US 20060046842A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2006/0046842 A1**

Mattice et al. (43) **Pub. Date: Mar. 2, 2006**

(54) **TICKET REDEMPTION USING ENCRYPTED BIOMETRIC DATA**

(75) Inventors: **Harold E. Mattice**, Gardnerville, NV (US); **Joseph E. Kaminkow**, Reno, NV (US)

Correspondence Address:
BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250 (US)

(73) Assignee: **IGT**

(21) Appl. No.: **11/262,059**

(22) Filed: **Oct. 28, 2005**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/214,936, filed on Aug. 6, 2002, which is a continuation-in-part of application No. 09/927,742, filed on Aug. 10, 2001, now abandoned.

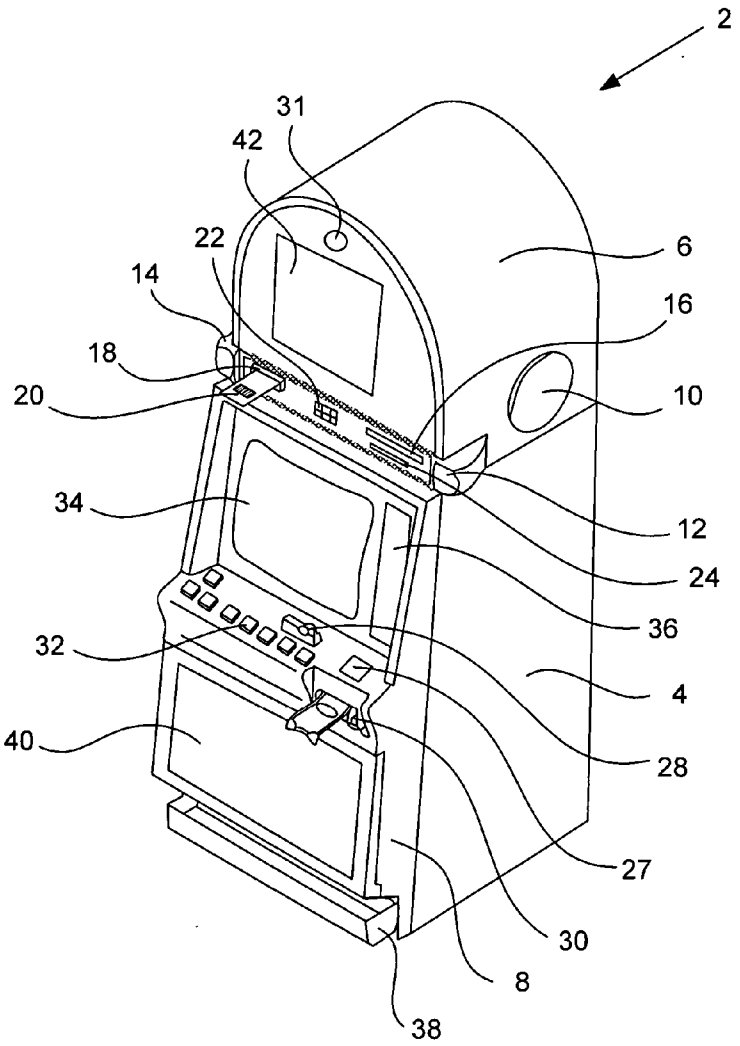
Publication Classification

(51) **Int. Cl.**
A63F 9/24 (2006.01)

(52) **U.S. Cl.** **463/29**

(57) **ABSTRACT**

Provided herein are systems and methods that improve the redemption integrity of portable gaming instruments such as tickets and magnetic cards. The systems and methods encrypt biometric data for a recipient of a portable gaming instrument and store the encrypted biometric data on the portable gaming instrument. When a person tries to redeem value on the portable gaming instrument, a comparison is made between: a) biometric data for the person trying to redeem the value, and b) the biometric data encrypted and stored on the portable gaming instrument.



