authenticating the mobile device user at the venue or event entry, the venue or event entry subsystem further (a) retrieves ticket information from the

database, and (b) allows or otherwise enables the authenticated mobile device user to redeem one or more tickets and gain entry to the venue/event.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] The foregoing will be apparent from the following more particular description of example embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating embodiments of the present invention.

[0019] FIG. **1** is a schematic view of a computer network environment in which embodiments of the present invention are deployed.

[0020] FIG. **2** is a block diagram of a computer node of the network of FIG. **1**.

[0021] FIG. **3** is a schematic diagram of a preferred embodiment.

[0022] FIG. **4** is a flow diagram of a venue entry sub system of the FIG. **3** embodiment.

DETAILED DESCRIPTION OF THE INVENTION

[0023] A description of example embodiments of the invention follows.

[0024] The teachings of all patents, published applications and references cited herein are incorporated by reference in their entirety.

[0025] FIG. **1** illustrates a computer network or similar digital processing environment in which the present invention may be implemented.

[0026] Client computer(s)/mobile devices **50** and server computer(s) **60** provide processing, storage, and input/output devices executing application programs and the like. Client computer(s)/devices **50** can also be linked through communications network **70** to other computing devices, including other client devices/processors **50** and server computer(s) **60**. Similarly, other supplemental processing or reading devices **21** may be operatively linked to server computers **60** through communications network **70**. Communications network **70** can be part of a remote access network, a global network (e.g., the Internet), a worldwide collection of computers, Local area or Wide area networks, and gateways that currently use respective protocols (TCP/IP, Bluetooth, etc.) to communicate with one another. Other electronic device/computer network architectures are suitable.

[0027] FIG. **2** is a diagram of the internal structure of a computer (e.g., client processor/device **50** or server computers **60** including supplemental devices **21**) in the computer system **100** of FIG. **1**. Each computer **50**, **60**, **21** contains system bus **79**, where a bus is a set of hardware lines used for data transfer among the components of a computer or processing system. Bus **79** is essentially a shared conduit that connects different elements of a computer system (e.g., processor, disk storage, memory, input/output ports, network ports, etc.) that enables the transfer of information between the elements. Attached to system bus **79** is I/O device interface **82** for connecting various input and output devices (e.g., keyboard, mouse, displays, printers, speakers, etc.) to the computer **50**, **60**, **21**. Network interface **86** allows the computer to connect to various other devices attached to a network (e.g., network **70** of FIG. **1**). Memory **90** provides volatile storage for computer software instructions **92** and data **94** used to implement an embodiment of the present invention (e.g., mobile device application **15** including QR code generation, client/server hashing, database management **31** and supporting code detailed below). Disk storage **95** provides non-volatile storage for computer software instructions **92** and data **94** used to implement an embodiment of the present invention. Central processor unit **84** is also attached to system bus **79** and provides for the execution of computer instructions.

[0028] In one embodiment, the processor routines **92** and data **94** are a computer program product (generally referenced **92**), including a computer readable medium (e.g., a removable storage medium such as one or more DVD-ROM's, CD-ROM's, diskettes, tapes, non-transient storage, etc.) that provides at least a portion of the software instructions for the invention system. Computer program product **92** can be installed by any suitable software installation procedure, as is well known in the art. In another embodiment, at least a portion of the software instructions may also be downloaded over a cable, communication and/or wireless connection. In other embodiments, the invention programs are a computer program propagated signal product **107** embodied on a propagated signal on a propagation medium (e.g., a radio wave, an infrared wave, a laser wave, a sound wave, or an electrical wave propagated over a global network such as the Internet, or other network(s)). Such carrier medium or signals provide at least a portion of the software instructions for the present invention routines/program **92**.

[0029] In alternate embodiments, the propagated signal is an analog carrier wave or digital signal carried on the propagated medium. For example, the propagated signal may be a digitized signal propagated over a global network (e.g., the Internet), a telecommunications network, or other network. In one embodiment, the propagated signal is a signal that is transmitted over the propagation medium over a period of time, such as the instructions for a software application sent in packets over a network over a period of milliseconds, seconds, minutes, or longer. In another embodiment, the computer readable medium of computer program product **92** is a propagation medium that the computer system **50** may receive and read, such as by receiving the propagation medium and identifying a propagated signal embodied in the propagation medium, as described above for computer program propagated signal product.

[0030] Generally speaking, the term "carrier medium" encompasses the foregoing transient signals, propagated signals, propagated medium, storage medium, non-transient medium and the like.

