

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

ALAN AMRON, Pro se

PLAINTIFF,

vs.

Civil Action No.

**COMPLAINT FOR PATENT INFRINGEMENT
JURY TRIAL DEMANDED**

MAJOR LEAGUE BASEBALL, MLB
ADVANCED MEDIA L.P.,
AZPB LIMITED PARTNERSHIP,
ATLANTA NATIONAL LEAGUE
BASEBALL CLUB, LLC,
BALTIMORE ORIOLES LIMITED
PARTNERSHIP,
BOSTON RED SOX BASEBALL CLUB
LIMITED PARTNERSHIP,
CHICAGO CUBS BASEBALL CLUB,
LLC,
CHICAGO WHITE SOX, LTD.,
THE CINCINNATI REDS LLC,
CLEVELAND GUARDIANS
BASEBALL COMPANY, LLC,
COLORADO ROCKIES BASEBALL
CLUB, LTD.,
DETROIT TIGERS, INC.,
HOUSTON ASTROS, LLC,
KANSAS CITY ROYALS BASEBALL
CLUB, LLC,
ANGELS BASEBALL LP,
LOS ANGELES DODGERS LLC,
MARLINS TEAMCO, LLC,
MILWAUKEE BREWERS BASEBALL
CLUB, LIMITED PARTNERSHIP,
MINNESOTA TWINS, LLC,
STERLING METS, L.P.,
NEW YORK YANKEES
PARTNERSHIP,
ATHLETICS INVESTMENT GROUP,
LLC,
THE PHILLIES,
PITTSBURGH ASSOCIATES,
PADRES L.P.,
THE BASEBALL CLUB OF SEATTLE,
LLLP,
ST. LOUIS CARDINALS, LLC,
RAYS BASEBALL CLUB, LLC,

RANGERS BASEBALL LLC,
ROGERS BLUE JAYS BASEBALL
PARTNERSHIP,
WASHINGTON NATIONALS AND
BASEBALL CLUB, LLC.

DEFENDANTS.

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Alan Amron inventor (“AA” or “Plaintiff”), for his Complaint against Defendants Major League Baseball, et al. (“MLB”) alleges the following:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*

THE PARTIES

2. Plaintiff Alan Amron (AA) is retired 75-year-old inventor with a residence at 103 Jessup Avenue box 354, Quogue, New York 11959.

3. On information and belief, the Defendants Major League Baseball et al. (MLB) are companies with a main place of business at 1271 Avenue of the Americas New York N.Y. 10020, and can be served through its representing agent Alan E. Littmann, Esq. of the law firm Goldman Ismail et al. located at 200 South Wacker Drive Chicago, Illinois 60606. On information and belief, MLB et al. sells, offers to sell, and/or uses products and services throughout the United States, including in this judicial district, and introduces infringing products and services into the stream of commerce knowing that they would be sold and/or used in this judicial district and elsewhere in the United States.

JURISDICTION AND VENUE

4. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

5. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

6. Venue is proper in this judicial district under 28 U.S.C. § 1400(b). On information and belief, each Defendant has committed acts of infringement in this judicial district and has a regular and established place of business within this judicial district.

7. On information and belief, each Defendant is subject to this Court's general and specific personal jurisdiction because each Defendant has sufficient minimum contacts within the State of New York.

8. MLB's infringement of AA's patent, as described in detail below, is substantially related to MLB's regular and established business in this judicial district because the tickets subject to the MLB box office ticketing service **Ballpark app** used by all MLB teams via the www.MLB.com and teams websites on the infringing MLB primary and secondary market digital ticket sales platforms, establishing the validity and authenticity of the digital tickets use the infringing MLB network system, and the box office ticketing service involve the use of the eChanging Barcodes AA patented systems and methods.

9. This Court has personal jurisdiction over MLB et al. because MLB and its' member teams have committed and continues to commit acts of infringement in this judicial district in violation of 35 U.S.C. subsection 271(a).

10. MLB has derived and continues to derive substantial revenues from its' patent infringement in this and other judicial districts throughout the country.

11. Venue is proper in this judicial district for MLB under 28 U.S.C. § 1400(b) because, among other reasons, MLB is registered to do business in the State of New York,

committed acts of infringement in this judicial district, and has a regular and established place of business within this judicial district.

BACKGROUND

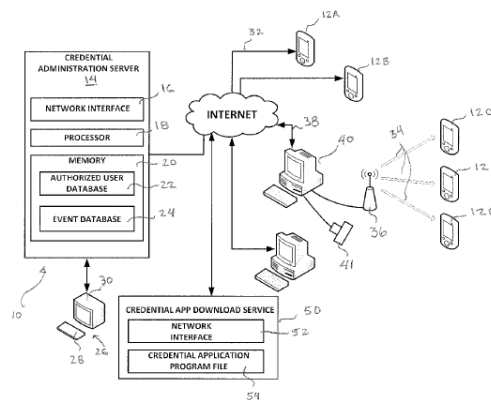
The Invention

12. Alan Amron is the inventor of U.S. Patent No. 9,047,715 (“the ’715 patent”) referred to hereinafter as the “Patent”. True and correct copies of the Patent is attached as **Exhibit**

A.



<p>(12) United States Patent Amron</p> <p>(54) SYSTEM AND METHOD FOR CREDENTIAL MANAGEMENT AND ADMINISTRATION</p> <p>(75) Inventor: Alan Amron, Boca Raton, FL (US)</p> <p>(73) Assignee: eCREDENTIALS, INC., Hempstead, NY (US)</p> <p>(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.</p> <p>(21) Appl. No.: 13/311,548</p> <p>(22) Filed: Dec. 6, 2011</p> <p>(65) Prior Publication Data US 2014/0055231 A1 Feb. 27, 2014</p> <p>Related U.S. Application Data</p> <p>(63) Continuation-in-part of application No. 13/196,342, filed on Aug. 2, 2011.</p> <p>(51) Int. Cl. G05B 23/00 (2006.01) G07C 9/00 (2006.01)</p> <p>(52) U.S. Cl. CPC G07C 9/00119 (2013.01); G07C 9/00103 (2013.01)</p> <p>(58) Field of Classification Search CPC G06Q 30/02; G07F 7/1008 USPC 340/10.1, 5.6, 12.5; 235/375 See application file for complete search history.</p>	<p>(10) Patent No.: US 9,047,715 B2</p> <p>(45) Date of Patent: Jun. 2, 2015</p> <p>(56) References Cited U.S. PATENT DOCUMENTS</p> <table border="0"> <tr><td>6,736,322 B2*</td><td>5/2004</td><td>Gobburu et al.</td><td>235/462,46</td></tr> <tr><td>7,044,362 B2*</td><td>5/2006</td><td>Yu</td><td>235/375</td></tr> <tr><td>7,437,755 B2*</td><td>10/2008</td><td>Farino et al.</td><td>726/5</td></tr> <tr><td>7,828,220 B2*</td><td>11/2010</td><td>Mullen</td><td>235/492</td></tr> <tr><td>8,267,314 B2*</td><td>9/2012</td><td>Ishihashi et al.</td><td>235/380</td></tr> <tr><td>8,628,019 B2*</td><td>1/2014</td><td>Audebert et al.</td><td>235/492</td></tr> <tr><td>2006/0106537 A1*</td><td>5/2006</td><td>Hamrick et al.</td><td>701/213</td></tr> <tr><td>2009/0172035 A1*</td><td>7/2009</td><td>Lessing et al.</td><td>707/104.1</td></tr> <tr><td>2010/0014277 A1*</td><td>1/2010</td><td>Delany</td><td>362/95</td></tr> <tr><td>2010/0238033 A1*</td><td>9/2010</td><td>Blumel et al.</td><td>340/573.4</td></tr> <tr><td>2012/0072249 A1*</td><td>3/2012</td><td>Weir et al.</td><td>705/5</td></tr> </table> <p>* cited by examiner</p> <p><i>Primary Examiner</i> — Vernal Brown (74) <i>Attorney, Agent, or Firm</i> — Cozen O'Connor</p> <p>(57) ABSTRACT A credential management and administration system and method by which the documented eligibility of persons to receive benefits, services, access to premises or events, and the like is centrally administered. In one embodiment, credentials are distributed to the individuals electronically, via communication network, to respective portable device having a corresponding display. Each display is configured to visually present certain qualifying information that is updated at periodic intervals. Alternatively, the qualifying information may be presented via wireless means to a suitable receiver proximate the location where services are delivered.</p> <p>46 Claims, 10 Drawing Sheets</p>	6,736,322 B2*	5/2004	Gobburu et al.	235/462,46	7,044,362 B2*	5/2006	Yu	235/375	7,437,755 B2*	10/2008	Farino et al.	726/5	7,828,220 B2*	11/2010	Mullen	235/492	8,267,314 B2*	9/2012	Ishihashi et al.	235/380	8,628,019 B2*	1/2014	Audebert et al.	235/492	2006/0106537 A1*	5/2006	Hamrick et al.	701/213	2009/0172035 A1*	7/2009	Lessing et al.	707/104.1	2010/0014277 A1*	1/2010	Delany	362/95	2010/0238033 A1*	9/2010	Blumel et al.	340/573.4	2012/0072249 A1*	3/2012	Weir et al.	705/5
6,736,322 B2*	5/2004	Gobburu et al.	235/462,46																																										
7,044,362 B2*	5/2006	Yu	235/375																																										
7,437,755 B2*	10/2008	Farino et al.	726/5																																										
7,828,220 B2*	11/2010	Mullen	235/492																																										
8,267,314 B2*	9/2012	Ishihashi et al.	235/380																																										
8,628,019 B2*	1/2014	Audebert et al.	235/492																																										
2006/0106537 A1*	5/2006	Hamrick et al.	701/213																																										
2009/0172035 A1*	7/2009	Lessing et al.	707/104.1																																										
2010/0014277 A1*	1/2010	Delany	362/95																																										
2010/0238033 A1*	9/2010	Blumel et al.	340/573.4																																										
2012/0072249 A1*	3/2012	Weir et al.	705/5																																										



13. The Patent resulted from the pioneering efforts of Alan Amron in the area of digital ticketing and access systems. These efforts resulted in the development of a method and system for preventing digital ticketing fraud and scalping. At the time of these pioneering efforts, the most widely used technology was static barcoded tickets, passes, and/or devices to provide access to a physical location, event, or service. Frequently these static barcoded tickets were screen shot and used fraudulently.

14. While these systems permitted access to the location, event, or service the use of physical and digital tickets gave rise to counterfeit and fraudulent tickets uses. In this new age of digital smartphones, more people have the ability to use secure digital ticketing, Amron's invented in 2011 and awarded a United States patented in 2015 invention has now solved this major problem and makes the digital ticket secure.

15. To eliminate the multiple use of the same ticket, screen shots, ticket issuers venues and event organizers introduced Amron's dynamic digital changing barcode technology so that, via a remote or connected scanner, in real-time no one can get in but the actual digital ticket holder. Such changing every 15-30 seconds readable barcode, QR code, or any other discernable image could not be duplicated physically or electronically, and thus eliminated counterfeiting and scalping.

Changing rotating barcode and QR code as examples shown here below.



16. In 2011, Amron conceived of the invention claimed in the '715 Patent as a way to eliminate the problems identified above.

Advantage Over the Prior Art

17. The patented invention disclosed, provides advantages over the prior art, and in particular improved the static ticketing systems for providing safe access to events, premises, and the like. (See '715 patent claims) The advantage of the patented invention is the changing of the digital barcode periodically (seconds) to eliminate any fraud.

18. Another advantage of the patented invention is the eliminating of the possibility of resale of a digital ticket on the secondary market without the proper barcoded authority.

19. These major advantages that are achieved through the use of the patented invention, issued on June 2, 2015, AA believes that the Patent offers significant commercial value and protection for all digital ticket sellers, venues and events.

Static still barcodes and QR codes as examples shown here below.



The Revolutionary Innovation

20. The patented invention disclosed resolves fraud and scalping related to electronic digital ticketing and access systems, particularly related to limiting access to authorized persons only, including limiting the conditions under which the authorized access can be transferred to another person. The digital age version of today's stagnant still static barcodes, updating the digital barcode from a static one to a rotating one that cannot be duplicated, to eliminate digital ticket fraud and scalping.

21. Dynamic Barcodes, invented by Amron in 2011, is a type of barcode that changes periodically to prevent duplication and fraud. Unlike static barcodes, which have a fixed representation and can be easily copied or scanned, dynamic barcodes use a rotating algorithm that updates the barcode image every 15-30 seconds or minutes. This makes it impossible for anyone to use a screenshot or a printout of the barcode to access a service or a product. Dynamic barcodes were first patented by Amron, with the United States Patent and Trademark Office issuing the patent (USPTO Amron Patent number: 9047715) in 2015. Amron developed the idea of dynamic barcodes after witnessing the problem of digital ticket fraud in various events and venues. He realized that the existing barcode system was vulnerable to counterfeiting and hacking, and decided to create a more secure and reliable solution. They have been used to enhance the security and convenience of digital tickets, boarding passes, hotel keys, coupons, and vouchers. They have also been used to prevent identity theft, phishing, and malware attacks. By using dynamic barcodes, users can enjoy the benefits of digital transactions without compromising their safety and privacy. Dynamic barcodes offer a simple and effective way to protect users from fraud and ensure the authenticity and integrity of digital data.

22. The 46 claims and 10 drawings of the '715 patent recite inventive concepts and provide a new and novel solution to specific digital ticketing problems.

23. The Amron '715 patent is a digital age version of today's stagnant still static barcodes, updating the digital barcode, QR code, Alphanumerical or any discernable image from a static one to a rotating one that cannot be duplicated to prevent digital ticket fraud.

PATENT '715 ABSTRACT

24. “A credential management and administration system and method by which the documented eligibility of persons to receive benefits, services, access to premises or events, and the like is centrally administered. In one embodiment, credentials are distributed to the individuals electronically, via communication network, to respective **portable device having a corresponding display**. Each display is configured to visually present **certain qualifying information that is updated at periodic intervals**. Alternatively, the qualifying information may be presented via wireless means to a suitable receiver proximate the location where services are delivered.” 46 claims, 10 Drawing Sheets.

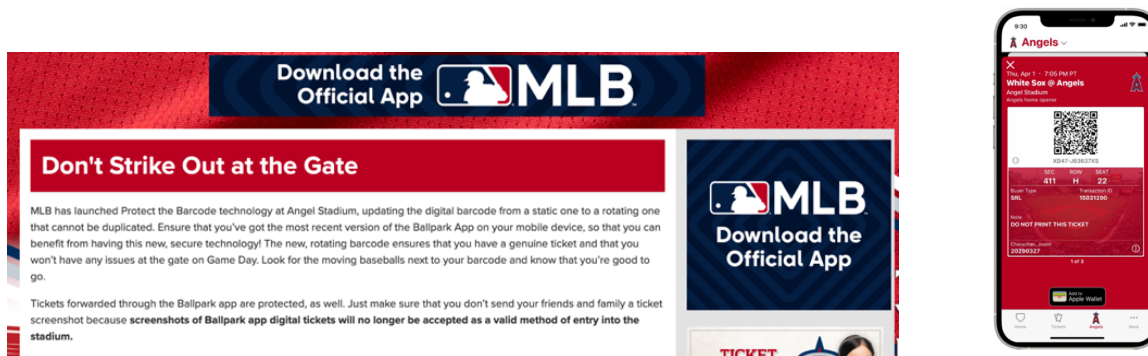
25. The use of dynamic changing barcodes as machine discernable images are covered in **Claim 1**. This claim specifies that the computer instructions stored in the non-transitory computer-readable storage medium, when executed by a processor, perform a method for configuring a portable electronic device as part of a credential management system. This method includes obtaining first visual symbol information for use by the portable electronic device in initiating display of a first machine discernable image to be presented as an access credential during a first specified time interval. The method also includes initiating wireless transmission of the obtained visual symbol information to the portable electronic device for visible display of the first machine discernable image by the portable device during the first-time interval. In this way, claim 1 also covers the use of dynamic barcodes as machine discernable images for the access credential.

26. **Claim 8** of the patent also covers the use of dynamic barcodes as machine discernable images. It specifies that the computer instructions stored in the non-transitory computer-readable storage medium, when executed by a processor, further perform a step of

transmitting a generation instruction to the portable electronic device, which is responsive to each generation instruction received to locally generate a corresponding bar code as the machine discernable image. Therefore, claim 8 covers the use of dynamic barcodes generated locally on the portable electronic device as the machine discernable image for the access credential.

27. While **Claim 1 and Claim 8** are the most relevant claims that cover the use of dynamic barcodes as machine discernable images, there are other claims in the patent that relate to the overall credential management system and method. For example, **claim 2** covers the association of visual symbol information with specific users during a time interval, while **Claim 3** covers the association of multiple visual symbol information with a specific user during different time intervals. **Claim 4** covers the use of previously associated visual symbol information if the user fails to display the current visual symbol information during the specified time interval. **Other claims** cover various aspects of the system and method, including the association of the portable electronic device with locations or services, the random selection of time intervals, and the transmission and reception of information between the credential administration server and the portable device.

28. MLB is administering digital tickets using dynamic barcodes as machine discernable images to prevent fraudulent entry to baseball games through their servers, as shown here.



STATEMENT OF CLAIM - CAUSE OF ACTION

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 9,047,715

29. The allegations set forth in the foregoing paragraphs are incorporated into this First Claim for Relief.

30. On June 2, 2015, the '715 patent was duly and legally issued by the United States Patent and Trademark Office under the title “System and Method for Credential Management and Administration”. (see **Exhibit A** attached here)

31. AA is the sole inventor assignee and owner of the right, title and interest in and to the '715 patent, including the right to assert all causes of action arising under said patent and the right to any remedies for infringement of it.

32. On information and belief, Defendants have and continue to directly infringe one or more claims of the '715 patent by selling, offering to sell, making, using, and/or providing and causing to be used one or more systems and methods for electronic ticketing, which by way of example include MBL ticketing management system (the “Accused **Ballpark app**”).

33. On information and belief, the Accused **Ballpark app** performs a system and method for changing the barcode periodically thereby providing secure digital access to a premise.

34. Infringement analysis attached as Exhibit F shows MLB's infringement of one or more claims of the 46 claims in the '715 patent set forth in **Exhibit A** attached here. This patent infringement by MLB analysis detailed in **Exhibit F** is clear and preliminary, as it is provided in advance of any discovery provided by Defendants with respect to the '715 patent. AA reserves all rights to amend, supplement and modify this infringement analysis. Nothing in the attached should be construed as any express or implied contention or admission regarding the construction of any term or phrase of the 46 claims of the '715 patent.