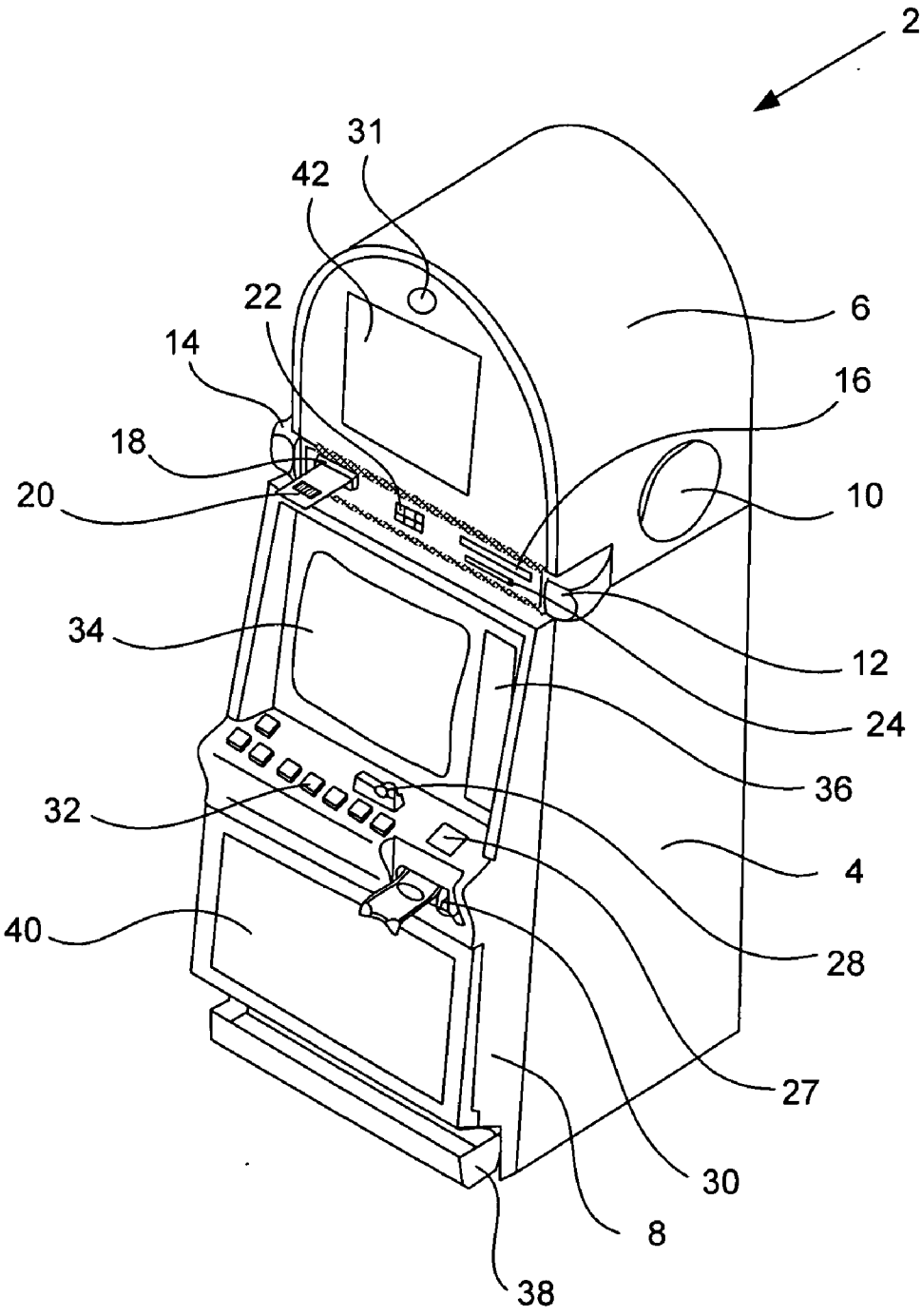


FIGURE 1

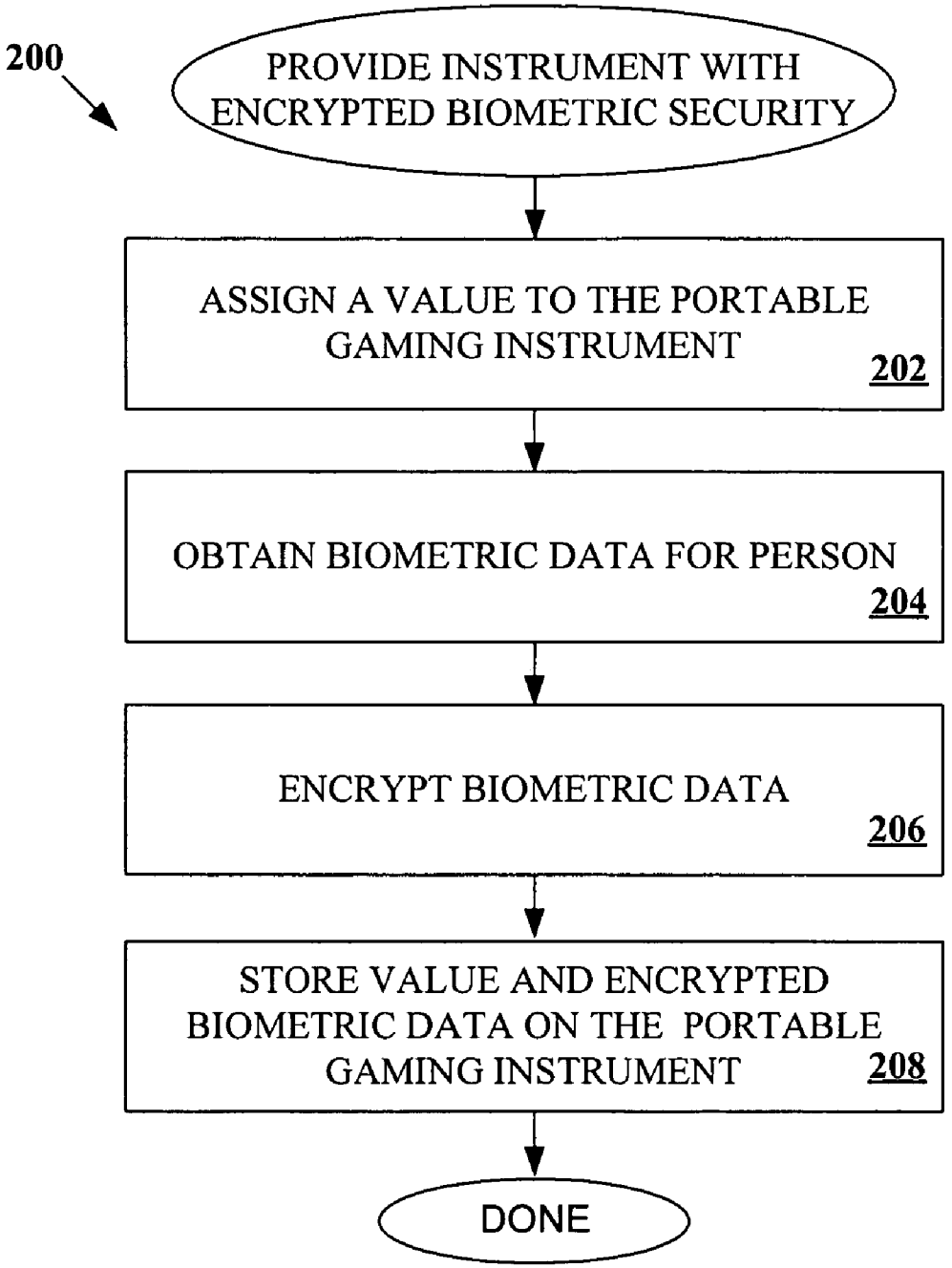

200
PROVIDE INSTRUMENT WITH ENCRYPTED BIOMETRIC SECURITY
ASSIGN A VALUE TO THE PORTABLE GAMING INSTRUMENT
202
OBTAIN BIOMETRIC DATA FOR PERSON
204
ENCRYPT BIOMETRIC DATA
206
STORE VALUE AND ENCRYPTED BIOMETRIC DATA ON THE PORTABLE GAMING INSTRUMENT
208
DONE