[0031] Turning to FIG. **3**, a preferred smartphone **50** embodiment is illustrated. It is understood that other mobile devices **50** with similar applications program **15** are suitable.

[0032] Applicant's smartphone application **15** provides ticket-holding patrons an alternative, digital means of verifying personal identification at entry to events. The smartphone application **15** periodically generates (locally creates) a unique QR code **13** (in barcode format) that contains a unique identifier (i.e. Mobile ID) which prompts the system **100** to recognize the customer.

[0033] QR Code Content

[0034] The QR code **13** locally created and generated by the mobile application **15** contains a unique identifier (or iPhoneMD5 for example) consisting of the customer's sys-

tem Member ID, Mobile ID and Coordinated Universal Time (UTC) date/time. Application **15** presents (outputs) the QR code **13** in barcode format.

[0035] At a venue entryway or other electronically controlled (automated) gate subsystem **23**, a scanner/reading device **21** hashes the system Member ID, Mobile ID and UTC date/time information from the QR code (barcode) **13** in the following manner: MemberID+MobileID+UTCdate/time+Md5Hash[MemberID+MobileID+UTCdate/time] where:

[0036] MemberID is a 64 bit integer using the first six digits from a customer's unique system Member ID (e.g. 999999),

[0037] MobileID is a 64 bit integer generated by the system server **60** and communicated to mobile application **15** or otherwise input/defined in application **15**. The Mobile ID is tied directly to the customer's mobile device **50** such that the customer can only have one system account tied to one mobile device (e.g. 9999990000000119). Server **60** stores in database **31**, per customer, his system Member ID, his corresponding Mobile ID and ticket data of his purchased tickets.

[0038] UTC date/time is Universal Time and Date (year, month, day followed by hour, minutes, seconds e.g. 2010-08-05 14:56:33 encoded as 20100805145633). In one embodiment, the mobile application **15** locally generates a unique date/time code every 60 seconds. Other frequencies of date/time code generation are suitable.

[0039] Md5Hash is a one-way encryption of MemberID+MobileID+UTCdate/time.

[0040] System **100** Setup

[0041] Continuing with FIGS. **1** and **3**, database **31** may be a relational or other configured datastore. It is understood that various system and network architectures of mobile devices **50** running application **15**, server **60** having database **31** and cooperating venue entry subsystems **23**, **21** are suitable. For example, a web server **60** with database **31** supports various and numerous venues, ticketing agents/distributors, brokers and so on across plural team sports, entertainment performers and the like, including for example but not limited to ticketing for games, concerts, presentations and live performances. Web server **60** with database **31** may be remote from venue servers **60** which are local to respective venues. The web server **60** and venue servers **60** (together with venue subsystem **23** and reader/scanners **21**) may be operatively coupled for communication and processing as a WAN (wide area network), LAN (local area network), or other working computer network over a cable network, the Internet, an extranet or the like. Thus, web server **60** and venue servers **60** are generically referred to as server **60** herein.

[0042] In embodiments, server **60** maintains database **31**. As new customers/patrons of participating venues become system **100** members, server **60** assigns respective unique system Member ID and records the same in database **31**. As mentioned above, each customer may 'register' (i.e., indicate to system **100**/server **60**) one mobile device **50** to correspond to or be associated with the customer's system account. Server **60** assigns and records in database **31** a unique Mobile ID for the customer (his account). The invention mobile application **15** is then configured or parameterized with the system Member ID (at least the first six digits in one embodiment) and the Mobile ID, and ultimately installed on the customer's subject mobile device **50**. To accomplish this, server **60** may download mobile application **15** so configured and parameterized to subject mobile device **50** through communications network **70** or otherwise.

[0043] As a customer purchases tickets to events at the various participating venues through server **60**, system **100**/server **60** records the ticket data accordingly in database **31** (i.e., tallied under the customer's system account). A "ticket" is a contractual right to attend a venue at a certain date and time or for a certain event. The contractual right may be to a certain seat or area in the venue or event. To the extent that an indication of the "ticket" is stored or held electronically, it is an "eticket" or "electronic ticket". Common or known technology is employed, and various techniques for displaying such tickets are suitable.

[0044] Venue Entry

[0045] A mobile device **50** user runs/executes the invention application program **15** on the subject smartphone/mobile device **50**. In turn, the executing application program **15** generates, or more precisely, locally creates the unique QR code (barcode) **13** and displays the same on the display screen/unit of the subject mobile device **50**. Step **39** of FIG. **4** is illustrative. Note, server **60** of the system **100** is not responsible for initially creating this unique bar code **13**; mobile device **50** running application **15** is.