35. The Accused system infringed and continues to infringe at least one or more of

Case 1:23-cv-10576-UA Document 1 Filed 12/04/23 Page 11 of 75
the 46 claims in the '715 patent. (see **Exhibit F** Patent infringement analysis report and charts)

36. In the Defendants' own advertised public words, they admit infringing the '715 patent. "**Don't Strike Out at the Gate** | Los Angeles Angels "MLB has launched Protect the Barcode technology at Angel Stadium, updating the digital barcode from a static one to a rotating one that cannot be duplicated". <https://www.mlb.com/angels/tickets/mobile/dont-strike-out-at-the-gate>

- a. "MLB has launched Protect the Barcode technology at Angel Stadium, updating the digital barcode from a static one to a rotating one that cannot be duplicated. Ensure that you've got the most recent version of the Ballpark App on your mobile device, so that you can benefit from having this new, secure technology! The new, rotating barcode ensures that you have a genuine ticket and that you won't have any issues at the gate on Game Day. Look for the moving baseballs next to your barcode and know that you're good to go. Tickets forwarded through the **Ballpark app** are protected, as well. Just make sure that you don't send your friends and family a ticket screenshot because **screenshots of Ballpark app digital tickets will no longer be accepted as a valid method of entry into the stadium.**"

(As quoted directly from the MLB website see **Exhibit D** attached here)

37. Original April 7, 2023 email first official notice to MLB of infringement and November 7, 2023 last offer email, and November 13, 2023 final MLB response in telephone call. (**Exhibits' B, C and E** attached here)

a. **April 7, 2023**

Dear Mr. Littmann,

Thank you for your email invitation to speak next week. However, I would like to keep our correspondence in writing for now.

I have downloaded the MLB Angels Stadium ticket app (which operates by updating the digital barcode from a static one to a rotating one that cannot be duplicated) and find that it literally reads on at least one of my issued 2015 patented claims.

That said, MLB can benefit from this opportunity, which is my unusual offer of a free life of the patents (9 more years) license to the Major League Baseball Angels Stadium digital ticketing, with “updating the digital barcode from a static one to a rotating one that cannot be duplicated”.

If you choose to accept this offer, let me know, and when we receive the revival documents from the PTO, we will enter into a formal license with no money down and no percentage royalty for the life of the patents (9 more years).

Sincerely,

Alan

b. November 7, 2023

Dear Mr. Littmann, I hope this email finds you well. I am pleased to inform you that my Petition to revive has been granted. I am writing to inquire as to whether you are still my MLB direct contact. I would now be willing to discuss the details over a phone call. I propose this exclusive to MLB offer: Granting the Angels, a free 8-year license (life of the patent) to use the 9,047,715 dynamic barcodes patent, specifically designed to prevent digital ticket fraud...

Sincerely,
Alan Amron

c. On Wednesday, November 8, 2023, 8:02 PM, Alan Littmann <alittmann@goldmanismail.com> wrote:

Mr. Amron,

I remain the contact on behalf of MLB. I am available to discuss this matter on Friday afternoon or Monday morning. Please let me know if either of those windows work.

Sincerely,

Alan

d. November 8, 2023

Mr. Littmann,

Thank you for your quick response. I will be available to discuss this matter with you on Monday November 13, 2023 at 11:00 am New York time.

Sincerely,

Alan Amron

e. November 13, 2023

@ 11:00 am telephone call end result was “MLB is not interested in acquiring a license”.

38. Each of Defendants were made aware of the '715 patent and its infringement thereof at least as early as April 7, 2023 and or the filing date of this complaint.

39. On information and belief, since Defendant MLB received notice, MLB has induced and continues to induce others to infringe at least one or more claims of the '715 patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to each of MLB's teams, partners, clients, customers, and end users, whose use of the Accused **Ballpark app** system constitutes direct infringement of at least one or more claims of the '715 patent.

40. In particular, MLB's actions that aid and abet others such as its teams, partners, customers, clients, and end users to infringe include advertising and distributing the Accused **Ballpark app** system and providing instruction materials, training, and services regarding the Accused system. On information and belief, the MLB has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because MLB has had actual knowledge of the '715 patent and knowledge that its acts were inducing infringement of the '715 patent since MLB received notice on or about that such activities infringed the '715 patent.

41. In particular, MLB provides knowledge and support materials for third parties to integrate the Accused system into their own mobile or web applications. Additionally, MLB provides support for digital ticket purchasers and digital ticket holders in using digital tickets that utilize the Accused **Ballpark app** system. (www.MLB.com)

42. On information and belief, MBL is liable as a contributory infringer of the '715 patent under 35 U.S.C. § 271(c) by offering to sell, selling and importing into the United States ticketing systems to be especially made or adapted for use in an infringement of the '715 patent.

43. Since at least the filing date of the complaint, each Defendants' infringement has been and continues to be willful.

44. AA has been harmed by the Defendants' infringing activities.

45. Amron '715 patent description vs MLB et al. public sites statement. **Exhibit D.**

a. **The Amron '715 patent** is a digital age version of today's stagnant still static barcodes, **updating the digital barcode**, QR code, Alphanumerical or any discernable image **from a static one to a rotating one that cannot be duplicated** to prevent digital ticket fraud.

b. **"MLB has launched Protect the Barcode technology** at Angel Stadium, **updating the digital barcode from a static one to a rotating one that cannot be duplicated.** Ensure that you've got the most recent version of the Ballpark App on your mobile device, so that you can benefit from having this new, secure technology! The new, rotating barcode ensures that you have a genuine ticket and that you won't have any issues at the gate on Game Day. Look for the moving baseballs next to your barcode and know that you're good to go." **MLB.com**

Summary of the key infringement points, but not limited to:

46. MLB's Protect the Barcode technology is a digital age version of the Amron '715 patent, which updates digital barcodes from static to rotating to prevent fraud.

47. MLB's ticket technology configures a portable electronic device (via the MLB Ballpark app) to display a machine-discernible image (MLB mobile ticket barcode) during a specified time interval (MLB is changing the barcode every many seconds time interval).

48. MLB's ticket technology involves the transmission of generation instructions to the portable electronic device (via the MLB Ballpark app), which locally generates a corresponding barcode (machine-discernible image) for the access credential (MLB digital ticket).

49. MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with event information (game details), which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine-discernible image (mobile ticket barcode).

50. MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with areas of a facility (stadium sections) to which the user is authorized for entry, which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine-discernible image (mobile ticket barcode).

51. MLB's ticketing system involves the receipt and storage of administrator input specifying the details of the credentials (digital tickets) to be distributed. This information is then transmitted to the portable electronic device (via the MLB Ballpark app) for display as machine-discernible images (mobile ticket barcodes).

52. MLB's ticketing system includes the receipt and storage of user input specifying user information (such as personal details or preferences), which is then transmitted to the credential administration server for association with the user's account.

53. Claim 1: MLB's ticket technology configures a portable electronic device (via the MLB Ballpark app) to display a machine discernable image (MLB mobile ticket barcode) during a specified time interval being specified to have a duration of seconds (MLB is changing barcode every many seconds time interval).

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, AA demands a trial by jury on all issues triable as such.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff AA demands judgment for himself and against Defendants as follows:

- A. An adjudication that the Defendants have infringed the '715 Patent.
- B. An award in the amount of \$29 million dollars in damages to be paid by Defendants to compensate AA for Defendants' past infringement of the '715 patent, and a 5% of total ticket sales on a monthly royalty of any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;
- C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of AA's reasonable costs, expenses and consulting attorneys' fees; and
- D. An award to AA of such further relief at law or in equity as the Court deems just and proper.

Respectfully submitted,

/Alan Amron/

/s/Alan Amron

Dated: December 4, 2023

Alan Amron, Pro se Plaintiff

Alan Amron
alanamron@yahoo.com
103 Jessup Avenue
Box 354 Quogue, New
York 11959
Telephone: (929) 250-3650

for Plaintiff:
Alan Amron, inventor Pro se

For Defendants:

Alan Littmann, Esq.

Assigned counsel for MLB
200 South Wacker Dr., 22nd Floor, Chicago, IL 60606
P 312-881-5969 C 312-404-1871 F 312-380-7019
goldmanismail.com
alittmann@goldmanismail.com

MAJOR LEAGUE BASEBALL, MLB
ADVANCED MEDIA L.P.,
AZPB LIMITED PARTNERSHIP,
ATLANTA NATIONAL LEAGUE
BASEBALL CLUB, LLC,
BALTIMORE ORIOLES LIMITED
PARTNERSHIP,
BOSTON RED SOX BASEBALL CLUB
LIMITED PARTNERSHIP,
CHICAGO CUBS BASEBALL CLUB,
LLC,
CHICAGO WHITE SOX, LTD.,
THE CINCINNATI REDS LLC,
CLEVELAND GUARDIANS
BASEBALL COMPANY, LLC,
COLORADO ROCKIES BASEBALL
CLUB, LTD.,
DETROIT TIGERS, INC.,
HOUSTON ASTROS, LLC,
KANSAS CITY ROYALS BASEBALL
CLUB, LLC,
ANGELS BASEBALL LP,
LOS ANGELES DODGERS LLC,
MARLINS TEAMCO, LLC,
MILWAUKEE BREWERS BASEBALL
CLUB, LIMITED PARTNERSHIP,
MINNESOTA TWINS, LLC,
STERLING METS, L.P.,
NEW YORK YANKEES
PARTNERSHIP,
ATHLETICS INVESTMENT GROUP,
LLC,
THE PHILLIES,
PITTSBURGH ASSOCIATES,
PADRES L.P.,
SAN FRANCISCO GIANTS
BASEBALL CLUB LLC,
THE BASEBALL CLUB OF SEATTLE,
LLLP,
ST. LOUIS CARDINALS, LLC,
RAYS BASEBALL CLUB, LLC,
RANGERS BASEBALL LLC,

ROGERS BLUE JAYS BASEBALL
PARTNERSHIP,
WASHINGTON NATIONALS AND
BASEBALL CLUB, LLC.

Jeff Manahan

Director Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
manahan.jeff@gmail.com

Lara Wisch, Esq.

Vice President General Counsel at Major League
Baseball
larapitaro.wisch@mlb.com
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800

John Tierney

Vice President Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
John.tierney@mlb.com

Daniel Halem

Deputy Commissioner, Baseball Administration at
Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
daniel.halem@mlb.com
Harvard law school

Nick Arndt

Director, Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
nickarndt216@gmail.com

Justin Charschan

Manager Ticketing at Major League Baseball
justin.charschan@gmail.com
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing **PLAINTIFF ALAN AMRON'S SUMMONS AND COMPLAINT** original has been filed with the Clerk of the Court and served, pursuant to Federal Civil Procedure, via the e Portals listed below, this 4th day of December, 2023 to:

Respectfully submitted,

/Alan Amron/ /s/Alan Amron

Alan Amron

Dated: December 4, 2023

for Plaintiff:

Alan Amron, Pro se Plaintiff
alanamron@yahoo.com

103 Jessup Avenue
Box 354 Quogue,
New York 11959
Telephone: (929) 250-3650

For Defendants:

Alan Littmann, Esq.

Assigned counsel for MLB
200 South Wacker Dr., 22nd Floor, Chicago, IL 60606
P 312-881-5969 C 312-404-1871 F 312-380-7019
goldmanismail.com
alittmann@goldmanismail.com

MAJOR LEAGUE BASEBALL, MLB
ADVANCED MEDIA L.P.,
AZPB LIMITED PARTNERSHIP,
ATLANTA NATIONAL LEAGUE
BASEBALL CLUB, LLC,
BALTIMORE ORIOLES LIMITED
PARTNERSHIP,
BOSTON RED SOX BASEBALL CLUB
LIMITED PARTNERSHIP,

CHICAGO CUBS BASEBALL CLUB, LLC,
CHICAGO WHITE SOX, LTD.,
THE CINCINNATI REDS LLC,
CLEVELAND GUARDIANS
BASEBALL COMPANY, LLC,
COLORADO ROCKIES BASEBALL CLUB,
LTD.,
DETROIT TIGERS, INC.,
HOUSTON ASTROS, LLC,
KANSAS CITY ROYALS BASEBALL
CLUB, LLC,
ANGELS BASEBALL LP,
LOS ANGELES DODGERS LLC,
MARLINS TEAMCO, LLC,
MILWAUKEE BREWERS BASEBALL
CLUB, LIMITED PARTNERSHIP,
MINNESOTA TWINS, LLC,
STERLING METS, L.P.,
NEW YORK YANKEES PARTNERSHIP,
ATHLETICS INVESTMENT GROUP, LLC,
THE PHILLIES,
PITTSBURGH ASSOCIATES,
PADRES L.P.,
SAN FRANCISCO GIANTS BASEBALL
CLUB LLC,
THE BASEBALL CLUB OF SEATTLE,
LLLP,
ST. LOUIS CARDINALS, LLC,
RAYS BASEBALL CLUB, LLC,
RANGERS BASEBALL LLC,
ROGERS BLUE JAYS BASEBALL
PARTNERSHIP,
WASHINGTON NATIONALS AND
BASEBALL CLUB, LLC.

Jeff Manahan

Director Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
manahan.jeff@gmail.com

Lara Wisch, Esq.

Vice President General Counsel at Major League
Baseball
larapitaro.wisch@mlb.com
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800

John Tierney

Vice President Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
John.tierney@mlb.com

Daniel Halem

Deputy Commissioner, Baseball Administration at
Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
daniel.halem@mlb.com
Harvard law school

Nick Arndt

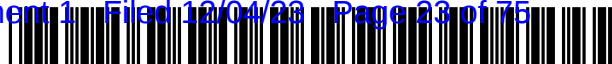
Director, Ticketing at Major League Baseball
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800
nickarndt216@gmail.com

Justin Charschan

Manager Ticketing at Major League Baseball
justin.charschan@gmail.com
1271 Avenue of The Americas
New York, NY 10020-1300
(212) 931-7800

EXHIBITS

- A- United States Patent Number 9,047,715
- B- First email notice of infringement offers a fair license agreement on April 7, 2023
- C- Email offering a reasonable license agreement again on November 7, 2023
- D- In the infringer's own public words on their MLB website - admission of infringement in their own advertised words. At www.mlb.com **Ballpark app**
- E- Email response from MLB on November 8, 2023 and my response to it – The result of phone call on November 13, 2023 at 11:00 am
- F- '715 patent infringement analysis of MLB and claim charts



US009047715B2

(12) **United States Patent**
Amron

(10) **Patent No.:** **US 9,047,715 B2**
(45) **Date of Patent:** **Jun. 2, 2015**

(54) **SYSTEM AND METHOD FOR CREDENTIAL MANAGEMENT AND ADMINISTRATION**

(56) **References Cited**

(75) Inventor: **Alan Amron**, Boca Raton, FL (US)
(73) Assignee: **eCREDENTIALS, INC.**, Hempstead, NY (US)
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

U.S. PATENT DOCUMENTS

6,736,322 B2 *	5/2004	Gobburu et al.	235/462.46
7,044,362 B2 *	5/2006	Yu	235/375
7,437,755 B2 *	10/2008	Farino et al.	726/5
7,828,220 B2 *	11/2010	Mullen	235/492
8,267,314 B2 *	9/2012	Ishibashi et al.	235/380
8,628,019 B2 *	1/2014	Audebert et al.	235/492
2006/0106537 A1 *	5/2006	Hamrick et al.	701/213
2009/0172035 A1 *	7/2009	Lessing et al.	707/104.1
2010/0014277 A1 *	1/2010	Delany	362/95
2010/0238033 A1 *	9/2010	Blumel et al.	340/573.4
2012/0072249 A1 *	3/2012	Weir et al.	705/5

(21) Appl. No.: **13/311,548**

* cited by examiner

(22) Filed: **Dec. 6, 2011**

(65) **Prior Publication Data**

US 2014/0055231 A1 Feb. 27, 2014

Primary Examiner — Vernal Brown

(74) Attorney, Agent, or Firm — Cozen O'Connor

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/196,342, filed on Aug. 2, 2011.

(51) **Int. Cl.**
G05B 23/00 (2006.01)
G07C 9/00 (2006.01)

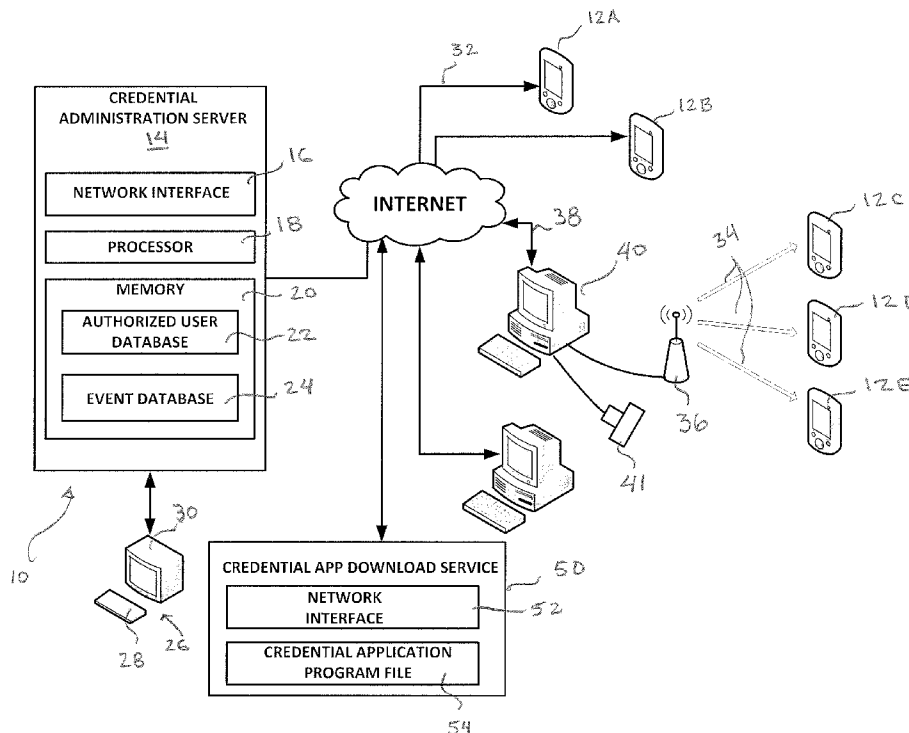
(52) **U.S. Cl.**
CPC **G07C 9/00119** (2013.01); **G07C 9/00103** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 30/02; G07F 7/1008
USPC 340/10.1, 5.6, 12.5; 235/375
See application file for complete search history.

(57) **ABSTRACT**

A credential management and administration system and method by which the documented eligibility of persons to receive benefits, services, access to premises or events, and the like is centrally administered. In one embodiment, credentials are distributed to the individuals electronically, via communication network, to respective portable device having a corresponding display. Each display is configured to visually present certain qualifying information that is updated at periodic intervals. Alternatively, the qualifying information may be presented via wireless means to a suitable receiver proximate the location where services are delivered.