FIGURE 2

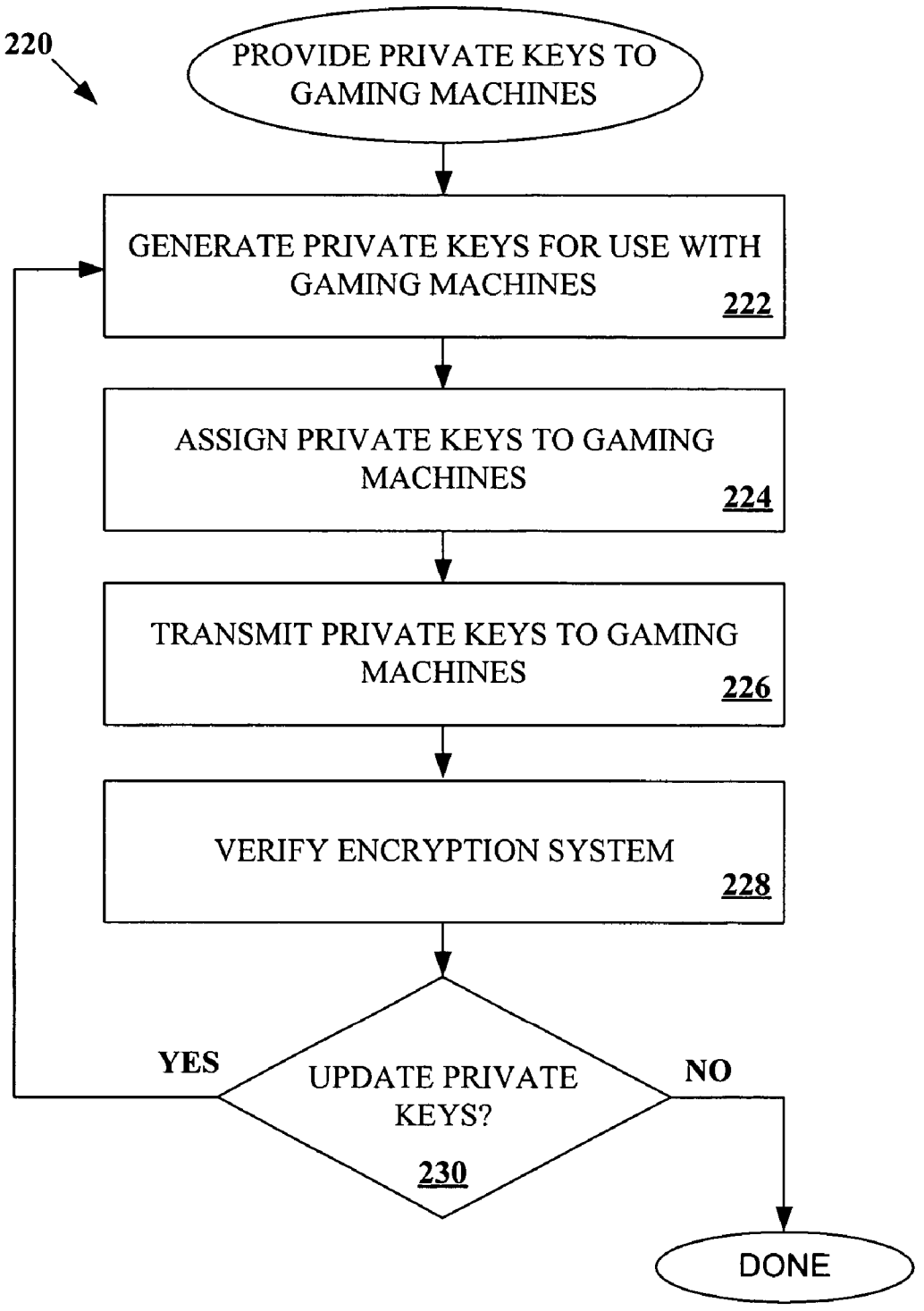

220
PROVIDE PRIVATE KEYS TO GAMING MACHINES
GENERATE PRIVATE KEYS FOR USE WITH GAMING MACHINES
222
ASSIGN PRIVATE KEYS TO GAMING MACHINES
224
TRANSMIT PRIVATE KEYS TO GAMING MACHINES
226
VERIFY ENCRYPTION SYSTEM
228
UPDATE PRIVATE KEYS?
230
YES
NO
DONE

FIGURE 3

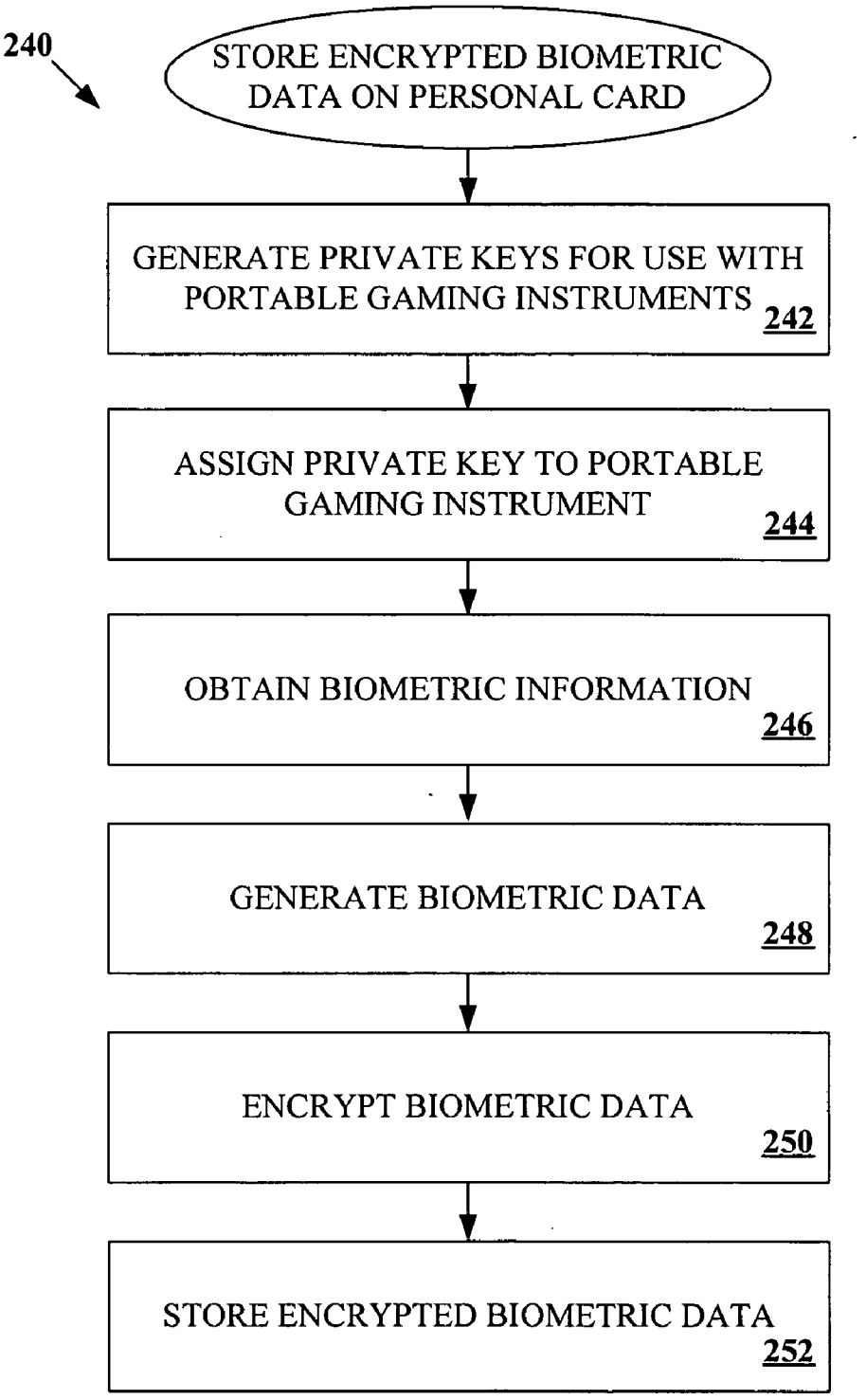

240
STORE ENCRYPTED BIOMETRIC DATA ON PERSONAL CARD
GENERATE PRIVATE KEYS FOR USE WITH PORTABLE GAMING INSTRUMENTS
242
ASSIGN PRIVATE KEY TO PORTABLE GAMING INSTRUMENT
244
OBTAIN BIOMETRIC INFORMATION
246
GENERATE BIOMETRIC DATA
248
ENCRYPT BIOMETRIC DATA
250
STORE ENCRYPTED BIOMETRIC DATA
252