[0046] At the venue gates or entry subsystem **23**, a scanner/reading device **21** scans the QR code (barcode) **13** from the mobile device **50** display screen (Step **40**, FIG. **4**). Scanner/reading device **21** utilizes common or known barcode reading technology and is configured to perform the MD5Hash (or similar hash) as made clear below.

[0047] Once the QR code (barcode) **13** is scanned from the display screen of mobile device **50**, the scanner/reading device **21** in electronic communication with server **60** and database **31** employs a series of checks in order to authenticate the user attempting to gain system account access and hence ticket and venue access. The progression of system **100** checks is as follows and diagrammed in FIG. **4**.

[0048] 1. Scanner/reader device **21** first decodes the contents of read barcode **13** (Step **41**). This results in a Member ID candidate value, Mobile ID candidate value and UTC date/time candidate value.

[0049] 2. Scanner/reader device **21** checks the UTC date/time candidate value to see if the read barcode **13** has expired or otherwise meets threshold date/time ranges as indicated by server **60** (Step **42**). If the date/time has expired, scanner device **21** issues an error message as pertinent.

[0050] 3. Scanner/reader device **21** in communication with server **60** uses the decoded results for MobileID candidate value to find System **100** stored corresponding Member ID in database **31**. Known database look up and/or download techniques are used (Step **43**). Server **60** and/or scanner device **21** issues any error message as pertinent if the Mobile ID candidate value does not properly index into database **31** or a corresponding Member ID is otherwise unable to be found in database **31**.

[0051] 4. If no errors have been produced up to this stage, then Step **44** verifies a hash of read barcode **13** by comparing (a) an MD5 (encrypted) hash of the Member ID candidate value+Mobile ID candidate value+UTC date/time candidate value to (b) MD5Hash encryption of the system Member ID stored in database **31**+corresponding Mobile ID stored in database **31**+UTC date/time candidate value. This effectively authenticates and verifies the subject mobile device **50** user.

[0052] It is understood that Step **44** processing may be performed by and at any combination of the server **60** and scanner/reader device **21**. That is for server **60** processing Step **44**, the server **60** (i) uploads from or otherwise commu-

nicates with the scanner/reader device **21** the read and decoded Member ID candidate value, the Mobile ID candidate value and the UTC date/time candidate value, (ii) utilizes the recently looked-up stored system Member ID and corresponding stored Mobile ID from database **31**, (iii) executes the hash routine on each set of data values and compares the two hash results, and (iv) communicates (downloads) the results of the comparison to scanner/reader device **21**. Where the comparison results in a match, then the user is authenticated (i.e., system verified).

[0053] Alternatively processing may be by or at the scanner/reader device **21** (i) requesting database **31** lookup of the stored Mobile ID corresponding to the system Member ID of Step **43** and obtaining (downloading) the results, and (ii) locally executing the hash routine on the two sets of data values (stored and candidate) and making the comparison of hash results. Where the comparison results in a match, the user is authenticated (i.e., system verified).

[0054] Other configurations of server **60** and/or scanner/reader **21** processing of Step **44** are suitable.

[0055] Where the comparison of hash results do not result in a match, then an error signal or message is provided by the scanner/reader **21**.

[0056] 5. Once Member ID, i.e., mobile device user authentication, is confirmed, scanner/reader device **21** and/or server **60** (step **45**) check for tickets in the user's account as indicated in database **31**. Common database look up using Member ID as an index is employed. The corresponding ticket data for this customer/mobile device user (via Member ID) may be downloaded from server **60** to venue gate subsystem **23** or scanner/reader devices **21**.

[0057] 6. Scanner/reader device **21** and/or venue gate subsystem **23** redeems tickets according to the downloaded ticket data (step **46**).

[0058] Preferably, successful matching of the QR code **13** as read from the user's mobile device **50** and hashed by the scanner/reader device **21** to that of the stored data in database **31**, as described above, may result in venue entry and prompts the scanner device **21** or venue entry subsystem **23** to print the customer's (mobile device **50** user's) seat locators and/or other ticket data. Unsuccessful matches prompt the scanner/reader device **21** or gate subsystem **23** to deny entry and refer the customer (mobile device user) to the venue box office.