46 Claims, 10 Drawing Sheets



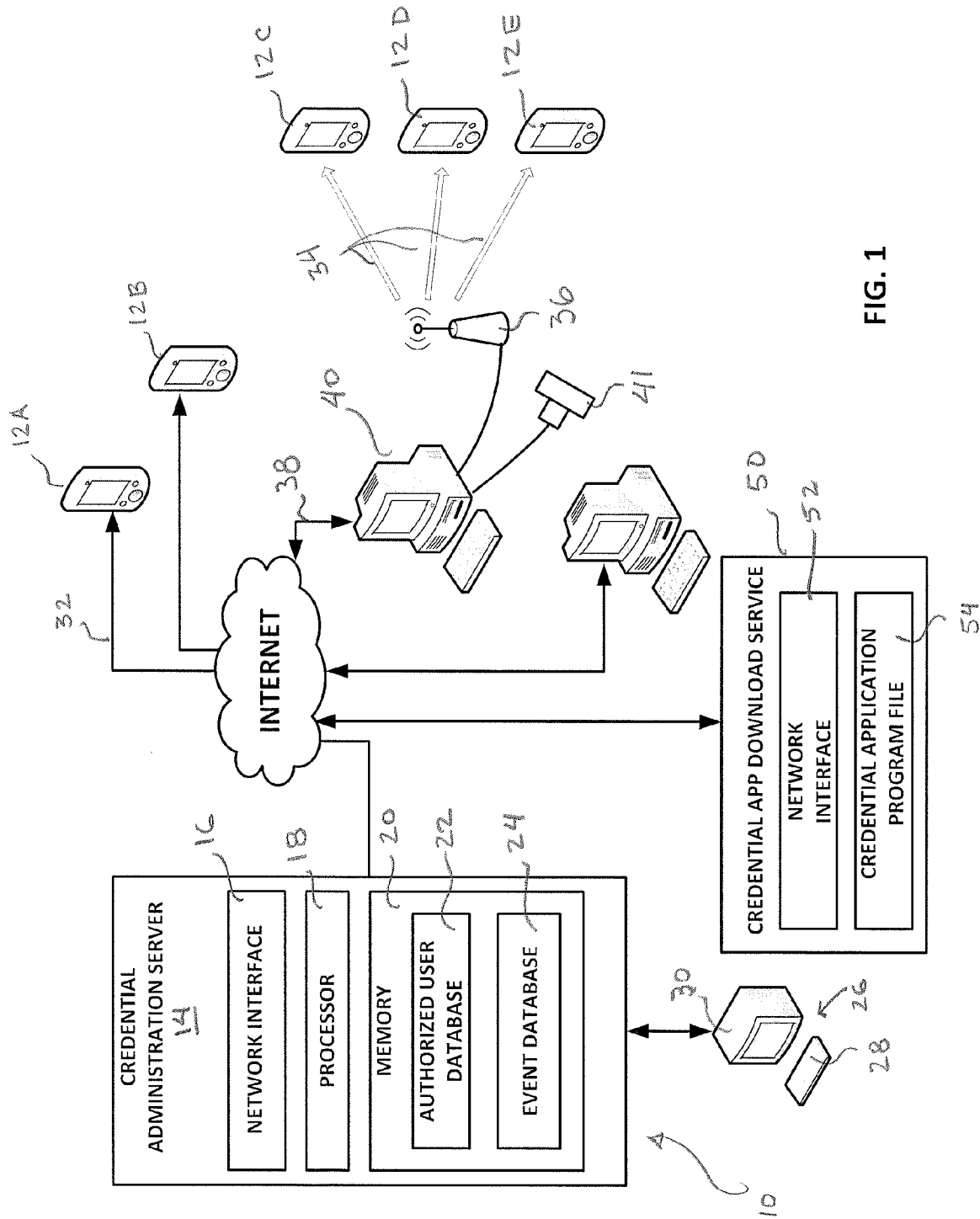


FIG. 1

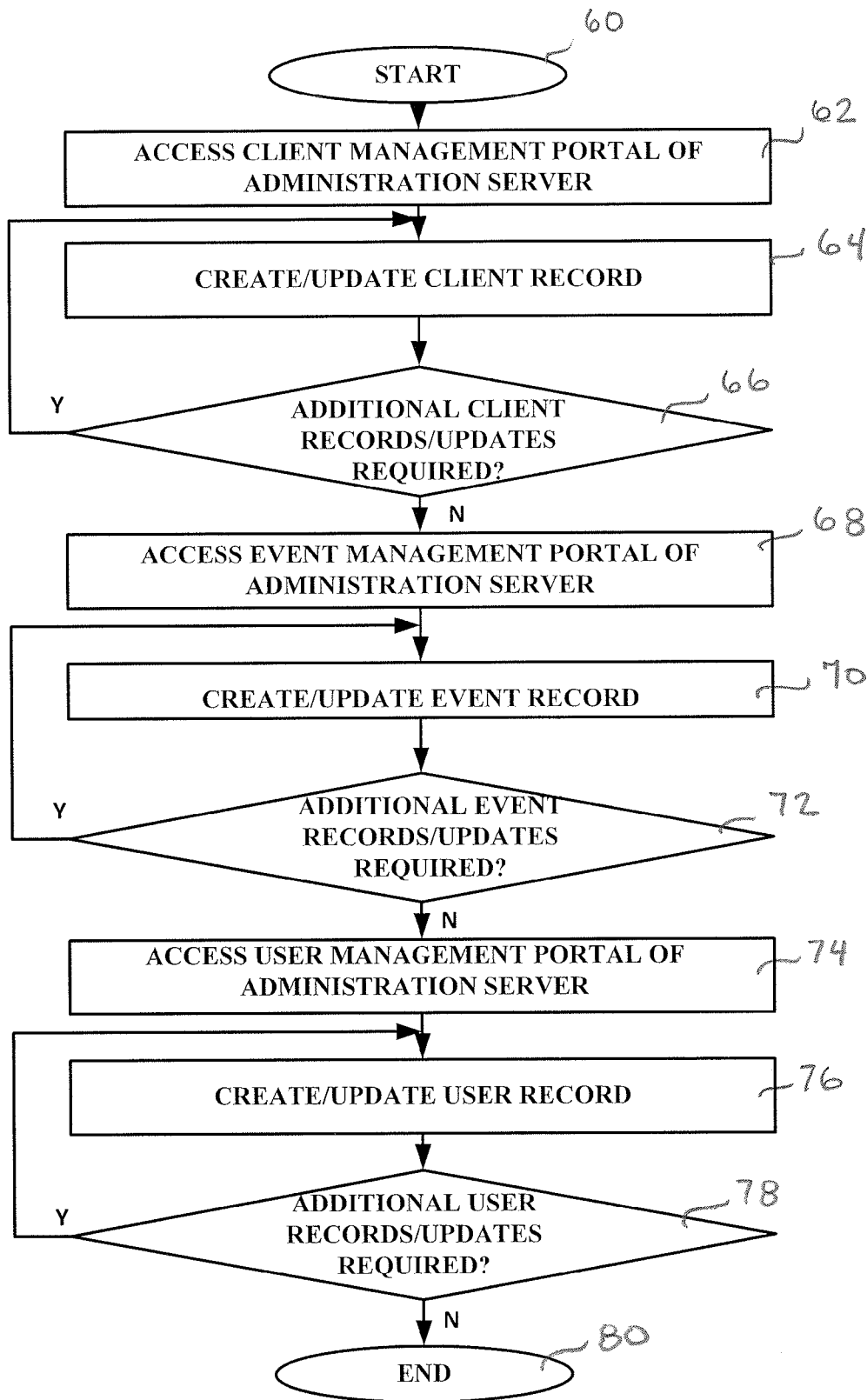


FIG. 2

FIG. 3A is a screenshot of a web application interface. At the top, there is a navigation bar with four tabs: "CLIENTS", "EVENTS", "USERS", and "SETTINGS". Below the navigation bar is a header section labeled "CLIENT MANAGEMENT" on the left and a "NEW" button on the right. A search bar is located between the header and the main content area. The main content area displays a list of clients with the following entries:

CLIENT NAME
National Football League
Nike
National Security Agency

Handwritten annotations include "642" pointing to the "CLIENTS" tab, "644" pointing to the search bar, and "640" pointing to the "NEW" button.

FIG. 3A

FIG. 3B is a screenshot of the "ADD CLIENT" form in the same application. The navigation bar and header are identical to FIG. 3A. The main content area is titled "ADD CLIENT" and contains the following fields:

- NAME: Nike
- LOGO: [Empty field with a small circular icon to its right]
- ADDRESS: NIKE, Inc.
One Bowerman Dr
Beaverton, OR 97005
- PHONE: 1-800-344-6453
- E-MAIL: Consumer.affairs.gbr@nike.com

At the bottom of the form are "SAVE" and "CANCEL" buttons. A handwritten annotation "646" points to the "SAVE" button.

FIG. 3B

FIG. 4A is a screenshot of a web application interface for event management. At the top, there are four tabs: CLIENTS, EVENTS, USERS, and SETTINGS. Below the tabs is a section titled 'EVENT MANAGEMENT' containing a dropdown menu set to 'Upcoming', another dropdown menu set to 'Client', a search input field, and a 'NEW' button. The main content is a table with the following data:

EVENT NAME	DATE	TIME	
Pre-Season Friendly	Sep 12, 2011	10:45 PM	
Emirates Cup	Oct 18, 2011	10:10 PM	
Barclays Premier League	Nov 21, 2011	11:45 PM	

Handwritten annotations are present: '682' points to the 'EVENTS' tab, '684' points to the 'Client' dropdown menu, and '686' points to the search input field.

FIG. 4A

FIG. 4B is a screenshot of the 'EVENT DETAILS' form in the same application. It features a top navigation bar with tabs for CLIENTS, EVENTS, USERS, and SETTINGS. Below the tabs is the 'EVENT MANAGEMENT' section with a search field and a 'NEW' button. The 'EVENT DETAILS' section contains the following fields:

- EVENT NAME:
- VENUE:
- TIME: (with handwritten annotation '688' pointing to it)
- DETAILS:

Below the event details is an 'ADVERTISEMENTS:' section with two rows, each containing a 'File:' label, a text input field (the first containing 'C:\video1'), and an 'UPLOAD' button. At the bottom of the form are 'SAVE' and 'CANCEL' buttons.

FIG. 4B

CLIENTS	EVENTS	USERS	SETTINGS
USER MANAGEMENT <input type="text" value="All"/> <input type="text"/> <input type="button" value="ASSIGN EVENT"/> <input type="button" value="NEW"/>			
USER NAME	DEVICE TYPE	E-MAIL	TELEPHONE
Allen Matthews	Smartphone	allen@gmail.com	xxx-xxx-xxxx
Albert Thoms	Smartphone	alt@gmail.com	xxx-xxx-xxxx
Alboz Hibs	RFID	Alboz@hotmail.com	xxx-xxx-xxxx

FIG. 5A

CLIENTS	EVENTS	USERS	SETTINGS
NEW USER <input type="text"/> <input type="button" value="NEW"/>			
ADD USER USER NAME: <input type="text"/> RFID: <input type="text"/> PHOTO: <input type="text"/> ADDRESS: <input type="text"/> PHONE: <input type="text"/> E-MAIL: <input type="text"/> <input type="button" value="SAVE"/> <input type="button" value="CANCEL"/>			

FIG. 5B

CLIENTS	EVENTS	USERS	SETTINGS
ASSIGN USERS TO EVENT			<input type="button" value="NEW USER"/>
<div style="display: flex; justify-content: space-between; margin-bottom: 20px;"> <div style="width: 45%;"> <p>CLIENT NAME: <input style="width: 100%;" type="text"/></p> <p>EVENT NAME: <input style="width: 100%;" type="text"/></p> </div> <div style="width: 45%;"></div> </div> <div style="display: flex; justify-content: space-around;"> <div style="width: 45%; border: 1px solid black; border-radius: 10px; padding: 5px;"> <p style="text-align: center; margin-bottom: 5px;">ALL USERS</p> <ul style="list-style-type: none"> Allen Matthews Albert Thoms Alboz Hibbs Ben Thompson Chaz Edwin Donald Adams Edward Samms <p style="text-align: center; margin-top: 10px;"><input type="button" value="OK"/></p> </div> <div style="width: 45%; border: 1px solid black; border-radius: 10px; padding: 5px;"> <p style="text-align: center; margin-bottom: 5px;">SELECTED USERS</p> <ul style="list-style-type: none"> Allen Matthews Alboz Hibbs Chaz Edwin <p style="text-align: center; margin-top: 10px;"><input type="button" value="CANCEL"/></p> </div> </div>			

FIG. 5C

CLIENTS	EVENTS	USERS	SETTINGS
USER MANAGEMENT			<input type="button" value="BACK"/>
<div style="border: 1px solid black; border-radius: 10px; padding: 10px;"> <p style="margin-bottom: 10px;">USER DETAILS</p> <div style="display: flex; align-items: flex-start;"> <div style="width: 25%; border: 1px solid black; margin-right: 10px; flex-grow: 1;"></div> <div style="width: 75%;"> <p>USER NAME: <input style="width: 100%;" type="text" value="BEN THOMPSON"/></p> <p>RFID: <input style="width: 100%;" type="text" value="1021 5455 2145 65214"/></p> <p>PHOTO: <input style="width: 100%;" type="text"/></p> <p>ADDRESS: <input style="width: 100%;" type="text"/></p> <p>PHONE: <input style="width: 100%;" type="text" value="XXX-XXX-XXXX"/></p> <p>E-MAIL: <input style="width: 100%;" type="text" value="ben@gmail.com"/></p> </div> </div> <p style="margin-top: 10px; margin-left: 10px;">UPLOADED PHOTO</p> <p style="text-align: right; margin-top: 10px;"> <input type="button" value="SAVE"/> <input type="button" value="CANCEL"/> </p> </div>			