FIGURE 4

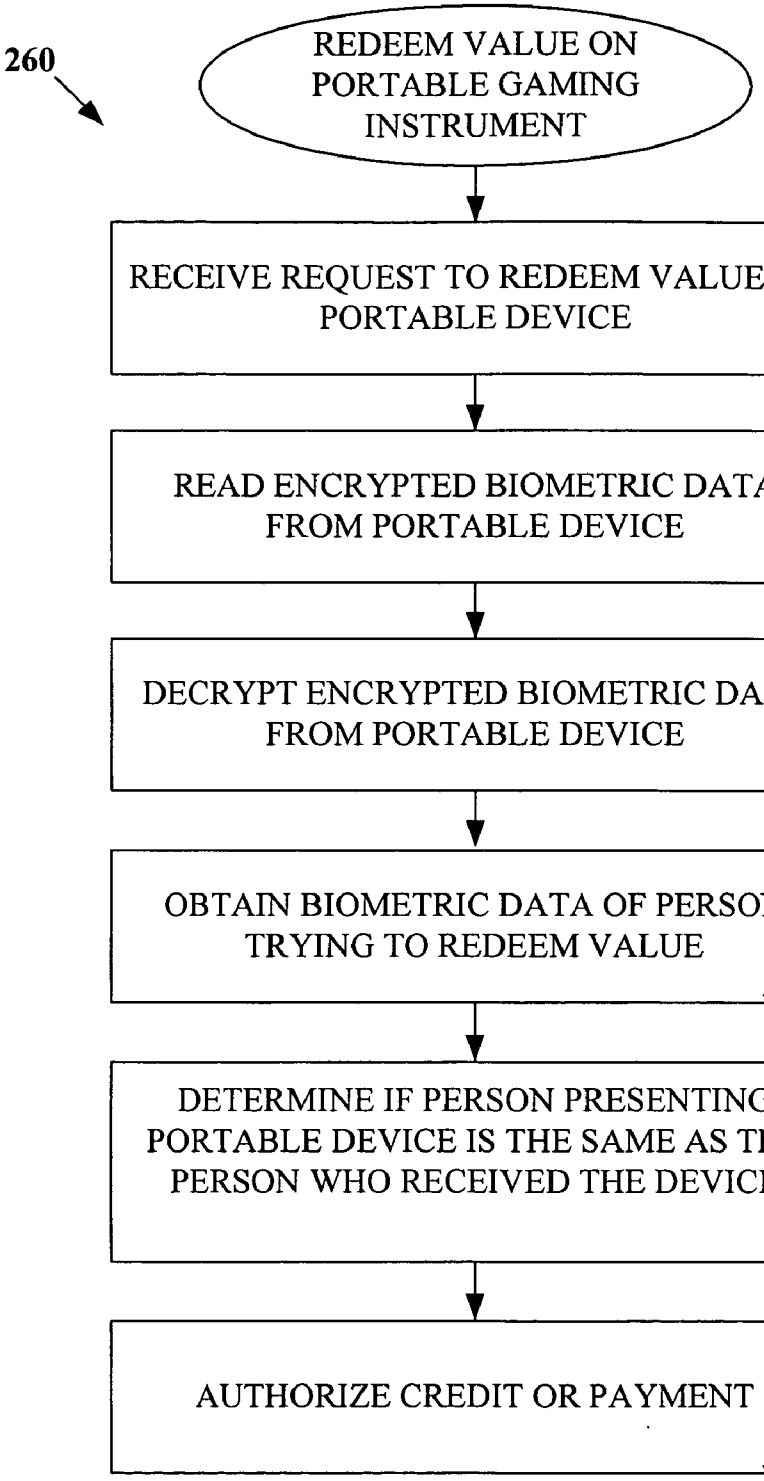

260
REDEEM VALUE ON PORTABLE GAMING INSTRUMENT
RECEIVE REQUEST TO REDEEM VALUE ON PORTABLE DEVICE
262
READ ENCRYPTED BIOMETRIC DATA FROM PORTABLE DEVICE
264
DECRYPT ENCRYPTED BIOMETRIC DATA FROM PORTABLE DEVICE
266
OBTAIN BIOMETRIC DATA OF PERSON TRYING TO REDEEM VALUE
268
DETERMINE IF PERSON PRESENTING PORTABLE DEVICE IS THE SAME AS THE PERSON WHO RECEIVED THE DEVICE
270
AUTHORIZE CREDIT OR PAYMENT
272

FIGURE 5A

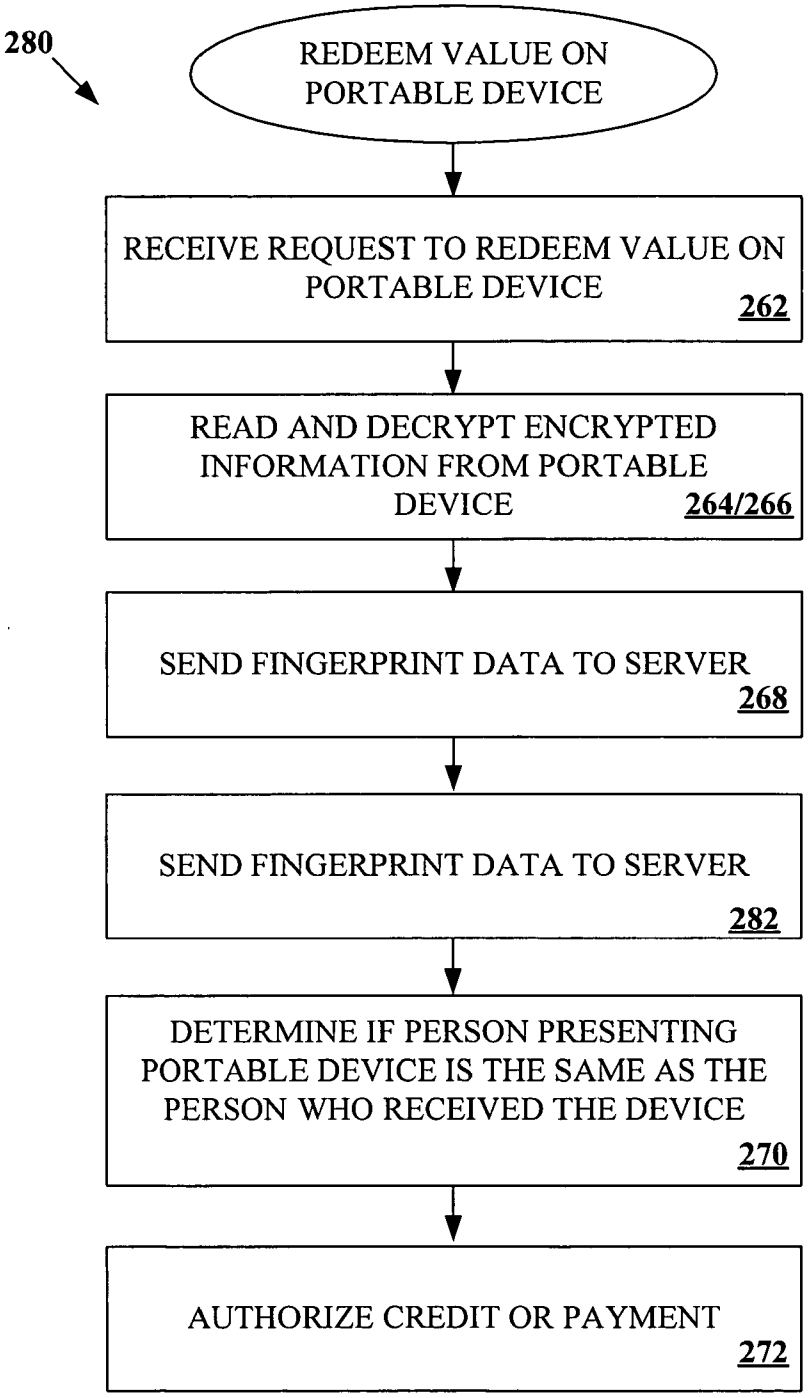

280
REDEEM VALUE ON PORTABLE DEVICE
RECEIVE REQUEST TO REDEEM VALUE ON PORTABLE DEVICE
262
READ AND DECRYPT ENCRYPTED INFORMATION FROM PORTABLE DEVICE
264/266
SEND FINGERPRINT DATA TO SERVER
268
SEND FINGERPRINT DATA TO SERVER
282
DETERMINE IF PERSON PRESENTING PORTABLE DEVICE IS THE SAME AS THE PERSON WHO RECEIVED THE DEVICE
270
AUTHORIZE CREDIT OR PAYMENT
272