[0059] Thus, the locally generated/created barcode **13** at mobile device **50** is not an "electronic ticket" to an event/venue (does not indicate venue and event) but rather is a digital means of verifying customer identity or authenticating a patron individual (bearer of the mobile device). After authentication of the mobile device user is completed, then system **100** considers (retrieves) the pertinent ticket/event data indicated in the user's system account uniquely tied to/associated with the subject mobile device **50**.

[0060] Exemplary

[0061] In an example, non-limiting embodiment of system **100**, web server **60** supports a website for making ticket transactions between patron/customers and ticket agents/distributors/resellers/brokers/venue box offices and the like, across multiple spectator/team sports and live performance-type events. An end user (would be patron/customer) logs on and registers with the website to become a member of system **100**. During registration, the end user states his name, address, email address and a mobile phone number of his mobile device **50** for example. In turn, server **60** creates a user account, assigns a unique Member ID to the end user and assigns a unique Mobile ID for the user indicated mobile device **50**. Also, Server **60** creates a record in data base **31** and stores or otherwise holds therein the newly created user account information (including pertinent user information), unique Member ID and unique Mobile ID corresponding to the end user.

[0062] Further server **60** configures mobile application **15** for use by the end user on his mobile device **50**. In particular, server **60** sets the Mobile ID and Member ID parameters in application **15** and downloads the configured/parameterized application **15** to end user mobile device **50**. The downloading may be accomplished by emailing an application link to the mobile device **50** or other installation techniques know in the art. The end user mobile device **50** equipped with the application **15** is able to create as desired (on user command) bar code **13** uniquely identifying the end user as the account holding member of system **100**, i.e., the registered member corresponding to the respective account.

[0063] As a registered account holding member of system **100**, the end user has access to various ticket offerings and sales through website/web server **60**. In one sample instance, say the end user purchases one or more tickets to an event through the website using a credit card to satisfy the financial aspect of the ticketing transaction. Server **60** records pertinent ticket data in the database **31** record and account of the end user indicting for example, event date/time, venue, title/name of the event, seat/location and amount paid. No paper form of the purchased ticket(s) needs to be mailed, printed from a computer screen display or otherwise provided to the end user.

[0064] On the event day/hour, the end user operates (i.e., executes) the application **15** on his mobile device **50** and creates bar code **13** on the display unit/screen of device **50**. At the venue gate **23**, a scanner/reader **21** scans and reads barcode **13** from end user mobile device **50**. Scanner/reader **21** and/or venue server **60** in communication with web server **60** and database **31** process the read barcode **13** as described in Steps **40-44** of FIG. **4**, and electronically authenticate the end user (i.e., verify his identity as an account holding, registered member of system **100** and not, at this stage, verifying him as a certain ticket holder to the subject event).

[0065] Once the end user is authenticated or verified as a system member (not, at this stage, as a subject event ticket holder) by system **100**, server **60** and scanner/reader **21** access the end user's system account and obtain his ticket/eticket to the event. This may redeem the ticket/eticket and operate gate **23** (turnstiles and the like) to allow passage (entry) of the end user. Scanner/reader **21**, gate **23** or networked printer at the venue may print a ticket receipt, seat information and the like for the end user.

[0066] While this invention has been particularly shown and described with references to example embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.

What is claimed is:

1. A computer-implemented method of electronically authenticating a person at a venue or event entry, comprising:

in a database, electronically storing an indication of a mobile device user, including indicating a certain mobile device for that user, the database being operatively coupled to a venue or event entry subsystem;

executing a code generating program on the certain mobile device such that the mobile device locally creates and displays a bar code unique to the mobile device user, the bar code being independent of venue and event data; and

at the venue or event entry subsystem, with the mobile device user displaying the locally created bar code on the certain mobile device: (a) electronically reading the bar code from the certain mobile device, (b) electronically decoding the bar code into a first indicator portion indicating mobile device user and a second indicator portion indicating mobile device, and (c) electronically accessing the database and comparing the decoded first indicator portion to the database stored indication of the mobile device user and comparing the decoded second indicator portion to the database stored indication of the certain mobile device,

wherein the comparing resulting in a match of the first indicator portion to the database stored indication of the mobile device user and a match of the second indicator portion to the database stored indication of the certain mobile device, then automatically positively authenticating the mobile device user at the venue or event entry.

2. A method as claimed in claim **1** wherein the method authenticates a person who is an account holding patron, the mobile device user being the person holding the account; and

the database stores account information, including for each account, the database stores an indication of one mobile device associated with the person holding the account.