FIG. 5D

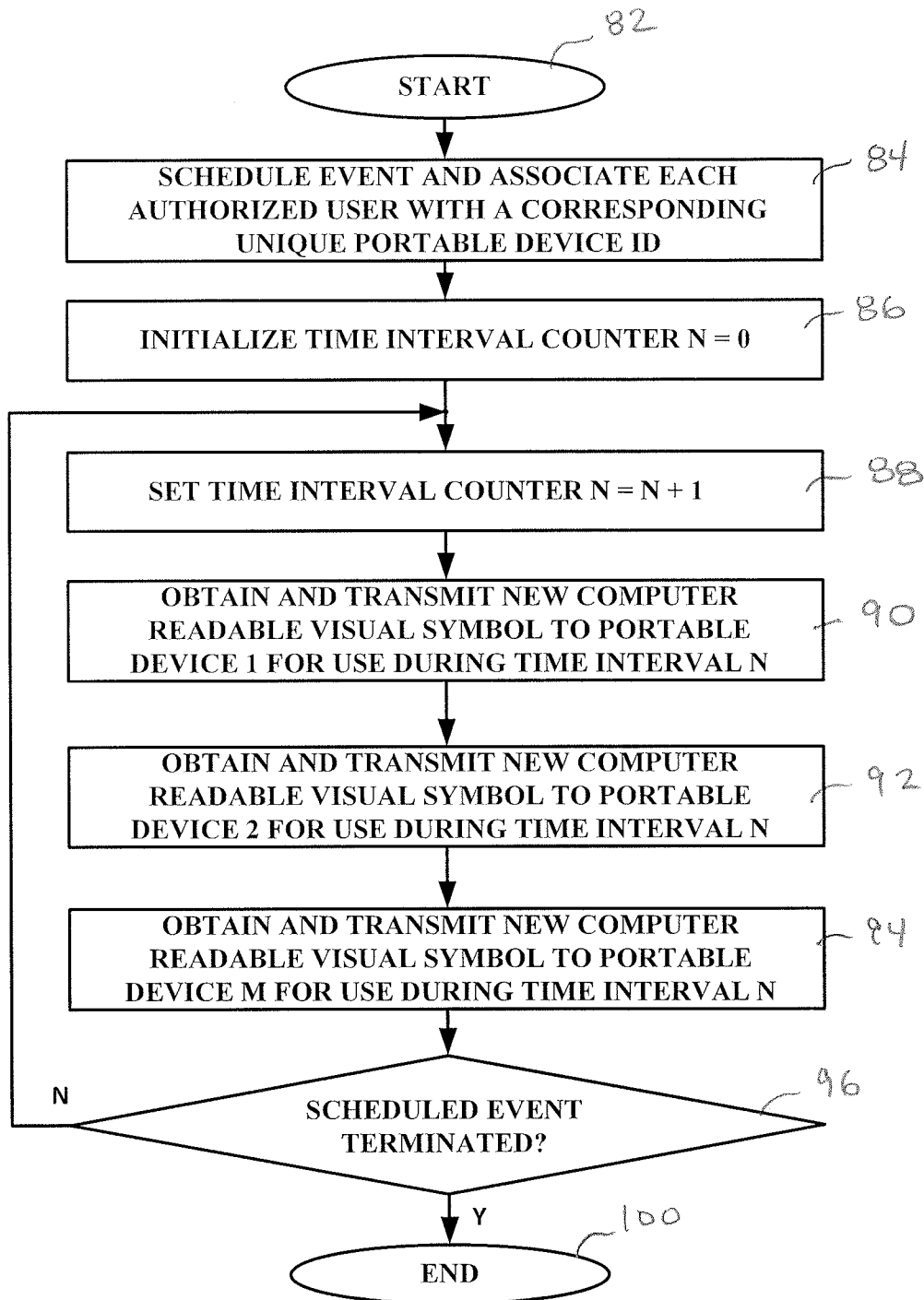


FIG. 6

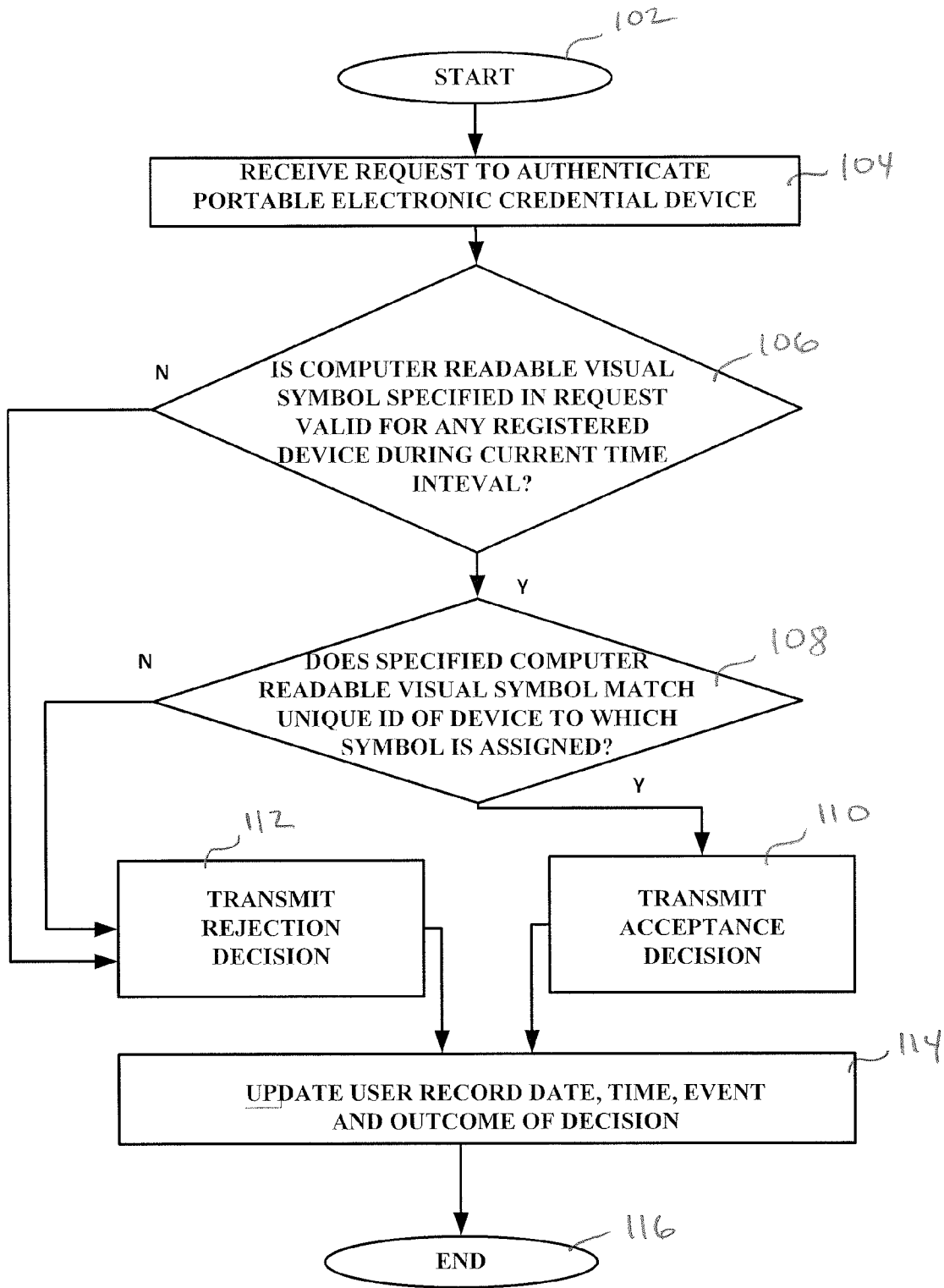


FIG. 7

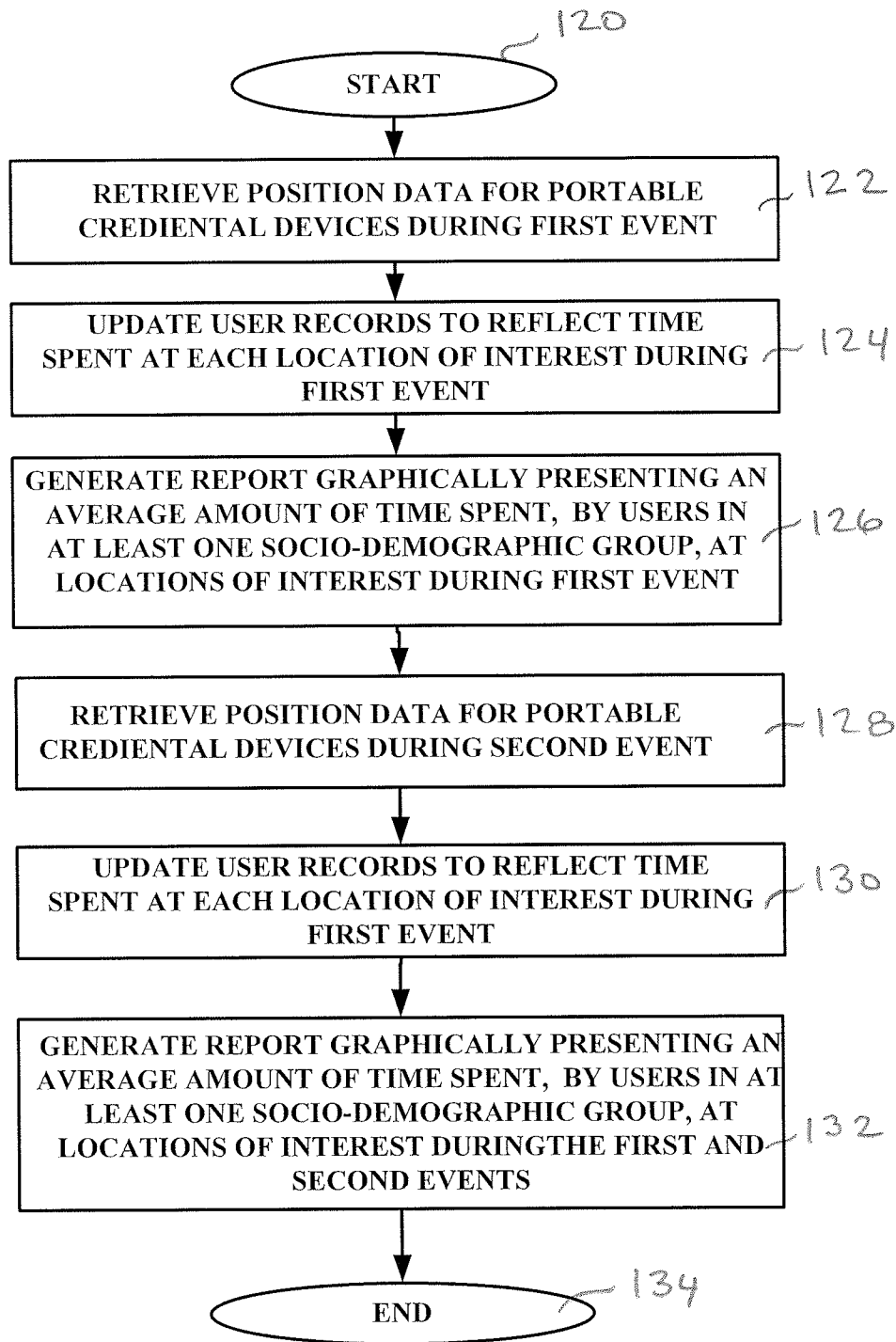


FIG. 8

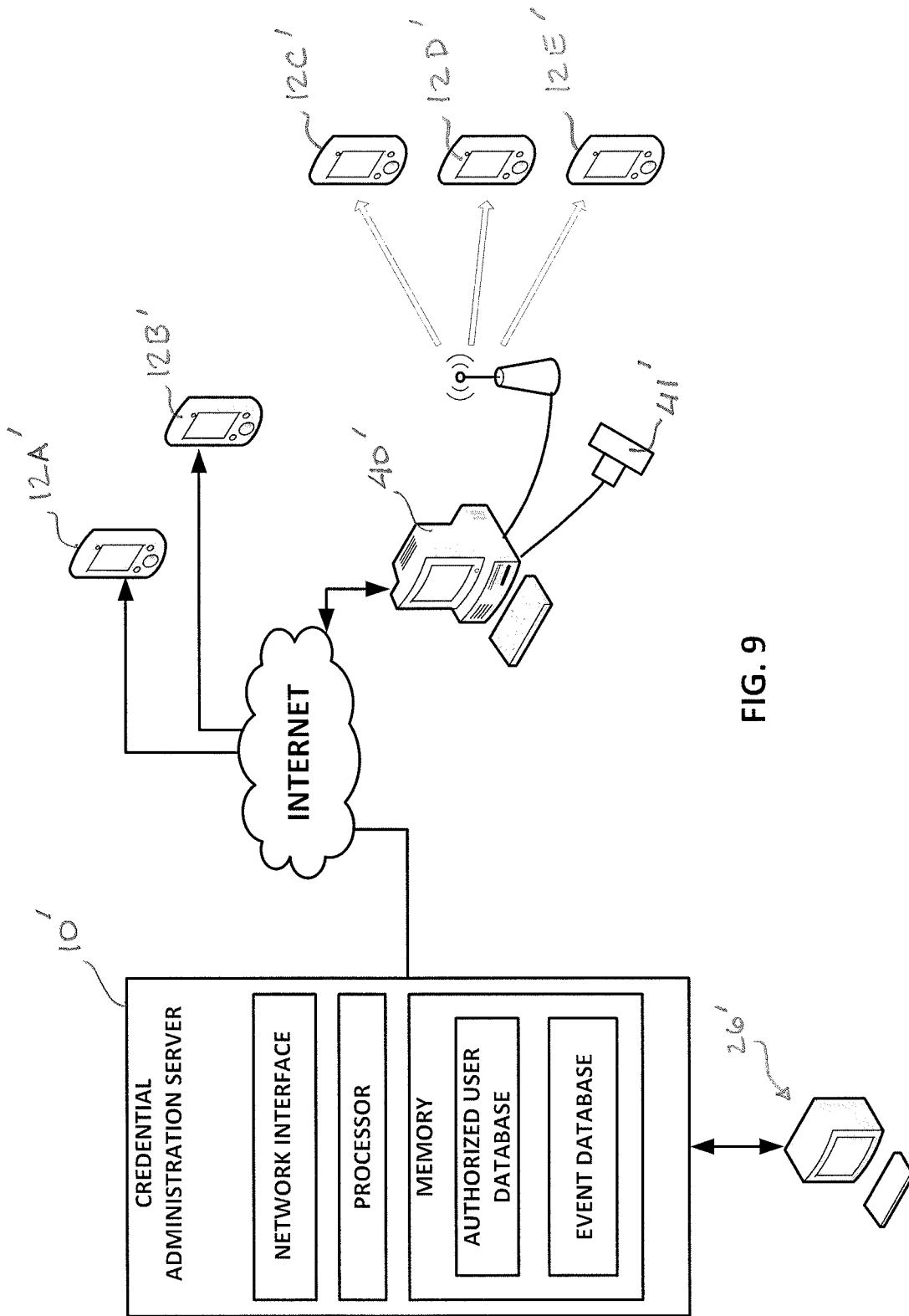


FIG. 9

US 9,047,715 B2

1

**SYSTEM AND METHOD FOR CREDENTIAL
MANAGEMENT AND ADMINISTRATION**

REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of co-pending patent application Ser. No. 13/196,342 filed by Alan Amron on Aug. 2, 2011 and entitled SYSTEM AND METHOD FOR ALLOCATING ACCESS AT EVENTS.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and techniques for administering the credentials of those individuals who are authorized, for example, to receive or benefit from a product or service, to enter an area of restricted access, to be present at an event or performance, or to collect governmental benefit, so that individuals bearing such credentials may be easily, accurately and consistently distinguished from individuals who are not so authorized.

2. Discussion of the Background Art

There are many situations where it is necessary to distinguish between those individuals with and without authorization to perform a particular act. Representative examples of such acts include entering into a restricted-access building or area of a building, attending a sporting event or performance, and receiving or collecting a governmental benefit (or, for that matter, state-run lottery winnings). The complexity associated with conferring authority upon select individuals or groups of individuals correlates closely with the population of individuals included in the group(s), the degree to which that population is static or dynamic, the number of groups (if applicable) within the population, and the need to accommodate variations in authority among those groups. For example, in building security situations where the number of individuals to be recognized is relatively small, the turnover among them is low, and the security workforce stable, it is generally possible to rely solely on recognition of each individual based on their physical appearance (i.e., “by sight”). Where the number of individuals having authority to enter secure areas and/or facilities is too large or is subject to a higher rate of turnover, or where the security staff itself is subject to turnover, however, it is not feasible to rely upon recognizing individuals by sight alone.

It has therefore become commonplace to distribute wearable badges or wallet-sized identification cards and to uniquely associate each such badge or ID card with the individual wearing or carrying it. A typical badge or ID card, for example, may include a photograph, a signature, a fingerprint, an RFID tag, and usually some combination of these. Specially designed doors equipped to admit only one person at a time and only upon recognition of an appropriate code (whether by keypad entry, passive RFID detection, biometric scanning, etc.) are also commonplace.

While the aforementioned identification systems are now ubiquitous in the workplace, there are certain limitations which make them undesirable for certain situations such, for example, as where a higher degree of protection against counterfeiting is required or as where one or more groups of individuals have only a transient need to enter a specific building, facility, or area thereof. The need to safeguard against counterfeiting, of course, arises from the widespread availability of image scanners, color printers, and field-programmable RFID tags. While the need to prevent unauthorized duplication or counterfeiting of credentials is particularly acute when it comes to law enforcement and

2

investigative personnel, additional safeguards would also be applicable to cards used to establish eligibility to receive government benefits (e.g., social security identification cards), to board an airplane as a passenger (e.g., a boarding pass), and even to collect lottery winnings

As for transient or frequently changing access requirements, consider the examples of traveling sports teams and performers. A professional football team may play eighteen games, with half of these being at a local or “home” stadium and the other half of the games being “away games” played at the home stadium of an adversary. A professional baseball team may play almost ten times as many games as a football team, but with a similar distribution of local and away games. In each of these cases, there are team members, supporting staff and other employees that all require a way of documenting their authority to enter a stadium on the day of an event (whether it be a practice session, a pre-season game, a regular season game, or a post season game). A musician or band may play at a large number of venues during a single tour, while a movie or television show may require filming at a number of different locations, with a concert or filming session at each discrete location also constituting an “event”.

In the aforementioned transient access situations, it has been customary to issue individuals who are authorized to be present at an event—whether they are attending as a member of the audience or in a supporting capacity—a discrete, temporary printed admission pass good only for the day of the event, after which it is to be discarded and cannot be used for admission to a subsequent event. These printed passes are expensive to produce, and each must be distributed to every authorized individual at some point prior to the applicable event(s). As the number of individuals with a need or desire to be present at multiple events grows, the cost and inefficiency of the approach quickly becomes apparent. While it would be possible to print and distribute a multiple use pass, the risk of unauthorized duplication and/or use, already quite high, increases dramatically.

In U.S. patent application Ser. No. 13/196,342, the inventor herein proposed a credential management system which obviates the need to design, produce and distribute one-time printed passes to individuals authorized to be present at an event such, for example, as cast members, stage crew, security details and staff, important guests, performers, players, officials and many others.

A continuing need exists for credential management systems which minimize the risks of unauthorized use or duplication of distributed credentials, passes, badges and tickets.

A further need exists for credential management systems having an optional location tracking capability whereby the whereabouts of each person to whom a credential is issued can be remotely monitored during an event.

Yet another need exists for credential management systems which can be centrally administered to accommodate levels of authorization among individuals in a single group, among individuals in plural groups associated with a single entity (e.g. a corporate client or government organization), and even among respective groups and individuals associated with a plurality of such entities.

SUMMARY OF THE INVENTION

The aforementioned needs are addressed, and an advance is made in the art, by methods of configuring and administering secure electronic devices so that they visually present an authenticating credential, pass, badge, ticket, etc. An illustrative method according to the invention includes the step of associating each of a plurality of portable electronic devices

with a corresponding user, utilizing an identifier that is unique to each device. The electronic devices can be smartphones, tablet computers, personal digital assistants (PDAs) adapted to utilize the services of a wireless telecommunications carrier and/or a wireless local area network (WLAN), they may be special purpose devices adapted for WLAN or physical link connections only, or they may be some combination of any or all of these devices. Non-limiting examples of useful unique identifiers include an internet protocol (IP) address, Ethernet media access control (MAC) address, a telephone number, an IMEI (International Mobile Equipment Identity) number, or an RFID tag.

The illustrative process further includes obtaining—for each of a group of secure electronic devices to be administered as a credential, pass, badge, ticket, permit or the like (collectively, “credentials”)—visual symbol information from which a unique visual symbol to be displayed during a first time interval can be derived. The visual symbol information can include a bar code, an alphanumeric sequence, or other type of machine-discernable image. The obtained visual symbol information is transmitted or otherwise supplied to a corresponding device and, for the duration of the first time interval, each administered electronic device of a group displays a visual symbol that is not displayed by any other administered electronic device of that group.

The illustrative process further includes obtaining and transmitting, for each of the group of electronic devices to be administered as a credential, visual symbol information from which the next unique credential to be displayed during the next time interval by each device can be derived. The time intervals may be of equal duration, on the order of 30 to 6000 seconds depending upon the rate at which each credential is to be updated, or the duration may be randomly selected so as to change from one interval to the next.

In accordance with another aspect of an illustrative embodiment of the present invention, a process of facilitating authentication of a candidate portable electronic device displaying a visual symbol and presented as a credential comprises determining, in a first determining step, whether the candidate portable electronic device is identifiable by a unique ID associated with an authorized user. In a second determining step, a determination is made as to whether the visual symbol displayed by the candidate portable electronic device corresponds to a visual symbol valid for an authorized user during a current time interval.

If a candidate portable electronic device is identifiable by a unique ID associated with an administered user and received data is representative of a visual symbol valid during a current time interval, a record associated with administered user is updated to reflect at least one of the time, date, location and event where the first portable electronic device was presented as a credential. Thereafter, an acceptance decision may be transmitted to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented. Optionally, an acceptance decision may also be transmitted to the remote terminal if the received data is representative of a visual symbol valid during a preceding time interval.

Conversely, if the candidate portable electronic device is not identifiable by a unique ID associated with an authorized user or if received data is not representative of a visual symbol valid during a current (or, optionally, a preceding) time interval and associated with any authorized user, a rejection decision is communicated to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.

In accordance with another aspect of illustrative embodiments of the present invention, at least some of the portable electronic devices include a global positioning satellite (GPS) receiver operative to obtain positional data and a corresponding cellular network transceiver for establishing a telecommunications link with a cellular network to thereby transmit position data for monitoring a location within a facility to which the first user has gained access using the first portable electronic device as a credential. Illustrative methods of administering such devices include a step of storing a record of locations visited by users of such devices while such users are present at a facility and a step of generating a report graphically presenting an average time spent, at respectively specified locations within the facility.

Alternate processes of administering devices may include steps of associating, in a database, each of a plurality of users with a corresponding portable electronic device having a memory, a display, at least one of a wireless transceiver and a global positioning satellite (GPS) receiver wherein each device is identifiable by a unique identifier, transmitting to each of said portable electronic devices an instruction to display at least one of a corporate logo, a respectively unique computer-readable visual symbol, and a personal photo for use as a credential to be presented at a facility; and collecting, from each device, data corresponding to time spent at a plurality of specified locations within a facility and to which each respective user has gained access using a corresponding portable electronic device as a credential. The collecting step may comprise receiving, at regular intervals, location data reported wirelessly by at least some of said portable electronic devices. Alternatively, the collecting step comprises performing wireless signal triangulation, at regular intervals, to locate at least some of said portable electronic devices. As yet another alternative, the collecting step may comprise downloading historical location data from at least some of the portable electronic devices via a physical link. The various reports may optionally incorporate socio-demographic information such that the movements of specific socio-demographic groups attending a particular event or visiting a given facility can be separately averaged and reported.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic representation of the elements of a credential management system constructed in accordance with an illustrative embodiment of the present invention, the system including a back-end credential management server and a credential application download service for configuring to use conventional communication network links to update a plurality of distributed, portable electronic credentials, passes, badges, tickets, permits, licenses and the like;

FIG. 2 is a flow chart depicting the client, event and user management processes of an exemplary back-end administrative process in accordance with an illustrative embodiment of the present invention;

FIGS. 3A and 3B depict the user interface of an exemplary client management portal which may be utilized by an administrator to enter and update client information;

FIGS. 4A and 4B depict the user interface of an exemplary event management portal which may be utilized by an administrator to enter and update event information;

US 9,047,715 B2

5

FIGS. 5A-5D depict the user interface of an exemplary user management portal which may be utilized by an administrator to enter and update client information;

FIG. 6 is a flow chart depicting an illustrative sequence of updating the respectively unique, computer readable visual symbols displayed by corresponding portable electronic credential devices so that they display a unique symbol during each of a plurality of consecutive time intervals spanning an event;

FIG. 7 is a flow chart depicting an illustrative process of portable credential device authentication, which may be optionally performed at the credential administration server;

FIG. 8 is a flow chart depicting an illustrative process for generating reports of interest to an event sponsor or other client, utilizing socio-demographic data entered by the administrator for at least some users as well as location data made available via wireless triangulation, gps tracking or other suitable means; and

FIG. 9 is a modified system in which a credential administration server constructed in accordance with the present invention is used to manage and update the credentials presented by a plurality of special purpose, portable electronic devices (as opposed to smart phones, pda's and tablet computers).