FIGURE 5B

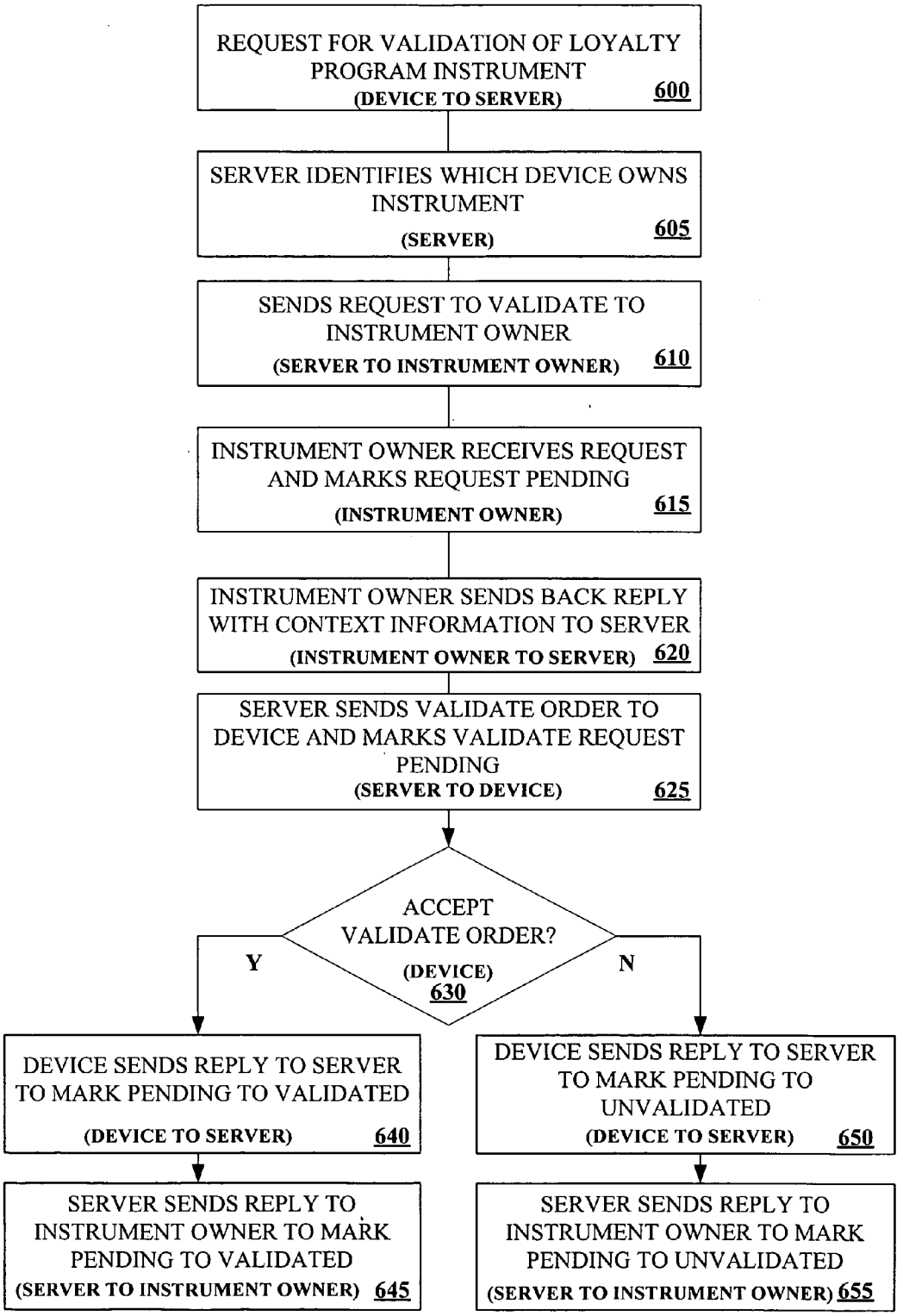

REQUEST FOR VALIDATION OF LOYALTY PROGRAM INSTRUMENT
(DEVICE TO SERVER) 600
SERVER IDENTIFIES WHICH DEVICE OWNS INSTRUMENT
(SERVER) 605
SENDS REQUEST TO VALIDATE TO INSTRUMENT OWNER
(SERVER TO INSTRUMENT OWNER) 610
INSTRUMENT OWNER RECEIVES REQUEST AND MARKS REQUEST PENDING
(INSTRUMENT OWNER) 615
INSTRUMENT OWNER SENDS BACK REPLY WITH CONTEXT INFORMATION TO SERVER
(INSTRUMENT OWNER TO SERVER) 620
SERVER SENDS VALIDATE ORDER TO DEVICE AND MARKS VALIDATE REQUEST PENDING
(SERVER TO DEVICE) 625
ACCEPT VALIDATE ORDER?
(DEVICE)
630
Y
N
DEVICE SENDS REPLY TO SERVER TO MARK PENDING TO VALIDATED
(DEVICE TO SERVER) 640
DEVICE SENDS REPLY TO SERVER TO MARK PENDING TO UNVALIDATED
(DEVICE TO SERVER) 650
SERVER SENDS REPLY TO INSTRUMENT OWNER TO MARK PENDING TO VALIDATED
(SERVER TO INSTRUMENT OWNER) 645
SERVER SENDS REPLY TO INSTRUMENT OWNER TO MARK PENDING TO UNVALIDATED
(SERVER TO INSTRUMENT OWNER) 655