3. A method as claimed in claim **2** wherein:

per account the database stores ticket information of one or more tickets owned by the mobile device user; and

the venue or event entry subsystem further (d) retrieves ticket information after positively authenticating the mobile device user at the venue or event entry, and (e) allows the mobile device user to redeem one or more tickets.

4. A method as claimed in claim **1** wherein the venue or event entry subsystem includes a gate or turnstile, and

the step of automatically positively authenticating the mobile device user further includes allowing the mobile device user to pass through the gate or turnstile.

5. A method as claimed in claim **1** wherein the certain mobile device is any of a mobile phone, a PDA, a smartphone and a handheld digital processing device.

6. A method as claimed in claim **1** wherein the comparing resulting in said match automatically authenticates identity of the mobile device user as an individual at the venue or event entry separate from and independent of authenticating him as a specific ticket holder.

7. A method as claimed in claim **1** further comprising:

after said authenticating the mobile device user at the venue or event entry, obtaining from the database ticket data of said user; and

redeeming a ticket of said user.

8. An electronic authentication apparatus electronically authenticating a person at a venue or event entry, comprising:

a computer database electronically storing an indication of a mobile device user, including indicating a certain mobile device for that user, the database being operatively coupled to a venue or event entry subsystem;

a code generation member executed on the certain mobile device such that the mobile device locally creates and displays a barcode unique to the mobile device user, the barcode being independent of venue and event data; and

the venue or event entry subsystem, with the mobile device user displaying the locally created barcode on the certain mobile device: (a) electronically reading the barcode from the certain mobile device, (b) electronically decoding the barcode into a first indicator portion indicating mobile device user and a second indicator portion indicating mobile device, and (c) electronically accessing the database and comparing the decoded first indicator portion to the database stored indication of the mobile device user and comparing the decoded second indicator portion to the database stored indication of the certain mobile device,

wherein the comparing resulting in a match of the first indicator portion to the database stored indication of the mobile device user and a match of the second indicator portion to the database stored indication of the certain mobile device, then the venue or event entry subsystem automatically positively authenticating the mobile device user at the venue or event entry.

9. Apparatus as claimed in claim **8**, wherein the venue or event entry subsystem authenticates a person who is an account holding patron, the mobile device user being the person holding the account; and

the database stores account information, including for each account, the database stores an indication of one mobile device associated with the person holding the account.

10. Apparatus as claimed in claim **9**, wherein:

per account, the database stores ticket information of one or more tickets owned by the mobile device user; and

the venue or event entry subsystem further: (d) retrieves ticket information after positively authenticating the mobile device user at the venue or event entry, and (e) allows the mobile device user to redeem one or more tickets.

11. Apparatus as claimed in claim **8**, wherein the venue or event entry subsystem includes a gate or turn-style, and the venue or event entry subsystem, after automatically positively authenticating the mobile device user, further allows the mobile device user to pass through the gate or turn-style.

12. Apparatus as claimed in claim **8**, wherein the certain mobile device is any of a mobile phone, a PDA, a smartphone and a hand-held digital processing device.

13. Apparatus as claimed in claim **8**, wherein the venue or event entry subsystem further authenticates identity of the mobile device user as an individual at the venue or event entry separate from and independent of authenticating him as a specific ticket holder.

14. Apparatus as claimed in claim **8**, wherein the venue or event entry subsystem further, after said authenticating the mobile device user at the venue or event entry, obtains from the database ticket data of said user; and

redeems a ticket of said user.

15. A computer-based electronic authentication system electronically authenticating a person at a venue or event entry, comprising:

a computer database electronically storing an indication of a mobile device user, including indicating a certain mobile device for that user;

a venue or event entry subsystem operatively coupled to the database, the subsystem: (a) electronically reading a locally created bar code on the certain mobile device, the certain mobile device executing a code generation program and locally creating and displaying the bar code, the bar code being unique to the mobile device user, and

the barcode being independent of venue and event data, (b) electronically decoding the barcode into a first indicator portion indicating mobile device user and a second indicator portion indicating mobile device, and (c) electronically accessing the database and comparing the decoded first indicator portion to the database stored indication of the mobile device user and comparing the decoded second indicator portion to the database stored indication of the certain mobile device,

wherein the comparing resulting in a match of the first indicator portion to the database stored indication of the mobile device user and a match of the second indicator portion to the database stored indication of the certain mobile device, then the venue or event entry subsystem automatically positively authenticates the mobile device user at the venue or event entry.

* * * * *