Like reference numerals indicate like elements in the drawings. Unless otherwise indicated, elements are not drawn to scale.

DETAILED DESCRIPTION

With initial reference to FIG. 1, there is shown an illustrative credential management system 10 for configuring a plurality of portable, secure electronic display devices indicated generally at 12A, 12B, 12C, 12D, and 12E, respectively. A characterizing feature of each of the devices 12A-12E depicted in FIG. 1 is the incorporation of a display dimensioned and arranged to present a visual symbol such that the device may serve as a secure electronic credential, pass, badge, ticket, permit, or license. As used herein, the phrase "visual symbol" is intended to encompass machine readable bar codes (e.g. UPC codes), alphanumeric sequences (which may consist of number sequences, letter sequences, or a combination thereof), images, and any other distinctive visible indicia apparent to a human observer and/or an optical scanning device. The term "credential" is intended to refer to a credential, badge, permit, license, and/or ticket as well as any combination of these.

Devices 12A-12E are dimensioned and arranged so that they can be carried, worn or otherwise presented—when depicting a visual symbol in accordance with the teachings of the present invention—as evidence, for example, of a person's authorization to be present at a particular facility or event (e.g., equivalent to an ID card issued by an employer, as a single- or multiple-event entry pass issued to staff, performers, members of the press, etc.), to receive a benefit (e.g., as a replacement for a social security card, health insurance card, other traditional indicia of entitlement), to exercise a governmentally regulated right or privilege (e.g., a license or permit credential), or to access the services of a common carrier (e.g., functioning as an airline boarding pass).

In any event, and with continued reference to FIG. 1, it will be appreciated that credential management system 10 includes a credential administration server 14 having a network interface 16, a processor 18, and memory 20. For a purpose which will be explained shortly, memory 20 defines an authorized user database indicated generally at reference number 22 and an event database indicated generally at ref-

6

erence numeral 24. Administrator input is supplied to credential administration server 14 by administrator terminal 26, which includes a keyboard 28, a display monitor 30, and other peripheral devices such as a mouse, scanning device, and printer (none of which are shown).

Interaction between credential management server 14 and electronic display devices 12A-12E is facilitated via a suitable network communication link as, for example, an internet link, established between network interface 16 and a corresponding interfaces and transceiver (not shown) within each respective electronic display device. In the latter regard, it should be emphasized that a credential management system constructed in accordance with the teachings of the present invention may be readily adapted to support a wide variety of electronic display devices. By way of illustrative example, and with continued reference to FIG. 1, display device 12A may be configured as a conventional smartphone device characterized by a processor, a memory containing operating software as well as executable software applications, a GPS receiver, a display, an alphanumeric input and/or touchscreen, and a wireless transceiver for interacting with the base station of a cellular network to set up a link 32 over which an internet connection to network interface 16 of administration server 14. Display device 12B, on the other hand, may be configured as a computer tablet device supported by a cellular carrier and equipped with the same generic components as a smartphone.

Devices 12C, 12D and 12E can, but need not be, configured as smartphone or table computer devices supported by a cellular carrier network. In the illustrative configuration shown in FIG. 1, each of these devices is configured with a suitable wireless transceiver for utilizing a corresponding wireless local area network link 34 which may be, for example, an IEEE 802.11 RF link. In this regard, devices 12C-12E may be configured as special-purpose devices. In the present inventor's co-pending U.S. patent application Ser. No. 13/196,342, the entire disclosure of which is expressly incorporated herein by reference, there are disclosed special purpose pass devices which further include a display, memory, power source, transceiver, an on/off slide switch for energizing and de-energizing the device, and optionally, a display screen select pushbutton for allowing the user to toggle between a first display screen, and one or more additional screens. In any event, via link 34, each devices as device 12C is capable of interacting with administrative server 14 via a link to the internet 38 established via base station 36 and associated local terminal 40.

In accordance with an optional aspect of the present invention, credential management system 10 further includes a credential application download server 50 which includes a network interface and a downloadable credential application program file 54. In a conventional manner, a portable electronic device as smartphone device 12A may access an online marketplace such, for example as the Google Apps Marketplace or the Apple® iStore, and download an executable program which, when executed by a device such as device 12A, allows administration server 14 to interact and update device 12A as a credential in accordance with the teachings of the present invention.

Where smartphone devices are employed as secure electronic credentials in accordance with the present invention, the executable software program is preferably configured to prompt the user to decide whether to accept or reject the call. If the call is accepted, the program suspends further display of the credential (including both the visible symbol and any accompanying graphics corresponding to a ticket, pass, permit, or license being represented) until the call terminates and then automatically resumes the display. To increase visibility

US 9,047,715 B2

7

of the credential for all visibility conditions, the brightness of the display is set at a relatively high level at all times unless and until overridden by the user. Special purpose embodiments of the display devices, on the other hand, may incorporate a high contrast electrophoretic display.

In any event, having now described the various components of an illustrative credential administration system constructed in accordance with the present invention, the administration and managing of portable electronic display devices using such a system will now be described in detail.

With reference now to FIG. 2, it will be seen that the process commences at block 60 and passes, at block 62, whereupon a client management portal of the administration server is accessed by the administrator. Using the client management portal, client records are either created or updated, via a series of input screens exemplified by FIGS. 3A and 3B. In the embodiment of FIGS. 2, 3A and 3B, it is contemplated that the credential administration needs of a plurality of client entities may be served by a single administration platform. In this regard, a single administration server as administration server 10 (FIG. 1) can support multiple categories of client organizations as well as multiple organizations in a single category. An example of the former would be a platform supporting law enforcement agencies, government benefit administration agencies, multinational corporations, professional sports organizations such as the National Football League (NFL). An example of the latter would be a platform supporting the site security needs of one or more multinational corporations. It suffices to say that credential management systems constructed in accordance with the teachings of the present invention are scalable to accommodate the particular needs of the client application(s).

In any event, the process continues to block 64 at which point a client record is either created or updated. As shown in FIG. 3A, an administrator can access a first client management screen 640 to determine whether a particular client has already been set up in the system. This is performed by clicking on a "Clients" tab indicated generally at reference numeral 642, at which point a list of clients is presented to the administrator. Illustratively, the list of clients displayed can be narrowed as the administrator begins typing a part of the client's name in client management field 644. In this case, typing the letter "N" causes the names of three pre-existing clients that have already set up in a client database. By clicking on one of the three entries, the administrator is presented with an opportunity to edit or add information for the selected client. As shown in FIG. 3B, each client record includes such data as the client name, file address for specifying a logo, the business address, the telephone number, and the e-mail address of the designated corporate contact. After entering any new data, the client file record is updated by clicking upon "save" button 646.

At decision block 66, a determination is made as to whether additional client records or updates are required. If so, the process returns to block 64, but if not the process proceeds to block 68. In the illustrative embodiment of FIGS. 2, 4A and 4B, a credential administration and management system is used to set up devices which will serve as credentials for entering an event such, for example, as football game or a concert, and for displaying indicia representative of the capacity in which the wearer or presenter of the device is serving (e.g., member of staff, press, performer etc.). Thus, as shown in block 68 of FIG. 2 and in FIGS. 4A and 4B, an administrator having clicked on the "Events" tab is presented with the opportunity to display upcoming events (events for which one or more entries already exist) and to either modify them, cancel them, or supplement them with additional

8

events. The process advances to block 70 for creation of or updates to a particular event record. FIG. 4A depicts a listing of upcoming events, as well as the date and time for which these events are scheduled. By clicking on client tab 684, the administrator can associate a new event entry (entered in field 686) with a particular client. The various details to be entered for each event are shown FIG. 4B. The start and end times for the event, for example, are entered via field 688. In embodiments of the present invention in which the devices distributed to users are instructed to display a sequence of visual symbols for the duration of an event, reference may be made to the entered start and end time data.

Returning to FIG. 2, it will be seen that at decision block 72, if there are further event records to be created or updated, the process returns to block 70, but if not then the process advances to block 74. At block 74, the user management portal of the credential administration server is accessed and, at block 76, a user record is created or updated. In this regard, it is understood that a user is the person on whose behalf a portable credential management device is to be administered and updated in accordance with the present invention. To this end, an association is created, in authorized user database 22 (FIG. 1), between unique identifiers (as, for example, the IP address, telephone number, mobile electronic serial number or ESN, or an RFID) and corresponding portable electronic display devices. As best seen in FIG. 5A, a typical entry for a particular authorized user may include the user's name, the type of display device assigned to or owned by the user, an email address for the user, and a telephone number associated with the user or with the display device itself (in the case of smartphones and the like). FIG. 5B depicts the screen accessed by the administrator to add a new user, while FIG. 5C depicts the screen used by the administrator to assign users to a specific event and/or client. Finally, FIG. 5D is a screen which allows the user to see, at a glance, the entirety of a given user's record.

In a manner which will soon be described, during an event or for a specified time period, a series of visual symbols are chosen and "pushed" to respective portable display devices. During a given time interval, each portable display device of a group of devices (for example, a plurality of devices associated with a given client or group of clients) are assigned a unique visual symbol. For example, for a given scheduled event, no two portable electronic display devices are sent the same visual symbol for display as a credential. As part of each user's record, the most recent visual symbol pushed to the corresponding display device is stored and, optionally, the immediately preceding visible symbol (or symbols) may also be stored. In addition to the visual symbol, other data and images may be pushed by credential management and administration system 10 (FIG. 1) to each portable electronic display device. Images files corresponding to the respective visual components making up an identification card, entry pass, license, and so on, for example, can be sent to each device with an instruction to display any combination of the foregoing. By updating this information at periodic, finite, intervals, it is possible to create a secure and unique "document" which is not readily subject to forgery or duplication.

The aforementioned capabilities are exemplified by FIG. 6 wherein it will be seen that a process of periodically pushing credential updates to a portable electronic device commences at start block 82 and then advances to block 84 wherein an administrator operates the system to schedule an event and to associate a user with a corresponding, unique portable device identifier (ID). At block 86, a time interval counter N is initialized and set to zero. While each time interval might, for example, be on the order of five to ten minutes, intervals of up

US 9,047,715 B2

9

to one hundred hours or more are possible. The principal advantage to intervals of shorter duration is that may provide a greater disincentive to would-be duplicators. It should also be mentioned that there is no requirement that the time intervals be of constant duration. Thus for example, each time interval may be randomly selected so as to be shorter or longer than the one which preceded it.

In any event and with continued reference to FIG. 6, it will be seen that the process then advances to block 88 wherein the interval counter is advanced by one, and thereafter to block 90 at which time credential management system 10 obtains and transmits the next visual symbol to be displayed by a particular portable display device (e.g., device 1). The same visual symbol obtaining and transmitting step is performed for devices 2 through M as exemplified by blocks 92 and 94. At decision block 96, a decision is made as to whether the event is still ongoing at the expiration of the first time interval, and if so, the process returns to block 88 and the interval counter N increments by one so that the steps (90-94) or updating display devices 1-M with respectively new visual symbols can be repeated. If it is determined that the event has terminated, on the other hand, the process ends at block 100.

Turning now to FIG. 7, it will be seen that a process of facilitating authentication of portable electronic devices presented as credentials in accordance with an aspect of the present invention commences at block 102 and advances to block 104 wherein a request is received to authenticate a portable electronic credential device. By way of illustrative example and with momentary reference to FIG. 1, the authentication process may be initiated when a visual symbol displayed by a portable electronic display device as device 12A is scanned (e.g., by security staff) by a conventional bar code scanner indicated generally at reference numeral 41 and associated with remote terminal 40. Alternatively, a passive RFID scanner may detect the presence of a portable electronic display device and trigger an authentication request via remote terminal 40. At decision block 106, an initial decision is made as to whether the visual symbol specified in a request is valid during the current time interval for any of the devices managed by the credential management and administration system, or whether it has already been used to gain access to the event. If the symbol is not valid or has already been used, a rejection decision is transmitted to the requesting terminal (block 112), a record of the attempt is made, and the process ends at block 116. If the reason for the rejection was due to prior use of the same visual symbol by a different device, this reason is transmitted as part of the rejection decision notification. Likewise, if visual symbol was not valid, then this information is returned as part of the rejection decision.

If, on the other hand, it is determined at block 106 that the visual symbol is valid for any administered display device (i.e., one for which a user or unique ID entry exists in the system), then the process advances to decision block 108. At decision block 108, a determination is made as to whether the visual symbol presented during the authentication request matches the unique device id and/or user to which it is assigned in the records of authorized user database 22 (FIG. 1). If the outcome is no, the process proceeds to blocks 112, 114, and 116 as described previously. However, if the outcome is yes, an acceptance decision is transmitted (block 110), the process advances to block 114 where in the client/user/event records are updated accordingly, and then the process terminates at block 116.

FIG. 8 depicts a process of operating a credential management and administration server to update user records using user location/mobility data. The location data can take the form of either obtaining location data directly from devices

10

such as devices 12A-12E (FIG. 1) (as might be obtained when the devices are equipped with GPS receivers) or by remote fixing using transmission signal triangulation or other conventional means. In any event, the process is entered at block 120 and advances to block 122, whereupon the position data is retrieved for portable credential devices during, for example, an event or within a specified time range during which devices as devices 12A-12E are being used as credentials in accordance with the present invention. The process then advances to block 124 whereupon the user records are updated to reflect time spent at each of a plurality of locations of interest specified by the administrator (and, in turn, by the client).

By way of illustrative example, a client may be interest in knowing how much time users spend waiting at line at specific locations (snack bar, souvenir shop, benefits window) or how long a staff member spent at a particular part of a building. To facilitate detailed reports which include such socio-demographic data as household income, gender, marital status and the like, the administrator may additionally include such information as part of each user's data record. To this end, at block 126 a report is generated which graphically presents an average amount of time spent, by users in at least one socio-demographic group, at locations of interest. This may be during a specific event or within a specific date range, as the case may be. It is further possible to collect user location data during additional events or over specific blocks of time (block 128) and updating the user records with the additional data (block 130) so that reports aggregating data from multiple events or dates/times can be generated (block 132). When all desired data entry and/or reporting activity is completed, the process terminates at block 134.

In FIG. 9 there is shown a modified embodiment of the configuration management system depicted in FIG. 1, wherein like elements are identified by like numerals. In the embodiment of FIG. 9, the portable electronic display devices as devices 12A'-12E' are pre-configured with the program for executing the program which enables them to be administered by system 10'.

Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

What is claimed:

1. A non transitory computer-readable storage medium encoded with computer-executable instructions which, when executed by a processor, perform a method for configuring a portable electronic device as part of a credential management system, comprising:

associating at a credential administration server, a first portable electronic device, identifiable by a unique identifier, with a first user and at least one of a location or a service subject to access restrictions;

obtaining first visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a first machine discernable image to be presented as an access credential by the first user during a first specified time interval, the first time interval being specified to have a duration of between 30 to 6000 seconds;

for visible display of the first machine discernable image by the first portable device during the first time interval,

US 9,047,715 B2

11

initiating wireless transmission of the obtained first visual symbol information to the first portable electronic device;

obtaining second visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a second machine discernable image to be presented as an access credential by the first user during a second specified time interval, the second time interval being specified to have a duration of between 30 to 6000 seconds; and

for visible display of the second machine discernable image by the first portable electronic device upon expiration of the first time interval, initiating wireless transmission of the obtained second visual symbol information to the first portable electronic device.

2. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the first visual symbol information with the first user during the first time interval.

3. The computer-readable storage medium according to claim 2, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the second visual symbol information with the first user during the second time interval.

4. The computer-readable storage medium according to claim 3, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the first visual symbol information with the first user during the second time interval, thereby facilitating authentication of the first user if the second visual symbol information is not received by the first portable electronic device.

5. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, specify that the first time interval and the second time interval are of equal duration.

6. The computer readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform a step of randomly selecting, at the credential administration server, the first and second time intervals such that they are of unequal duration.

7. The computer-readable storage medium according to claim 1, wherein the first portable electronic device includes a processor, a power source, and a display for visually reproducing the first and second machine discernable images.

8. The computer-readable storage medium according to claim 7, wherein computer instructions stored therein, when executed by a processor, further perform a step of transmitting a generation instruction to the first portable electronic device, the first portable electronic device being responsive to each generation instruction received to locally generate a corresponding bar code as the machine discernable image.

9. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform receiving and storing, at the credential administration server, administrator input specifying at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an event.

10. The computer-readable storage medium according to claim 9, wherein computer instructions stored therein, when executed by a processor, further perform transmitting, to the first portable device, information representative of at least one

12

of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an event.

11. The computer readable storage medium according to claim 1, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

12. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform receiving from the first portable electronic device, information specifying at least one of the unique identifier, an event to be attended by the first user, and first and last names of the first user.

13. The computer-readable storage medium according to claim 7, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

14. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform

associating at a credential administration server a second portable electronic device, identifiable by a unique identifier, with a second user and at least one of a location or a service subject to access restrictions;

obtaining third visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a third machine discernable image to be presented by the second user as an access credential during the first time interval;

for visible display of the third machine discernable image by the second portable device during the first time interval, initiating wireless transmission of the obtained third visual symbol information to the second portable electronic device;

obtaining fourth visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a fourth machine discernable image to be presented by the second user as an access credential during the second time interval; and

for visible display of the fourth machine discernable image by the second portable device commencing at expiration of the first time interval, initiating wireless transmission of the fourth visual symbol to the second portable electronic device.

15. The computer-readable storage medium according to claim 14, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information with the second user during the first time interval.

16. The computer-readable storage medium according to claim 15, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information and the fourth visual symbol information with the second user during the second time interval, thereby facilitating authentication of the second user during the second time interval in the event the fourth visual symbol information is not received by the second portable electronic device.

US 9,047,715 B2

13

17. The computer-readable storage medium according to claim 14, wherein obtaining each of said first and said second visual symbol information includes generating first bar code information and second bar code information, respectively and wherein obtaining each of said third and said fourth visual symbol information includes generating third and fourth bar code information, respectively, thereby facilitating display of a respectively different bar code by each portable electronic device during each corresponding time interval.

18. The computer-readable storage medium according to claim 1, wherein obtaining each of said first and said second visual symbol information includes generating first bar code information and second bar code information, respectively, thereby facilitating display of a different bar code by the first portable electronic device during each corresponding time interval.

19. A method for configuring a plurality of portable electronic devices having a memory, a transceiver, and a display, using a credential management system, comprising:

associating at a credential administration server a first portable electronic device, identifiable by a unique identifier, with a first user and at least one of a location or a service subject to access restrictions;

obtaining first visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a first machine discernable image to be presented as an access credential by the first user during a first specified time interval, the first time interval being specified to have a duration of between 30 to 6000 seconds;

providing instructions executable by the first portable electronic device for causing display of the first machine discernable image by the first portable device during the first time interval;

wirelessly transmitting the first visual symbol information to the first portable electronic device;

obtaining second visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a second machine discernable image to be presented as an access credential by the first user during a second specified time interval, the second time interval being specified to have a duration of between 30 to 6000 seconds;

providing instructions executable by the first portable electronic device for causing display of the second machine discernable image by the first portable device during the second time interval commencing at expiration of the first time interval, and

wirelessly transmitting the second visual symbol information to the first portable electronic device.

20. The method according to claim 19, further comprising a step of associating, at the credential administrative server, the first visual symbol information with the first user during the first time interval.