FIGURE 6

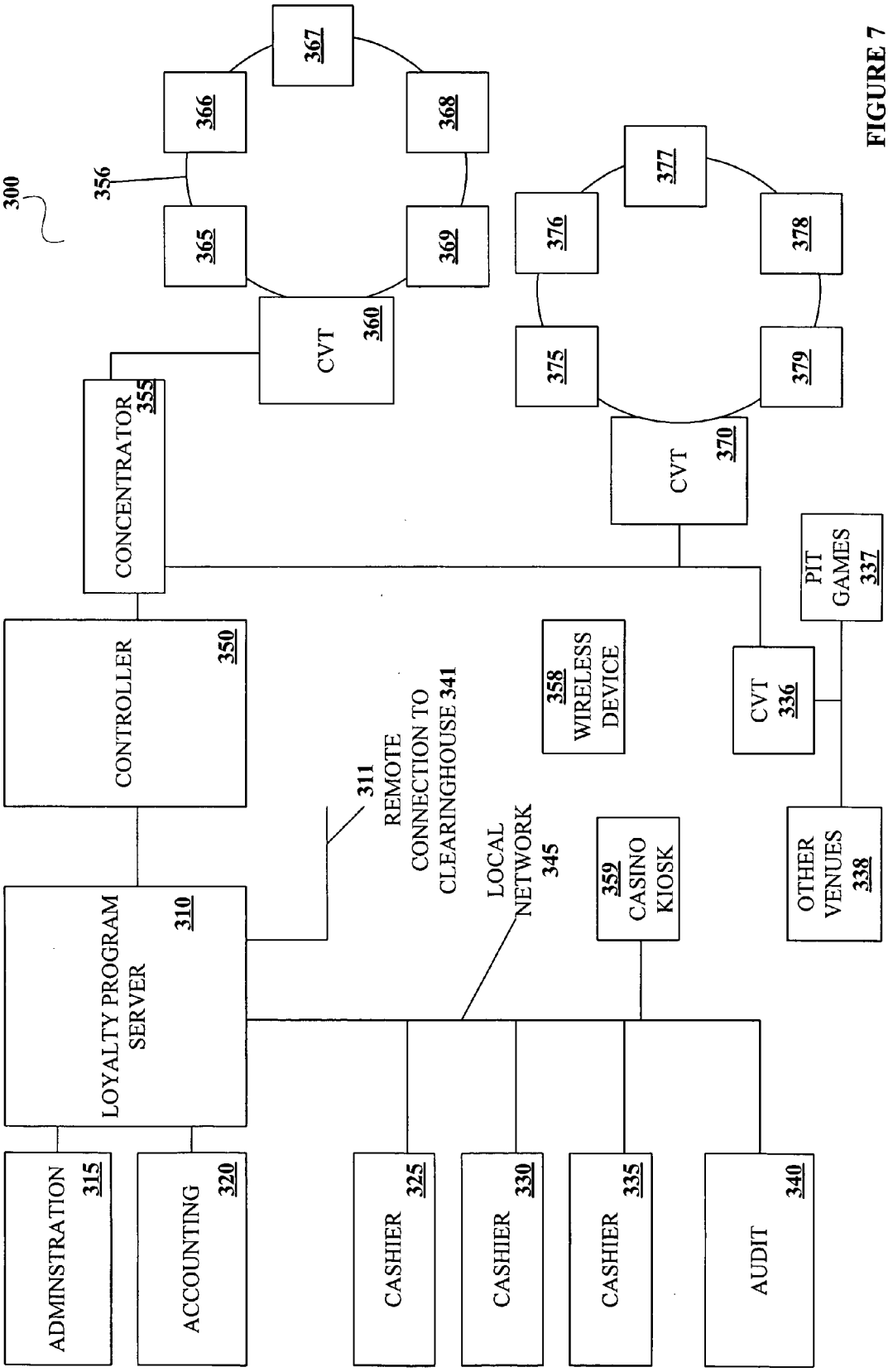

300
356
367
366
368
365
362
CVT 360
CONCENTRATOR 355
376
377
378
375
379
CVT 370
PIT GAMES 337
CONTROLLER 350
358 WIRELESS DEVICE
CVT 336
311 REMOTE CONNECTION TO CLEARINGHOUSE 341
LOCAL NETWORK 345
359 CASINO KIOSK
OTHER VENUES 338
LOYALTY PROGRAM SERVER 310
ADMINSTRATION 315
ACCOUNTING 320
CASHIER 325
CASHIER 330
CASHIER 335
AUDIT 340

FIGURE 7

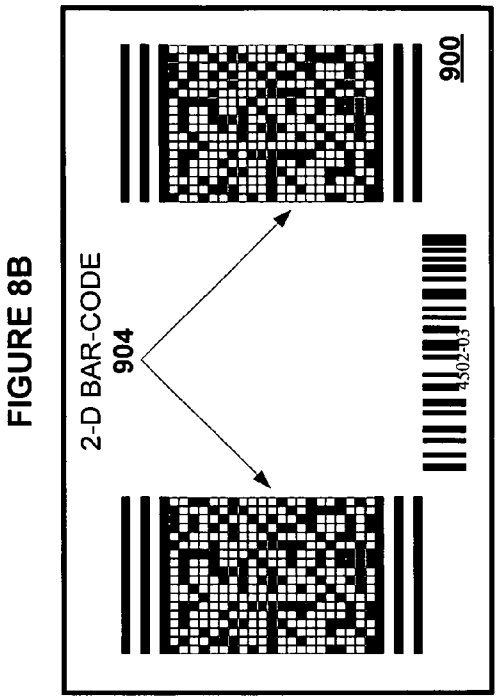


FIGURE 8B

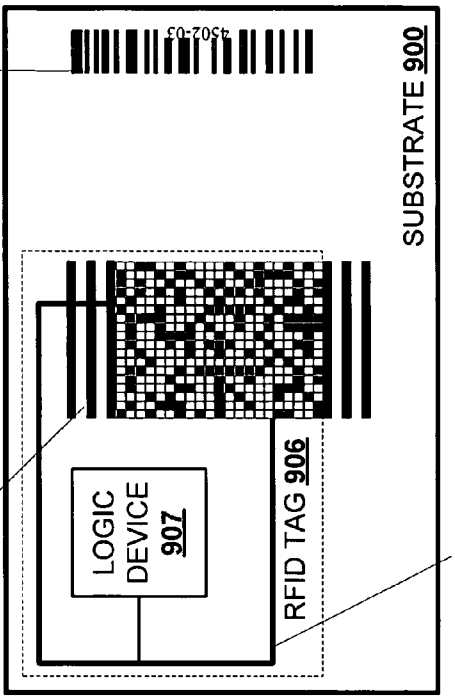


FIGURE 8D

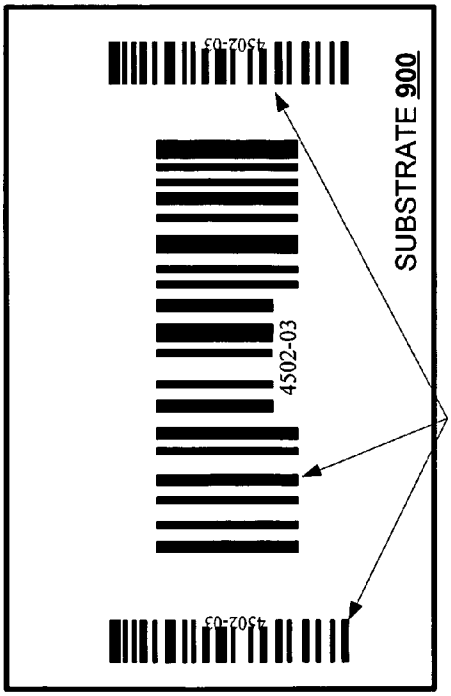


FIGURE 8A

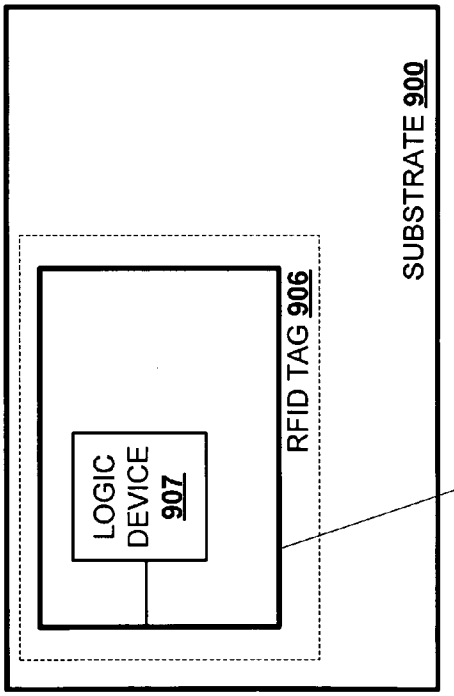


FIGURE 8C

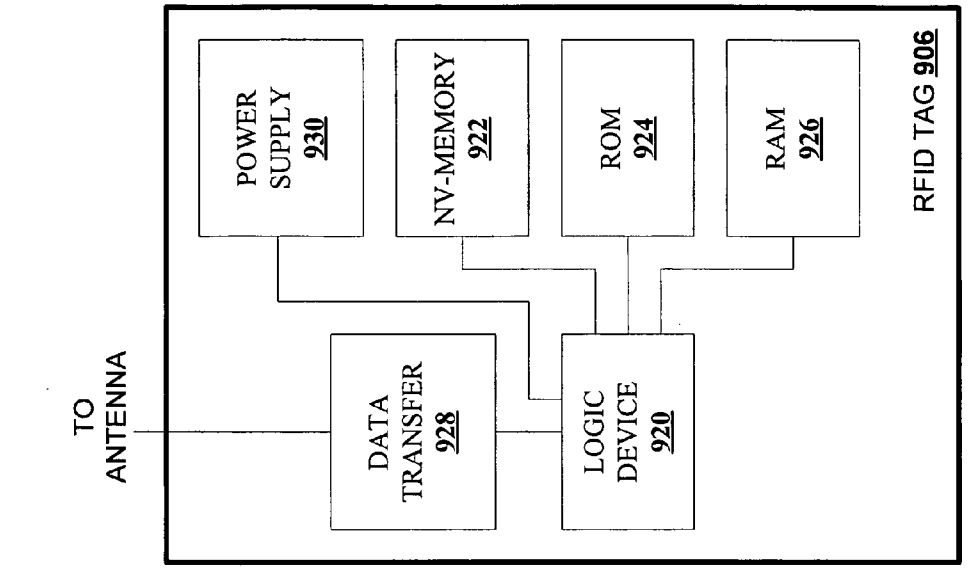


FIGURE 9C

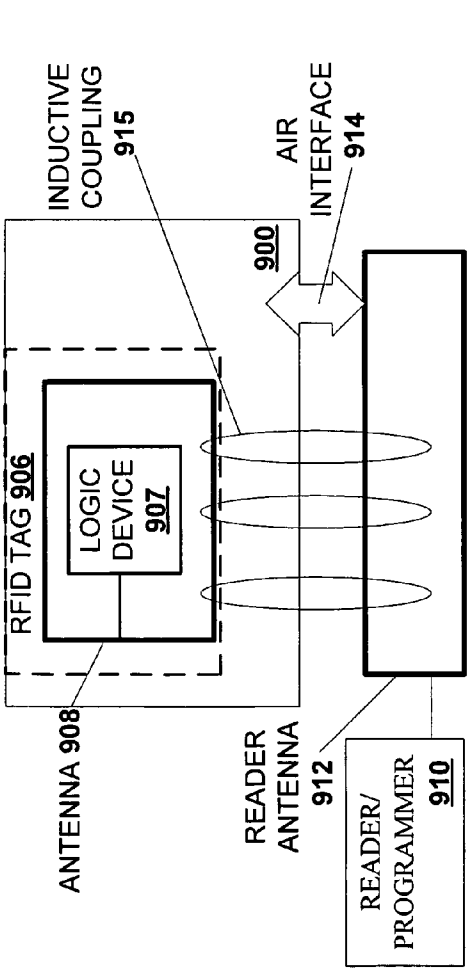


FIGURE 9A

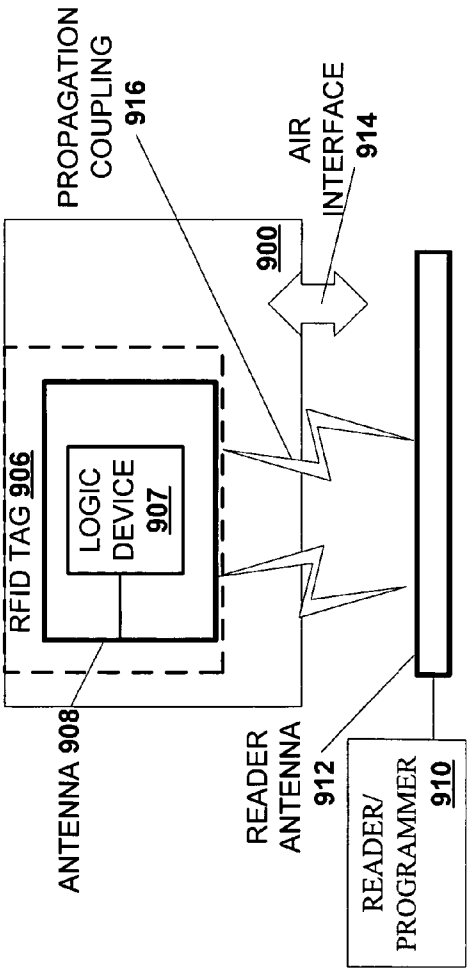


FIGURE 9B

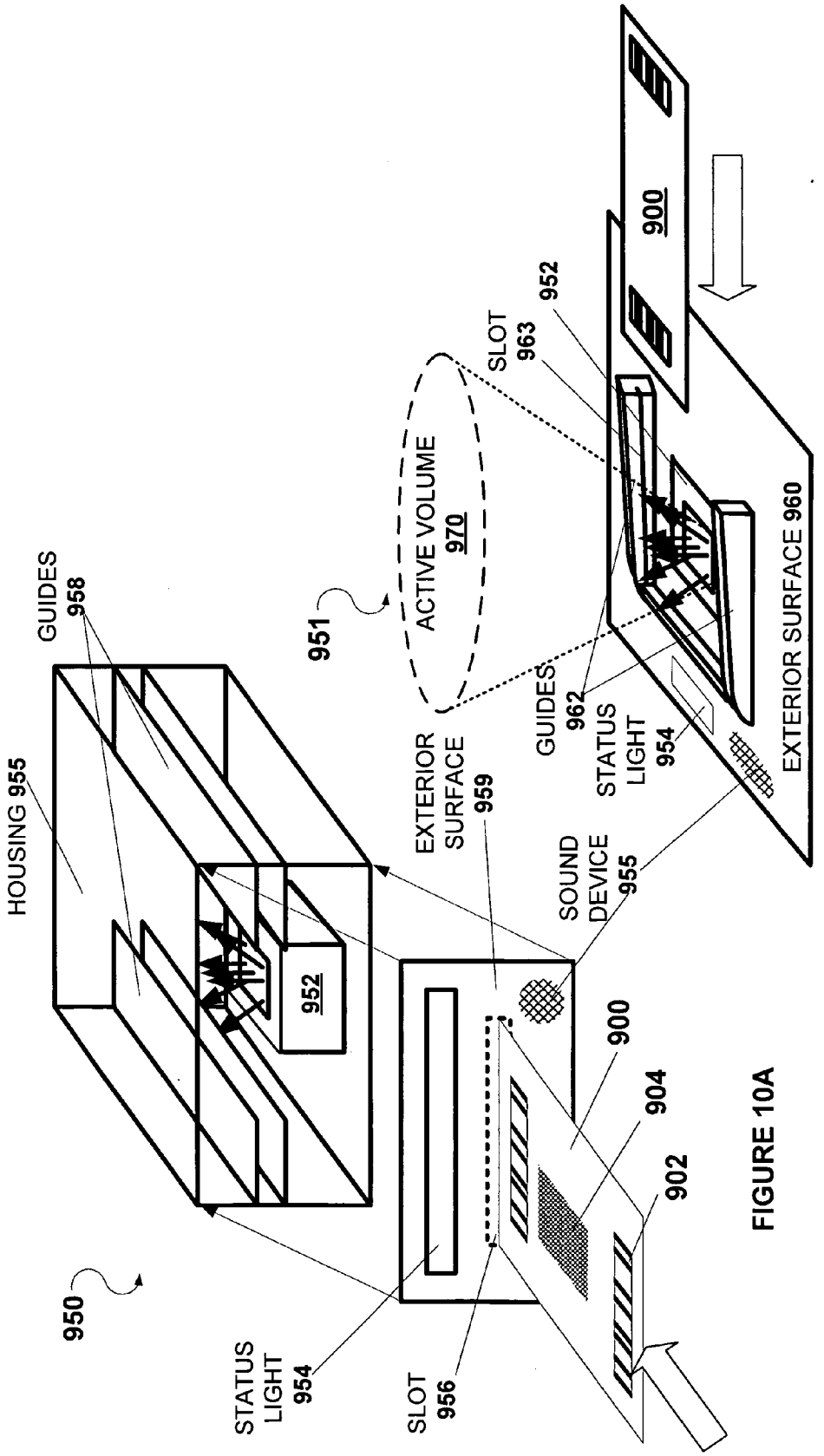


FIGURE 10A

FIGURE 10B

TICKET REDEMPTION USING ENCRYPTED BIOMETRIC DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of U.S. patent application Ser. No. 10/214,936 entitled "FLEXIBLE LOYALTY POINTS PROGRAMS," filed Aug. 6, 2002, which is incorporated herein by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

[0002] This invention relates to systems and methods for use with gaming machines. More particularly, the present invention relates to systems and methods for validating the redemption of value stored on portable credit devices that are used with gaming machines.

[0003] As technology in the gaming industry progresses, the traditional mechanically driven reel slot machines are being replaced or supplemented with electronic counterparts having CRT, LCD video displays or the like. Processor-based gaming machines are becoming increasingly popular. Part of the reason for their increased popularity is the nearly endless variety of games that can be implemented on gaming machines utilizing advanced electronic technology. In some cases, newer gaming machines are utilizing computing architectures developed for personal computers. These video/electronic gaming advancements enable the operation of more complex games, which would not otherwise be possible on mechanical-driven gaming machines.

[0004] Typically, utilizing a master gaming controller (or gaming machine controller or main processor), the gaming machine controls various combinations of devices that allow a player to play a game on the gaming machine. For example, a game played on a gaming machine usually requires a player to input money or indicia of credit into the gaming machine, indicate a wager amount, and initiate a game play. These steps require the gaming machine to control input devices, including bill validators and coin acceptors, to accept money into the gaming machine and recognize user inputs from devices, including touch screens and button pads, to determine the wager amount and initiate game play.

[0005] After game play has been initiated, the master gaming controller determines a game outcome, presents the game outcome to the person and may dispense an award of some type depending on the outcome of the game. A game outcome presentation may use various visual and audio components such as flashing lights, music, sounds and graphics. The visual and audio components may be used to draw a player's attention to various game features and to heighten the player's interest in additional game play.

[0006] Transaction currency on gaming machines has also evolved. Where once only coin handling mechanisms were present on gaming machines, credit devices such as cash-out vouchers now find wide use. Some casinos issue magnetic player cards that players use to obtain awards for frequent playing. A player holding such a card inserts it into a card reader provided on a gaming machine before play begins. Other casinos now issue bar-coded tickets. When a player terminates interaction on a gaming machine, the gaming machine prints a ticket, which visibly indicates the player's final status such as a cash-out value and the time. The player then retrieves the ticket and may redeem it for credit at another game or exchange it for cash at a change booth or a pay machine.