21. The method according to claim 20, further comprising a step of associating, at the credential administration server, the second visual symbol information with the first user during the second time interval.

22. The method according to claim 20, further comprising a step of associating, at the credential administration server, the first visual symbol information with the first user during the second time interval, thereby facilitating authentication of the first user during the second interval if the second computer-readable visual symbol is not received by the first portable electronic device.

14

23. The method according to claim 19, wherein the first time interval and the second time interval are of equal duration.

24. The method according to claim 19, further including a step of randomly selecting, at the credential administration server, each of the first and second time intervals such that they are of unequal duration.

25. The method according to claim 19, wherein each of the first and second visual symbols are bar codes, the method further including a step of initiating, from the credential administration server, transmission of a generation instruction to the first portable electronic device and the first portable electronic device being responsive to each generation instruction received to locally generate and display a corresponding bar code as the machine discernable image.

26. The method according to claim 19, further including a step of receiving and storing, at the credential administration server, administrator input specifying at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an identified event.

27. The method according to claim 26, further including a step of transmitting, to the first portable device, information representative of at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an identified event.

28. The method according to claim 26, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

29. The method according to claim 28, further including a step of receiving from the first portable electronic device, information specifying at least one of the unique identifier, an event to be attended by the first user, and first and last names of the first user.

30. The method according to claim 19, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

31. The method according to claim 19, further including:

associating at a credential administration server a second portable electronic device, identifiable by a unique identifier, with a second user and at least one of a location or a service subject to access restrictions;

obtaining third visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a third machine discernable image to be presented as an access credential by the second user during the first specified time interval;

providing instructions executable by the second portable electronic device for causing display of the third machine discernable image by the second portable device during the first time interval;

wirelessly transmitting the third visual symbol information to the second portable electronic device;

obtaining fourth visual symbol information, at the credential administration server, for use by the second portable

US 9,047,715 B2

15

electronic device in initiating display of a fourth machine discernable image to be presented as an access credential by the second user during the second specified time interval;

providing instructions executable by the second portable electronic device for causing display of the fourth machine discernable image by the second portable device during the second time interval commencing at expiration of the first time interval, and

wirelessly transmitting the fourth visual symbol information to the second portable electronic device.

32. The method according to claim 31, further including a step of associating, at the credential administration server, the third visual symbol with the second user during the first time interval.

33. The method according to claim 32, further including a step of associating, at the credential administration server, the third visual symbol and the fourth visual symbol with the second user during the second time interval, thereby facilitating authentication of the second user during the second interval in the event the third visual symbol is not received by the second portable electronic device.

34. The method according to claim 31, further including a step of facilitating authentication of a candidate portable electronic device displaying a machine discernable image as a credential by determining, in a first determining step, whether the candidate portable electronic device is identifiable by a unique ID associated with an authorized user; and determining, in a second determining step, whether the machine discernable displayed by the candidate portable electronic device corresponds to a visual symbol valid for an authorized user during a current time interval.

35. The method according to claim 34, wherein if the candidate portable electronic device is identifiable by a unique ID associated with the first user and the received data is representative of a visual symbol valid during a current time interval, updating a record associated with the first user to reflect at least one of the time, date, location and event where the first portable electronic device was presented as a credential.

36. The method according to claim 35, further including a step of communicating an acceptance decision to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.

37. The method according to claim 34, wherein if the candidate portable electronic device is identifiable by a unique ID associated with the first user and the received data is representative of a visual symbol valid during a current time interval or an immediately preceding time interval associated with the first user, updating a record associated with the first user to reflect at least one of the time, date, location and event where the first portable electronic device was presented as a credential.

38. The method according to claim 34, wherein if the candidate portable electronic device is not identifiable by a unique ID associated with an authorized user or if the received data is not representative of a visual symbol valid during a current time interval and associated with any authorized user, communicating a rejection decision to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.

39. The method according to claim 19, wherein the first portable electronic device includes a global positioning satellite (GPS) receiver operative to obtain positional data and a corresponding cellular network transceiver for establishing a telecommunications link with a cellular network to thereby transmit position data for monitoring a location within a

16

facility to which the first user has gained access using the first portable electronic device as a credential, said method further including a step of storing a record of locations visited by the first user while the first user is present at the facility.

40. The method according to claim 39, further including a step of generating a report graphically presenting an average time spent, at respectively specified locations within a facility, by users presenting a portable electronic device as a credential.

41. A method for configuring portable electronic devices each having a memory, a transceiver, and a display, using a credential management system, comprising:

obtaining first information corresponding to a first machine discernable image to be used by a first user during a specified first time interval of specified duration;

providing first instructions executable by a first portable electronic device associated with the first user for causing presentation of the first machine discernable image by the first portable device during the first time interval; wirelessly transmitting the first information to the first portable electronic device;

obtaining second information corresponding to a second machine discernable image to be used by the first user during a second specified time interval of specified duration;

providing second instructions executable by the portable electronic device for automatically causing presentation of the second machine discernable image by the first portable device during the second time interval commencing at expiration of the first time interval;

wirelessly transmitting the second symbol information to the first portable electronic device; and

transmitting over a communication network from a credential administrative server, data to be displayed by the first portable device during the first and second time intervals and together with each machine discernable image, the data including

an assigned seating location, an event start time, an event date, and names of competing teams, or

an identity of an issuing authority, or

an identity of a transportation carrier, a departure date, a departure time, and a gate assignment;

whereby the first portable device is caused, by execution of the first instructions, to cease presenting the first machine discernable image at expiration of the first time interval, and

whereby the first portable device is caused, by execution of the second instructions, to commence presenting the second machine discernable image, at initiation of the second time interval.

42. The method of claim 41, further including a step of updating data to be displayed by the first portable device by transmitting, from the credential administrative server, at least one of a changed seating assignment, a changed gate assignment, and a changed departure time.

43. The method of claim 42, further including a step of transmitting one of an e-mail and a text message to a user of the first portable device as notification of any transmission of updating data.

44. The method of claim 41, wherein each of the first and the second machine discernable image is a respective bar code displayed continuously during the first interval and the second interval, respectively.

45. The method of claim 41, further including a step of collecting, from each respective portable electronic device, data corresponding to time spent by a corresponding user at one or more locations within a facility and to which the

US 9,047,715 B2

17

corresponding user has gained access after using a corresponding portable electronic device as a credential to enter the facility.

46. The method of claim 45, further including a step of generating a report graphically presenting average time spent, 5 by respective socio-demographic groups of users who presented a portable electronic device as a credential to gain access to an event, at the one or more specified locations.

* * * * *

18



● **Alan Amron** <alanamron@yahoo.com>

To: Alan Littmann

Cc: Iveta Saksone, Chris Van Dam

Bcc: Philip Josephson, David robotvillage.com, Richard Grobman, Brian Woods



Fri, Apr 7 at 8:29 AM



Dear Mr. Littmann,

Thank you for your email invitation to speak next week. However, I would like to keep our correspondence in writing for now.

I have downloaded the MLB Angels Stadium ticket app (which operates by updating the digital barcode from a static one to a rotating one that cannot be duplicated) and find that it literally reads on at least one of my issued 2015 patented claims.

That said, MLB can benefit from this opportunity, which is my unusual offer of a free life of the patents (9 more years) license to the Major League Baseball Angels Stadium digital ticketing, with “updating the digital barcode from a static one to a rotating one that cannot be duplicated”.

If you choose to accept this offer, let me know, and when we receive the revival documents from the PTO, we will enter into a formal license with no money down and no percentage royalty for the life of the patents (9 more years).

Sincerely,

Alan

Alan Amron (Inventor/Founder)

eChanging Barcode, Inc.

103 Jessup Ave

Suite Box 354

Quogue, New York 11959

USA

+1 (929) 250-3650

<http://www.eChangingBarcode.com> (site not yet published)

"We are the digital age version of today's stagnant still static barcodes, updating the digital barcode from a static one to a rotating one that cannot be duplicated."

On Thursday, April 6, 2023, 7:35 PM, Alan Littmann <alittmann@goldmanismail.com> wrote:

Mr. Amron,

I am available to talk next week if you like. Please let me know if 3:30pm ET on 4/13 or 2pm ET on 4/14 work for you.

Sincerely,

Alan



● Alan Amron <alanamron@yahoo.com>

To: Alan Littmann

Cc: Iveta Saksone, Chris Van Dam

Dear Mr. Littmann,

I hope this email finds you well. I am pleased to inform you that my Petition to revive has been granted. I am writing to inquire as to whether you are still my MLB direct contact.

I would now be willing to discuss the details over a phone call. I propose this exclusive to MLB offer:

1. Granting the Angels a free 8-year license (life of the patent) to use the 9,047,715 dynamic barcodes patent, specifically designed to prevent digital ticket fraud.
2. The remaining 29 teams in the MLB would pay a small one-time fee of \$2,500 per team (\$72,500 in total) for a 8-year license (life of the patent) to use the 9,047,715 dynamic barcodes patent, effectively preventing digital ticket fraud across the entire league.
3. We can issue a joint press release regarding our collaboration; however, the financial details of the agreement will not be disclosed.

Here's a proposed joint press release:

"Major League Baseball and eChanging Barcodes, LLC have reached an agreement to utilize the patented 9,047,715 dynamic barcodes technology, enhancing security and preventing fraud in digital ticketing for all MLB teams.

As part of this effort, all 30 MLB teams will have access to a 8-year license, ensuring the safety and integrity of digital ticketing.

This reflects our shared dedication to providing fans with an exceptional experience while safeguarding the authenticity of digital ticketing."

Sincerely,

Alan Amron

eChanging Barcodes, LLC.

New York, NY 11959

(929) 250-3650

<http://www.DynamicBarcodes.com>

Download the
Official App



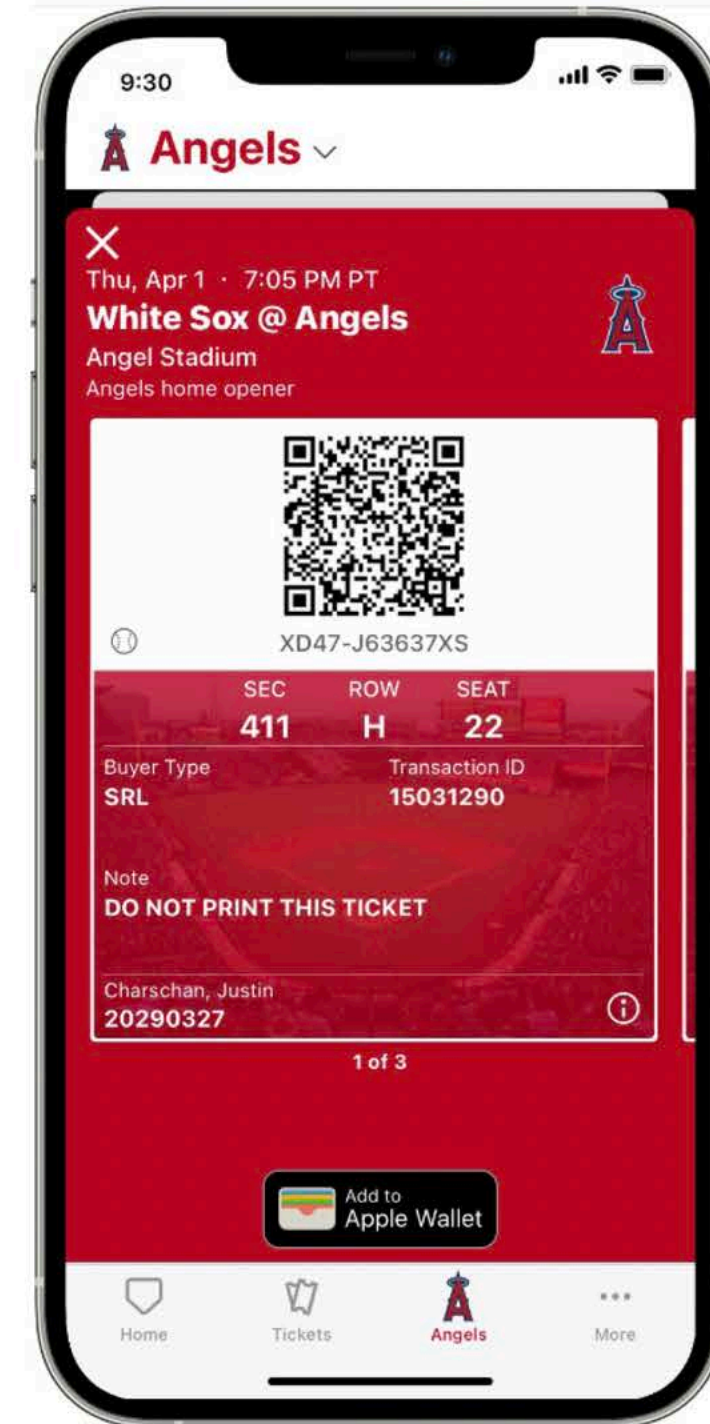
Don't Strike Out at the Gate

MLB has launched Protect the Barcode technology at Angel Stadium, updating the digital barcode from a static one to a rotating one that cannot be duplicated. Ensure that you've got the most recent version of the Ballpark App on your mobile device, so that you can benefit from having this new, secure technology! The new, rotating barcode ensures that you have a genuine ticket and that you won't have any issues at the gate on Game Day. Look for the moving baseballs next to your barcode and know that you're good to go.

Tickets forwarded through the Ballpark app are protected, as well. Just make sure that you don't send your friends and family a ticket screenshot because **screenshots of Ballpark app digital tickets will no longer be accepted as a valid method of entry into the stadium.**

MLB
Download the
Official App

TICKET



● Re: Patents / MLB



● Alan Amron <alanamron@yahoo.com>

To: Alan Littmann

Cc: Iveta Saksone, Chris Van Dam



Wed, Nov 8 at 10:06 PM ☆

Mr. Littmann,

Thank you for your quick response. I will be available to discuss this matter with you on Monday November 13, 2023 at 11:00 am New York time.

Sincerely,

Alan Amron

On Wednesday, November 8, 2023, 8:02 PM, Alan Littmann <alittmann@goldmanismail.com> wrote:

Mr. Amron,

I remain the contact on behalf of MLB. I am available to discuss this matter on Friday afternoon or Monday morning. Please let me know if either of those windows work.

Sincerely,

Alan

Alan Littmann200 South Wacker Dr., 22nd Floor, Chicago, IL 60606

P 312-881-5969 C 312-404-1871 F 312-380-7019

goldmanismail.com**GOLDMAN ISMAIL TOMASELLI BRENNAN & BAUM LLP**

The information contained in this communication is confidential and should be considered to be attorney work product and/or attorney-client privileged. This communication is the property of Goldman Ismail Tomaselli Brennan & Baum LLP and is intended only for the use of the addressee. If you are not the intended recipient, please notify the sender, delete the message, and note that any distribution or copying of this message is prohibited. Any discussion of tax matters contained herein is not intended or written to be used, and cannot be used, for the purpose of avoiding any penalties that may be imposed under federal tax laws.

Patent Infringement Analysis Report

November 9, 2023

Introduction

This report analyzes whether MLB's digital ticketing technology infringes on issued US Patent No. 9,047,715, titled "SYSTEM AND METHOD FOR CREDENTIAL MANAGEMENT AND ADMINISTRATION." The patent describes a system and method for managing and administering digital access credentials, such as digital tickets.

MLB's digital ticketing technology allows users to purchase and download digital tickets to MLB games on their smartphones. The app then generates a unique mobile ticket barcode for each ticket. The mobile ticket barcode is constantly rotating, making it difficult to counterfeit.

INDEX

Page

Introduction	Cover
Section A	Patent claims analyzed and compared to MLB uses ... 2
Summary of the key points	2
Section B	Patent claims analyzed and explained ... 5
Section C	Actual patent claims as written in patent 715 ... 11
Section D	Comparisons Charts Patent Infringement Analysis Report 19
Claim Chart	20
Discussion of Claims	22
Conclusion	23
Limitations	23
Recommendations	23
Additional Suggestions	23
Final Introduction	23
Final Claim Chart	24
Final Discussion of Claims	28
Final Conclusion	28
Final Recommendations	28
Images	29

Here's a simplified patent infringement analysis of how MLB's digital ticketing technology aligns with and or literally infringes one or more of the 46 claims in the 9,047,715 issued patent:

SECTION A

Patent claims analyzed compared to MLB uses

The Amron 715 patent is a digital age version of today's stagnant still static barcodes, **updating the digital barcode**, QR code, Alphanumeric or any discernable image **from a static one to a rotating one that cannot be duplicated** to prevent digital ticket fraud.

“MLB has launched Protect the Barcode technology at Angel Stadium, **updating the digital barcode from a static one to a rotating one that cannot be duplicated**. Ensure that you've got the most recent version of the Ballpark App on your mobile device, so that you can benefit from having this new, secure technology! The new, rotating barcode ensures that you have a genuine ticket and that you won't have any issues at the gate on Game Day. Look for the moving baseballs next to your barcode and know that you're good to go.” MLB.com

Summary of the key points to be shown below:

- MLB's Protect the Barcode technology is a digital age version of the Amron 715 patent, which updates digital barcodes from static to rotating to prevent fraud.
- MLB's ticket technology configures a portable electronic device (via the MLB Ballpark app) to display a machine-discernible image (MLB mobile ticket barcode) during a specified time interval (MLB is changing the barcode every many seconds time interval).
- MLB's ticket technology involves the transmission of generation instructions to the portable electronic device (via the MLB Ballpark app), which locally generates a corresponding barcode (machine-discernible image) for the access credential (MLB digital ticket).
- MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with event information (game details), which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine-discernible image (mobile ticket barcode).
- MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with areas of a facility (stadium sections) to which the user is authorized for entry, which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine-discernible image (mobile ticket barcode).
- MLB's ticketing system involves the receipt and storage of administrator input specifying the details of the credentials (digital tickets) to be distributed. This information is then transmitted to the portable electronic device (via the MLB Ballpark app) for display as machine-discernible images (mobile ticket barcodes).
- MLB's ticketing system includes the receipt and storage of user input specifying user information (such as personal details or preferences), which is then transmitted to the credential administration server for association with the user's account.

1. Claim 1: MLB's ticket technology configures a portable electronic device (via the MLB Ballpark app) to display a machine discernable image (MLB mobile ticket barcode) during a specified time interval being specified to have a duration of seconds (MLB is changing barcode every many seconds time interval).

8. Claim 8: MLB's ticket technology involves the transmission of generation instructions to the portable electronic device (via the MLB Ballpark app), which locally generates a corresponding barcode (machine discernable image) for the access credential (MLB digital ticket).

9. Claim 9: MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with event information (game details), which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine discernable image (mobile ticket barcode).

11. Claim 11: MLB's ticket technology generates visual symbol information (mobile ticket barcode) associated with areas of a facility (stadium sections) to which the user is authorized for entry, which is transmitted to the portable electronic device (via the MLB Ballpark app) for display as a machine discernable image (mobile ticket barcode).

12. Claim 12: MLB's ticketing system involves the receipt and storage of administrator input specifying the details of the credentials (digital tickets) to be distributed. This information is then transmitted to the portable electronic device (via the MLB Ballpark app) for display as machine discernable images (mobile ticket barcodes).

13. Claim 13: MLB's ticketing system includes the receipt and storage of user input specifying user information (such as personal details or preferences), which is then transmitted to the credential administration server for association with the user's access credentials (digital tickets).

Claims 14-18: These claims primarily focus on the use of a computer-readable storage medium to store instructions for executing the credential management system and method. While the specific implementation details are not provided, it can be inferred that MLB's ticketing system likely utilizes a computer-readable storage medium to store the necessary instructions and data for managing and administering digital tickets.

Claims 19-25: These claims cover the method of configuring multiple portable electronic devices using the credential management system. MLB's ticketing system, through the MLB Ballpark app, likely allows for the configuration and association of multiple devices (such as smartphones) with different users, enabling the distribution and display of machine discernable images (mobile ticket barcodes) on those devices during specific time intervals.

21. Claim 21: MLB's ticketing system associates the second visual symbol information (mobile ticket barcode) with the first user during the second time interval. This allows for authentication in the event that the second visual symbol information is not received by the first portable electronic device (via the MLB Ballpark app).

22. Claim 22: MLB's ticketing system facilitates authentication by associating the first visual symbol information (mobile ticket barcode) with the first user during the second time interval, in case the second visual symbol information is not received by the first portable electronic device (via the MLB Ballpark app).

23. Claim 23: MLB's ticketing system utilizes time intervals of equal duration for the display of machine discernable images (mobile ticket barcodes). This ensures consistency in the validity period of the digital tickets.

24. Claim 24: MLB's ticketing system incorporates the random selection of time intervals of unequal duration for displaying machine discernable images (mobile ticket barcodes). This variability in time intervals adds an additional layer of security to the digital tickets.

25. Claim 25: MLB's ticketing system employs barcodes as visual symbols (mobile ticket barcodes) and transmits generation instructions to the portable electronic devices (via the MLB Ballpark app) for locally generating and displaying the corresponding barcodes (machine discernable images).

Claims 26-30: These claims highlight additional features of the credential management system and method. While the specific implementation details are not provided, it can be inferred that MLB's ticketing system may incorporate some aspects covered by these claims, such as receiving and storing administrator input specifying event details and user information, transmitting this information to portable devices, using different types of portable electronic devices and unique identifiers, and receiving information from the portable devices.

31. Claim 31: MLB's ticketing system associates a second portable electronic device (such as a friend's smartphone) with a second user, obtains visual symbol information (mobile ticket barcode) for use by the device during the first- and second-time intervals, and wirelessly transmits the visual symbol information to the device (via the MLB Ballpark app).

32. Claim 32: MLB's ticketing system associates a third visual symbol (mobile ticket barcode) with the second user during the first-time interval. This ensures that the second user can authenticate themselves if the second visual symbol is not received by their portable electronic device.

33. Claim 33: MLB's ticketing system associates a third and fourth visual symbol (mobile ticket barcode) with the second user during the second time interval. This facilitates authentication in case the third visual symbol is not received by the second portable electronic device (via the MLB Ballpark app).

34. Claim 34: MLB's ticketing system facilitates authentication of a portable electronic device (such as a smartphone) displaying a machine discernable image (mobile ticket barcode) as a credential. It determines whether the device is identifiable by a unique ID associated with an authorized user and whether the displayed visual symbol is valid for the authorized user during the current time interval.

Claims 35-37: These claims cover additional aspects of the credential management system and method that may not directly align with MLB's ticketing system, such as communication of acceptance/rejection decisions and updating of records associated with users. However, MLB's ticketing system may incorporate some similar functionalities without precisely aligning with these claims.

Claims 37-41: These claims introduce further aspects of the credential management system and method, such as communication of rejection decisions, monitoring user location using GPS, generating reports on user behavior, and configuring portable electronic devices for presenting machine discernable images. While MLB's ticketing system may not directly align with these specific functionalities, it may have its own mechanisms and processes for managing ticketing and user behavior.

Claims 42-46: These claims cover additional features of the credential management system and method, such as updating data displayed on portable devices, sending notifications to users, using barcodes as machine discernable images, collecting data on user behavior at different locations, and generating reports based on socio-demographic groups. While MLB's ticketing system may have some similarities with these claims, it may also have its unique approaches and features for managing ticketing and user data.

Major League Baseball's rotating changing barcode technology is now being used on all ball club tickets, to prevent fraud.

The MLB Ballpark app displays regular season, Postseason, Spring Training and other event tickets within the Wallet. Each ticket has a mobile ticket barcode that must be scanned for entry into the stadium via your mobile device. Within the Wallet, you can tap on an individual ticket to view its barcode. For entry to the stadium, present your mobile device with the mobile barcode open and available to scan. It is not recommended to use a screenshot of your digital ticket at the gate as it increases the chances of the ticket becoming obscured and unreadable. Your barcode includes technology to protect it, so you won't be able to use screenshots or print outs. The technology is continually updating the digital barcode from a static one to a rotating one that cannot be duplicated. Barcode scanners record and translate barcodes from the image present on the ticket into alphanumeric digits. The scanner then sends that information to a computer database, either through a wired or wireless connection. When the ticket is presented for admission, a staff member or event volunteer will scan the barcode through a scanner.

SECTION B:

Patent claims analyzed and explained

9,047,715 patent issued June 2, 2015 - 46 claims and method claims here:

ABSTRACT

A credential management and administration system and method by which the documented eligibility of persons to receive benefits, services, access to premises or events, and the like is centrally administered. In one embodiment, credentials are distributed to the individuals electronically, via communication network, to respective **portable device having a corresponding display**. Each display is configured to visually present **certain qualifying information that is updated at periodic intervals**. Alternatively, the qualifying information may be presented via wireless means to a suitable receiver proximate the location where services are delivered.

46 Claims, 10 Drawing Sheets

Please note that, the use of dynamic barcodes as machine discernable images is also covered in **Claim 1**. This claim specifies that the computer instructions stored in the non-transitory computer-readable storage medium, when executed by a processor, perform a method for configuring a portable electronic device as part of a credential management system. This method includes obtaining first visual symbol information for use by the portable electronic device in initiating display of a first machine discernable image to be presented as an access credential during a first specified time interval. The method also includes initiating wireless transmission of the obtained visual symbol information to the portable electronic device for

visible display of the first machine discernable image by the portable device during the first-time interval. In this way, claim 1 also covers the use of dynamic barcodes as machine discernable images for the access credential.

Claim 8 of the patent covers the use of dynamic barcodes as machine discernable images. It specifies that the computer instructions stored in the non-transitory computer-readable storage medium, when executed by a processor, further perform a step of transmitting a generation instruction to the portable electronic device, which is responsive to each generation instruction received to locally generate a corresponding bar code as the machine discernable image. Therefore, claim 8 covers the use of dynamic barcodes generated locally on the portable electronic device as the machine discernable image for the access credential.

While Claim 1 and Claim 8 are the most relevant claims that cover the use of dynamic barcodes as machine discernable images, there are other claims in the patent that relate to the overall credential management system and method. For example, **claim 2** covers the association of visual symbol information with specific users during a time interval, while **Claim 3** covers the association of multiple visual symbol information with a specific user during different time intervals. **Claim 4** covers the use of previously associated visual symbol information if the user fails to display the current visual symbol information during the specified time interval. **Other claims** cover various aspects of the system and method, including the association of the portable electronic device with locations or services, the random selection of time intervals, and the transmission and reception of information between the credential administration server and the portable device.

MLB is administering digital tickets using dynamic barcodes as machine discernable images to prevent fraudulent entry to baseball games through their servers.

MLB's technology is like the system and method covered in Claim 8 of the 9,047,715 patent, which covers a system for managing and administering credentials using dynamic barcodes as machine discernable images.

Therefore, MLB's technology does infringe on the patent, in which case the patent holder has grounds for legal action.

MLB's technology infringes on both **Claim 1 and Claim 8 of the 9,047,715 patent**. Claim 1 covers a method for configuring a portable electronic device for display of a machine discernable image during a specified time interval, while Claim 8 covers a system for managing and administering credentials using dynamic barcodes as machine discernable images.

MLB's technology involves both the configuration of a portable electronic device for display of a machine discernable image during a specified time interval, as well as the use of dynamic barcodes as machine discernable images for the access credentials, then it **infringes on both claims**.

Claims 5-13 of the 9,047,715 patent cover various aspects of the credential management system and method. Here is a brief summary of each claim:

- Claim 5 covers the association of a portable electronic device with a location or service subject to access restrictions, and the display of machine discernable images corresponding to the associated location or service.
- Claim 6 covers the random selection of the duration of the time intervals during which the machine discernable images are displayed.
- Claim 7 covers the association of portable electronic devices with specific users during specific time intervals, and the display of machine discernable images corresponding to the associated users.
- Claim 8, as we discussed earlier, covers the use of dynamic barcodes as machine discernable images for the access credentials.
- Claim 9 covers the generation of visual symbol information associated with event information, which is transmitted to the portable electronic device for display as a machine discernable image.
- Claim 10 covers the generation of visual symbol information associated with employer identification, which is transmitted to the portable electronic device for display as a machine discernable image.
- Claim 11 covers the generation of visual symbol information associated with areas of a facility to which the user is authorized for entry, which is transmitted to the portable electronic device for display as a machine discernable image.
- Claim 12 covers the receipt and storage of administrator input specifying the details of the credentials to be distributed, and the transmission of that information to the portable electronic device for display as machine discernable images.
- Claim 13 covers the receipt and storage of user input specifying user information, and the transmission of that information to the credential administration server for association with the user's access credentials.

Overall, claims 5-13 cover a variety of features and aspects of the credential management system and method covered in the patent.

Claims 14-18 of the 9,047,715 patent cover the use of a computer-readable storage medium to store instructions for executing the credential management system and method. Here is a brief summary of each claim:

- Claim 14 covers the use of a computer-readable storage medium for executing the credential management system and method, including associating a second portable electronic device with a second user and generating visual symbol information for use by the second device during the first- and second-time intervals.
- Claim 15 covers associating the visual symbol information with the second user during the first-time interval.

- Claim 16 covers associating the visual symbol information with the second user during the second time interval, to facilitate authentication in the event that the fourth visual symbol information is not received by the second portable electronic device.
- Claim 17 covers the use of bar code information to generate the visual symbol information for each portable electronic device, thereby allowing for the display of a different bar code by each device during each corresponding time interval.
- Claim 18 covers the use of a computer-readable storage medium to store instructions for executing the credential management system and method, including the steps of generating and transmitting visual symbol information to portable electronic devices, associating the visual symbol information with users, and validating the visual symbol information during the specified time intervals.

Overall, claims 14-18 cover the use of a computer-readable storage medium to store and execute the credential management system and method covered in the patent.

Claims 19-25 of the 9,047,715 patent cover a method for configuring a plurality of portable electronic devices using the credential management system. Here is a brief summary of each claim:

- Claim 19 covers the method of configuring a plurality of portable electronic devices using the credential management system, including associating a first portable electronic device with a first user and obtaining visual symbol information for use by the device during the first- and second-time intervals.
- Claim 20 covers associating the first visual symbol information with the first user during the first-time interval.
- Claim 21 covers associating the second visual symbol information with the first user during the second time interval.
- Claim 22 covers associating the first visual symbol information with the first user during the second time interval, to facilitate authentication in the event that the second visual symbol information is not received by the first portable electronic device.
- Claim 23 covers the use of time intervals of equal duration.
- Claim 24 covers the random selection of time intervals of unequal duration.
- Claim 25 covers the use of bar codes as visual symbols, and the transmission of generation instructions to the portable electronic devices for locally generating and displaying the corresponding bar codes.

Overall, claims 19-25 cover the method of configuring a plurality of portable electronic devices for use with the credential management system covered in the patent.

Claims 26-30 of the 9,047,715 patent cover additional features of the credential management system and method. Here is a brief summary of each claim:

- Claim 26 covers receiving and storing administrator input specifying event details and user information, such as employer identification and authorized areas of a facility.
- Claim 27 covers transmitting this information to the first portable device.
- Claim 28 covers the use of different types of portable electronic devices and unique identifiers, such as IP address, telephone number, electronic serial number, and RFID identifier.
- Claim 29 covers receiving information from the first portable electronic device, such as the unique identifier, event details, and user information.
- Claim 30 reiterates the use of different types of portable electronic devices and unique identifiers.

Overall, claims 26-30 cover additional features of the credential management system and method, including the storage and transmission of event and user information, and the use of different types of portable electronic devices and unique identifiers.

Claims 31-34 of the 9,047,715 patent cover additional aspects of the credential management system and method. Here is a brief summary of each claim:

- Claim 31 covers the association of a second portable electronic device with a second user, obtaining visual symbol information for use by the device during the first- and second-time intervals, and wirelessly transmitting the visual symbol information to the device.
- Claim 32 covers associating the third visual symbol with the second user during the first-time interval.
- Claim 33 covers associating the third and fourth visual symbols with the second user during the second time interval, to facilitate authentication in the event that the third visual symbol is not received by the second portable electronic device.
- Claim 34 covers facilitating authentication of a portable electronic device displaying a machine discernable image as a credential, by determining whether the device is identifiable by a unique ID associated with an authorized user, and whether the displayed visual symbol is valid for the authorized user during the current time interval.

Overall, claims 31-34 cover additional aspects of the credential management system and method, including the association of multiple portable electronic devices and users, and the authentication of candidate portable electronic devices.

Claims 35-37 of the 9,047,715 patent cover further aspects of the credential management system and method. Here is a brief summary of each claim:

- Claim 35 covers the computer-readable storage medium and the steps of associating a second portable electronic device with a second user, obtaining visual symbol information for use by the device during the first- and second-time intervals, and initiating wireless transmission of the visual symbol information to the device.

- Claim 36 covers the step of communicating an acceptance decision to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.
- Claim 37 covers updating a record associated with the first user if the candidate portable electronic device is identifiable by a unique ID associated with the first user and the received data is representative of a visual symbol valid during a current or immediately preceding time interval associated with the first user.

Overall, claims 35-37 cover further aspects of the credential management system and method, including the use of a computer-readable storage medium to perform certain steps, communication of acceptance decisions, and updating of records associated with users.

Claims 37-41 of the 9,047,715 patent cover additional aspects of the credential management system and method. Here is a brief summary of each claim:

- Claim 38 covers communicating a rejection decision to a remote terminal accessible by personnel if the candidate portable electronic device is not identifiable by a unique ID associated with an authorized user or if the received data is not representative of a valid visual symbol.
- Claim 39 covers the use of a GPS receiver in the first portable electronic device to obtain positional data and a corresponding cellular network transceiver for transmitting the data to monitor a user's location within a facility, and storing a record of locations visited by the user.
- Claim 40 covers generating a report graphically presenting the average time spent by users presenting a portable electronic device as a credential at specified locations within a facility.
- Claim 41 covers a method for configuring portable electronic devices using the credential management system, including obtaining information for machine discernable images to be presented during specified time intervals, providing instructions for causing presentation of the images, and transmitting data to be displayed along with the images, such as assigned seating location, event start time, event date, names of competing teams, or identity of an issuing authority or transportation carrier.

Overall, claims 37-41 cover additional aspects of the credential management system and method, including communicating rejection decisions, using GPS to monitor user location, generating reports, and configuring portable electronic devices for presenting machine discernable images.

Claims 42-46 of the 9,047,715 patent cover further aspects of the credential management system and method. Here is a brief summary of each claim:

- Claim 42 covers updating data to be displayed by the first portable device by transmitting changed seating assignment, gate assignment, or departure time from the credential administrative server.
- Claim 43 covers transmitting an email or text message to a user of the first portable device as notification of any transmission of updating data.

- Claim 44 covers using barcodes as machine discernable images displayed continuously during the first- and second-time intervals.
- Claim 45 covers collecting data corresponding to time spent by users at different locations within a facility and to which they have gained access using a portable electronic device as a credential.
- Claim 46 covers generating a report graphically presenting the average time spent by different socio-demographic groups of users who presented a portable electronic device as a credential to gain access to an event, at specified locations within a facility.

Overall, claims 42-46 cover further aspects of the credential management system and method, including updating data displayed by portable electronic devices, using barcodes as machine discernable images, collecting and analyzing data on user behavior, and generating reports based on socio-demographic groups.

The 9,047,715 patent covers the use of QR codes or other alphanumeric symbols that can be discerned by a machine, as an alternative to barcodes. These symbols are also dynamic and changing to prevent fraud, and the system includes methods for generating and transmitting the symbol information to the portable electronic devices. The system also includes a credential administration server that associates each device with a unique user and provides the changing symbol information during specified time intervals. Additionally, the system can use GPS to monitor user location and generate reports on user behavior. The patent includes multiple claims covering various aspects of the system and method, such as updating data displayed by the devices, communicating acceptance or rejection decisions, and generating reports based on socio-demographic groups.

Major League Baseball's rotating changing barcode technology is now being used on all ball club tickets, to prevent fraud.

The MLB Ballpark app displays regular season, Postseason, Spring Training and other event tickets within the Wallet. Each ticket has a mobile ticket barcode that must be scanned for entry into the stadium via your mobile device. Within the Wallet, you can tap on an individual ticket to view its barcode. For entry to the stadium, present your mobile device with the mobile barcode open and available to scan. It is not recommended to use a screenshot of your digital ticket at the gate as it increases the chances of the ticket becoming obscured and unreadable. Your barcode includes technology to protect it, so you won't be able to use screenshots or print outs. The technology is continually updating the digital barcode from a static one to a rotating one that cannot be duplicated. Barcode scanners record and translate barcodes from the image present on the ticket into alphanumeric digits. The scanner then sends that information to a computer database, either through a wired or wireless connection. When the ticket is presented for admission, a staff member or event volunteer will scan the barcode through a scanner.

SECTION C:

Actual patent claims as written in patent 715

9,047,715 patent issued June 2, 2015 - 46 claims and method claims here

ABSTRACT

A credential management and administration system and method by which the documented eligibility of persons to receive benefits, services, access to premises or events, and the like is centrally administered. In one embodiment, credentials are distributed to the individuals electronically, via communication network, to respective **portable device having a corresponding display**. Each display is configured to visually present **certain qualifying information that is updated at periodic intervals**. Alternatively, the qualifying information may be presented via wireless means to a suitable receiver proximate the location where services are delivered.

46 Claims, 10 Drawing Sheets

What is claimed:

1. A non-transitory computer-readable storage medium encoded with computer-executable instructions which, when executed by a processor, perform a method for configuring a portable electronic device as part of a credential management system, comprising:

associating at a credential administration server, a first portable electronic device, identifiable by a unique identifier, with a first user and at least one of a location or a service subject to access restrictions;

obtaining first visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a first machine discernable image to be presented as an access credential by the first user during a first specified time interval, the first time interval being specified to have a duration of between 30 to 6000 seconds; for visible display of the first machine discernable image by the first portable device during the first time interval, initiating wireless transmission of the obtained first visual symbol information to the first portable electronic device;

obtaining second visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a second machine discernable image to be presented as an access credential by the first user during a second specified time interval, the second time interval being specified to have a duration of between 30 to 6000 seconds; and for visible display of the second machine discernable image by the first portable electronic device upon expiration of the first time interval, initiating wireless transmission of the obtained second visual symbol information to the first portable electronic device.

2. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the first visual symbol information with the first user during the first-time interval.

3. The computer-readable storage medium according to claim 2, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the second visual symbol information with the first user during the second time interval.

4. The computer-readable storage medium according to claim 3, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the first visual symbol information with

the first user during the second time interval, thereby facilitating authentication of the first user if the second visual symbol information is not received by the first portable electronic device.

- 5.** The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, specify that the first-time interval and the second time interval are of equal duration.
- 6.** The computer readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform a step of randomly selecting, at the credential administration server, the first- and second-time intervals such that they are of unequal duration.
- 7.** The computer-readable storage medium according to claim 1, wherein the first portable electronic device includes a processor, a power source, and a display for visually reproducing the first and second machine discernable images.
- 8.** The computer-readable storage medium according to claim 7, wherein computer instructions stored therein, when executed by a processor, further perform a step of transmitting a generation instruction to the first portable electronic device, the first portable electronic device being responsive to each generation instruction received to locally generate a corresponding bar code as the machine discernable image.
- 9.** The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform receiving and storing, at the credential administration server, administrator input specifying at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an event.
- 10.** The computer-readable storage medium according to claim 9, wherein computer instructions stored therein, when executed by a processor, further perform transmitting, to the first portable device, information representative of at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an event.
- 11.** The computer readable storage medium according to claim 1, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.
- 12.** The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform receiving from the first portable electronic device, information specifying at least one of the unique identifier, an event to be attended by the first user, and first and last names of the first user.
- 13.** The computer-readable storage medium according to claim 7, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a

special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

14. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform associating at a credential administration server a second portable electronic device, identifiable by a unique identifier, with a second user and at least one of a location or a service subject to access restrictions; obtaining third visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a third machine discernable image to be presented by the second user as an access credential during the first time interval;

for visible display of the third machine discernable image by the second portable device during the first-time interval, initiating wireless transmission of the obtained third visual symbol information to the second portable electronic device;

obtaining fourth visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a fourth machine discernable image to be presented by the second user as an access credential during the second time interval;

and for visible display of the fourth machine discernable image by the second portable device commencing at expiration of the first-time interval, initiating wireless transmission of the fourth visual symbol to the second portable electronic device.

15. The computer-readable storage medium according to claim 14, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information with the second user during the first-time interval.

16. The computer-readable storage medium according to claim 15, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information and the fourth visual symbol information with the second user during the second time interval, thereby facilitating authentication of the second user during the second time interval in the event the fourth visual symbol information is not received by the second portable electronic device.

17. The computer-readable storage medium according to claim 14, wherein obtaining each of said first and said second visual symbol information includes generating first bar code information and second bar code information, respectively and wherein obtaining each of said third and said fourth visual symbol information includes generating third and fourth bar code information, respectively, thereby facilitating display of a respectively different bar code by each portable electronic device during each corresponding time interval.

18. The computer-readable storage medium according to claim 1, wherein obtaining each of said first and said second visual symbol information includes generating first bar code information and second bar code information, respectively, thereby facilitating display of a

different bar code by the first portable electronic device during each corresponding time interval.

19. A method for configuring a plurality of portable electronic devices having a memory, a transceiver, and a display, using a credential management system, comprising: associating at a credential administration server a first portable electronic device, identifiable by a unique identifier, with a first user and at least one of a location or a service subject to access restrictions; obtaining first visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a first machine discernable image to be presented as an access credential by the first user during a first specified time interval, the first time interval being specified to have a duration of between 30 to 6000 seconds; providing instructions executable by the first portable electronic device for causing display of the first machine discernable image by the first portable device during the first time interval; wirelessly transmitting the first visual symbol information to the first portable electronic device; obtaining second visual symbol information, at the credential administration server, for use by the first portable electronic device in initiating display of a second machine discernable image to be presented as an access credential by the first user during a second specified time interval, the second time interval being specified to have a duration of between 30 to 6000 seconds; providing instructions executable by the first portable electronic device for causing display of the second machine discernable image by the first portable device during the second time interval commencing at expiration of the first time interval, and wirelessly transmitting the second visual symbol information to the first portable electronic device.

20. The method according to claim 19, further comprising a step of associating, at the credential administrative server, the first visual symbol information with the first user during the first-time interval.

21. The method according to claim 20, further comprising a step of associating, at the credential administration server, the second visual symbol information with the first user during the second time interval.

22. The method according to claim 20, further comprising a step of associating, at the credential administration server, the first visual symbol information with the first user during the second time interval, thereby facilitating authentication of the first user during the second interval if the second computer-readable visual symbol is not received by the first portable electronic device.

23. The method according to claim 19, wherein the first-time interval and the second time interval are of equal duration.

24. The method according to claim 19, further including a step of randomly selecting, at the credential administration server, each of the first- and second-time intervals such that they are of unequal duration.

25. The method according to claim 19, wherein each of the first and second visual symbols are bar codes, the method further including a step of initiating, from the credential administration server, transmission of a generation instruction to the first portable electronic device and the first portable electronic device being responsive to each generation instruction

received to locally generate and display a corresponding bar code as the machine discernable image.

26. The method according to claim 19, further including a step of receiving and storing, at the credential administration server, administrator input specifying at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an identified event.

27. The method according to claim 26, further including a step of transmitting, to the first portable device, information representative of at least one of an identity of an event to be attended by the first user, an event logo, an employer logo, an employer identification, first and last names of the first user, or areas of a facility to which the first user is authorized for entry during an identified event.

28. The method according to claim 26, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

address, a telephone number, an electronic serial number, and an RFID identifier.

29. The method according to claim 28, further including a step of receiving from the first portable electronic device, information specifying at least one of the unique identifier, an event to be attended by the first user, and first and last names of the first user.

30. The method according to claim 19, wherein the first portable electronic device is one of a smartphone, a tablet computer, a personal digital assistant, and a special purpose device having a display, memory and processor and wherein the unique identifier is one of an internet protocol (IP) address, a telephone number, an electronic serial number, and an RFID identifier.

31. The method according to claim 19, further including: associating at a credential administration server a second portable electronic device, identifiable by a unique identifier, with a second user and at least one of a location or a service subject to access restrictions;

obtaining third visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a third machine discernable image to be presented as an access credential by the second user during the first specified time interval;

providing instructions executable by the second portable electronic device for causing display of the third machine discernable image by the second portable device during the first-time interval;

wirelessly transmitting the third visual symbol information to the second portable electronic device;

obtaining fourth visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a fourth machine discernable image to be presented as an access credential by the second user during the second specified time interval; providing instructions executable by the second portable electronic device for causing display of the fourth machine discernable image by the second portable device during the second time interval commencing at expiration of the first time interval, and wirelessly transmitting the fourth visual symbol information to the second portable electronic device.

32. The method according to claim 31, further including a step of associating, at the credential administration server, the third visual symbol with the second user during the first-time interval.

33. The method according to claim 32, further including a step of associating, at the credential administration server, the third visual symbol and the fourth visual symbol with the second user during the second time interval, thereby facilitating authentication of the second user during the second interval in the event the third visual symbol is not received by the second portable electronic device.

34. The method according to claim 31, further including a step of facilitating authentication of a candidate portable electronic device displaying a machine discernable image as a credential by determining, in a first determining step, whether the candidate portable electronic device is identifiable by a unique ID associated with an authorized user; and determining, in a second determining step, whether the machine discernable displayed by the candidate portable electronic device corresponds to a visual symbol valid for an authorized user during a current time interval.

35. The method according to claim 34, 14. The computer-readable storage medium according to claim 1, wherein computer instructions stored therein, when executed by a processor, further perform associating at a credential administration server a second portable electronic device, identifiable by a unique identifier, with a second user and at least one of a location or a service subject to access restrictions; obtaining third visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a third machine discernable image to be presented by the second user as an access credential during the first time interval; for visible display of the third machine discernable image by the second portable device during the first time interval, initiating wireless transmission of the obtained third visual symbol information to the second portable electronic device;

obtaining fourth visual symbol information, at the credential administration server, for use by the second portable electronic device in initiating display of a fourth machine discernable image to be presented by the second user as an access credential during the second time interval;

and for visible display of the fourth machine discernable image by the second portable device commencing at expiration of the first time interval, initiating wireless transmission of the fourth visual symbol to the second portable electronic device.

The computer-readable storage medium according to claim 14, wherein computer instructions stored therein.

when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information with the second user during the first-time interval.

The computer-readable storage medium according to claim 15, wherein computer instructions stored therein, when executed by a processor, further perform a step of associating, at the credential administration server, the third visual symbol information and the fourth visual symbol information with the second user during the second time interval, thereby facilitating authentication of the second user during the second time interval in the event the fourth visual symbol information is not received by the second portable electronic device.

wherein if the candidate portable electronic device is identifiable by a unique ID associated with the first user and the received data is representative of a visual symbol valid during a current time interval, updating a record associated with the first user to reflect at least one of the time, date, location and event where the first portable electronic device was presented as a credential.

36. The method according to claim 35, further including a step of communicating an acceptance decision to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.

37. The method according to claim 34, wherein if the candidate portable electronic device is identifiable by a unique ID associated with the first user and the received data is representative of a visual symbol valid during a current time interval or an immediately preceding time interval associated with the first user, updating a record associated with the first user to reflect at least one of the time, date, location and event where the first portable electronic device was presented as a credential.

38. The method according to claim 34, wherein if the candidate portable electronic device is not identifiable by a unique ID associated with an authorized user or if the received data is not representative of a visual symbol valid during a current time interval and associated with any authorized user, communicating a rejection decision to a remote terminal accessible by personnel to whom the candidate portable electronic device was presented.

39. The method according to claim 19, wherein the first portable electronic device includes a global positioning satellite (GPS) receiver operative to obtain positional data and a corresponding cellular network transceiver for establishing a telecommunications link with a cellular network to thereby transmit position data for monitoring a location within a facility to which the first user has gained access using the first portable electronic device as a credential, said method further including a step of storing a record of locations visited by the first user while the first user is present at the facility.

40. The method according to claim 39, further including a step of generating a report graphically presenting an average time spent, at respectively specified locations within a facility, by users presenting a portable electronic device as a credential.

41. A method for configuring portable electronic devices each having a memory, a transceiver, and a display, using a credential management system, comprising: obtaining first information corresponding to a first machine discernable image to be used by a first user during a specified first-time interval of specified duration; providing first

instructions executable by a first portable electronic device associated with the first user for causing presentation of the first machine discernable image by the first portable device during the first-time interval; wirelessly transmitting the first information to the first portable electronic device;

obtaining second information corresponding to a second machine discernable image to be used by the first user during a second specified time interval of specified duration: providing second instructions executable by the portable electronic device for automatically causing presentation of the second machine discernable image by the first portable device during the second time interval commencing at expiration of the first-time interval;

wirelessly transmitting the second symbol information to the first portable electronic device; and transmitting over a communication network from a credential administrative server, data to be displayed by the first portable device during the first and second time intervals and together with each machine discernable image, the data including an assigned seating location, an event start time, an event date, and names of competing teams, or an identity of an issuing authority, or an identity of a transportation carrier, a departure date, a departure time, and a gate assignment; whereby the first portable device is caused, by execution of the first instructions, to cease presenting the first machine discernable image at expiration of the first time interval, and whereby the first portable device is caused, by execution of the second instructions, to commence presenting the second machine discernable image, at initiation of the second time interval.

42. The method of claim 41, further including a step of updating data to be displayed by the first portable device by transmitting, from the credential administrative server, at least one of a changed seating assignment, a changed gate assignment, and a changed departure time.

43. The method of claim 42, further including a step of transmitting one of an e-mail and a text message to a user of the first portable device as notification of any transmission of updating data.

44. The method of claim 41, wherein each of the first and the second machine discernable image is a respective bar code displayed continuously during the first interval and the second interval, respectively.

45. The method of claim 41, further including a step of collecting, from each respective portable electronic device, data corresponding to time spent by a corresponding user at one or more locations within a facility and to which the corresponding user has gained access after using a corresponding portable electronic device as a credential to enter the facility.

46. The method of claim 45, further including a step of generating a report graphically presenting average time spent, by respective socio-demographic groups of users who presented a portable electronic device as a credential to gain access to an event, at the one or more specified locations.

SECTION D: Comparisons Charts

Patent Infringement Analysis Charts Report

Introduction

This report analyzes whether MLB's digital ticketing technology infringes on US Patent No. 9,047,715, titled "Credential Management System and Method." The patent describes a system and method for managing and administering digital access credentials, such as digital tickets.

MLB's digital ticketing technology allows users to purchase and download digital tickets to MLB games on their smartphones. The app then generates a unique mobile ticket barcode for each ticket. The mobile ticket barcode is constantly rotating, making it difficult to counterfeit.

Claim Chart

The following claim chart compares the claims of the 9,047,715 patent to MLB's digital ticketing technology:

Claim Element	Patent Claim 1	MLB Digital Ticketing Technology
Configures a portable electronic device to display a machine discernable image during a specified time interval	Yes	Yes
Machine discernable image (barcode) changes every many seconds	Yes	Yes
Transmission of generation instructions to the portable electronic device (via	Yes	Yes

the MLB
Ballpark app)

Generates
visual symbol
information
(mobile ticket
barcode)
associated
with event
information
(game
details)

Yes Yes

Generates
visual symbol
information
(mobile ticket
barcode)
associated
with areas of
a facility
(stadium
sections)

Yes Yes

Receipt and
storage of
administrator
input
specifying the
details of the
credentials
(digital
tickets) to be
distributed

Yes Yes

Receipt and
storage of
user input
specifying
user
information
(such as
personal

Yes Yes

details or preferences)

Use of a computer-readable storage medium to store instructions for executing the credential management system and method

Likely Likely

Configuring multiple portable electronic devices using the credential management system

Yes Yes

Associates the second visual symbol information (mobile ticket barcode) with the first user during the second time interval

Yes Yes

Discussion of Claims

MLB's digital ticketing technology meets the elements of all of the asserted patent claims.

- Claim 1: MLB's digital ticketing technology configures the user's smartphone to display the mobile ticket barcode during the specified time interval (the game).
- Claim 8: MLB's digital ticketing technology transmits generation instructions to the user's smartphone, which then locally generates the mobile ticket barcode.

- Claim 9: MLB's digital ticketing technology generates the mobile ticket barcode, which is associated with the event information (game details).
- Claim 11: MLB's digital ticketing technology generates the mobile ticket barcode, which is associated with the areas of the facility (stadium sections) to which the user is authorized for entry.
- Claim 12: MLB's digital ticketing system receives and stores administrator input specifying the details of the digital tickets to be distributed, and then transmits this information to the user's smartphone for display as the mobile ticket barcode.
- Claim 13: MLB's digital ticketing system receives and stores user input specifying user information, and then transmits this information to the credential administration server for association with the user's digital tickets.
- Claims 14-18: MLB's digital ticketing system likely utilizes a computer-readable storage medium to store the necessary instructions and data for managing and administering digital tickets.
- Claims 19-25: MLB's digital ticketing system allows for the configuration and association of multiple devices (such as smartphones) with different users, enabling the distribution and display of mobile ticket barcodes on those devices during specific time intervals.
- Claim 21: MLB's digital ticketing system associates the second mobile ticket barcode with the first user during the second time interval, allowing for authentication in the event that the second mobile ticket barcode is transferred to another user.

Conclusion

MLB's digital ticketing technology infringes on all of the asserted patent claims.

Limitations

This analysis is based on the information that is currently available. It is possible that additional information could come to light that could affect the conclusion.

Recommendations

The patent holder should consider taking legal action to enforce their patent rights against MLB.

Additional Suggestions

- The patent holder could consider conducting a more detailed analysis of MLB's digital ticketing technology to identify any potential defenses or counterarguments that MLB could raise.

Final Introduction

This report analyzes whether MLB's digital ticketing technology infringes on US Patent No. 9,047,715, titled "SYSTEM AND METHOD FOR CREDENTIAL MANAGEMENT AND ADMINISTRATION." The patent describes a system and method for managing and administering digital access credentials, such as digital tickets.

Final Claim Chart

The following claim chart compares the claims of the 9,047,715 patent to MLB's digital ticketing technology:

Claim Element	Patent Claim	MLB Digital Ticketing Technology
Configures a portable electronic device to display a machine discernable image during a specified time interval	1	Yes
Machine discernable image (barcode) changes every many seconds	8	Yes
Transmission of generation instructions to the portable electronic device (via the MLB Ballpark app)	9	Yes
Generates visual symbol	11	Yes

information
(mobile ticket
barcode)
associated with
event
information
(game details)

Generates
visual symbol
information
(mobile ticket
barcode)
associated with
areas of a
facility
(stadium
sections)

12 Yes

Receipt and
storage of
administrator
input
specifying the
details of the
credentials
(digital tickets)
to be
distributed

13 Yes

Receipt and
storage of user
input
specifying user
information
(such as
personal
details or
preferences)

14 Yes

Use of a
computer-
readable
storage

15-
18 Likely

medium to store instructions for executing the credential management system and method

Configuring multiple portable electronic devices using the credential management system

19-25 Yes

Associates the second visual symbol information (mobile ticket barcode) with the first user during the second time interval

21 Yes

Generating a report graphically presenting the average time spent by users presenting a portable electronic device as a credential at specified locations within a facility

40 No

Communicating a rejection decision regarding a credential to the credential holder	38	No
Monitoring the location of the credential holder using GPS	39	No
Using a QR code as the machine-discernable image	9	Yes
Continually updating the machine-discernable image from a static one to a rotating one that cannot be duplicated	31	Yes
Associating each portable electronic device with a unique user	41	Yes
Providing the changing symbol information during specified time intervals	42	Yes

Using a credential administration server to associate each portable electronic device with a unique user and to provide the changing symbol information during specified time intervals	44	Yes
Using GPS to monitor user location	45	No
Generating reports on user behavior	46	No

Final Discussion of Claims

MLB's digital ticketing technology infringes on claims 1, 8, 9, 11, 12, 13, 14, 15-18 (likely), 19-25, 21, 39, 40, 41, 42, and 43 of the 9,047,715 patent.


Final Conclusion

MLB's digital ticketing technology infringes on 14 of the 46 claims of US Patent No. 9,047,715.

Final Recommendations

The patent holder should consider taking legal action to enforce their patent rights against MLB.



Download the Official App 

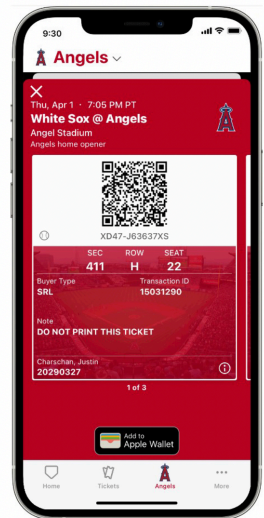
Don't Strike Out at the Gate

MLB has launched Protect the Barcode technology at Angel Stadium, updating the digital barcode from a static one to a rotating one that cannot be duplicated. Ensure that you've got the most recent version of the Ballpark App on your mobile device, so that you can benefit from having this new, secure technology! The new, rotating barcode ensures that you have a genuine ticket and that you won't have any issues at the gate on Game Day. Look for the moving baseballs next to your barcode and know that you're good to go.

Tickets forwarded through the Ballpark app are protected, as well. Just make sure that you don't send your friends and family a ticket screenshot because **screenshots of Ballpark app digital tickets will no longer be accepted as a valid method of entry into the stadium.**

Download the Official App

TICKET



END REPORT