[0007] People lose the magnetic player cards and paper tickets. All too often, other people find the misplaced cards and tickets—and attempt to redeem them. Player cards and paper tickets can also be stolen. Attempts at false redemption of tickets and cards occur often, and are undesirable to both casinos and legitimate ticket and card owners. At the least, casinos like to reward patronage and protect the winnings of legitimate winners. In addition, casinos would like to protect the integrity of the cashless systems by thwarting unscrupulous or other attempts at false redemption.

[0008] In view of the above, it would be desirable to provide solutions that improve and protect the redemption of portable credit devices.

SUMMARY OF THE INVENTION

[0009] This invention provides systems and methods that improve the redemption integrity of portable gaming instruments such as tickets and magnetic cards. The systems and methods encrypt biometric data for a recipient of a portable gaming instrument and store the encrypted biometric data on the portable gaming instrument. When a person tries to redeem value on the portable gaming instrument, a comparison is made between: a) biometric data for the person trying to redeem the value, and b) the biometric data encrypted and stored on the portable gaming instrument.

[0010] Redemption may occur at a gaming machine, cash-out station, or any other redemption location in an establishment that offers one or more gaming machines.

[0011] The present invention permits the use of various forms of biometric data. For example, fingerprinting, facial recognition, voice-recognition and retinal detection are forms of biometric validation suitable for use with the present invention.

[0012] Networked systems and methods may employ a server that maintains biometric data records for numerous people. The server offers centralized validation of portable gaming instruments provided to a gaming machine or other redemption location that communicates on the network. The server may also coordinate encrypted functionality. One server embodiment maintains a log of public and private keys distributed to gaming machines and portable gaming instruments used within a networked gaming environment. In one embodiment, a gaming machine in the network obtains biometric data of a person that has interacted with the gaming machine. The gaming machine then encrypts and signs the biometric data with a private key assigned, by the server, to the gaming machine or to the portable gaming instrument. The gaming machine then stores the encrypted and signed data on a portable gaming instrument, and provides the portable gaming instrument to the person.

[0013] A copy of the encrypted and signed data may also be sent to, and stored by, the server. The server then assigns and stores the corresponding private key to permit the encrypted data to be opened and used for comparison. Subsequently, when someone attempts to redeem value from the ticket, his or her biometric data is obtained. Obtaining

the biometric data may include reading biometric data from the person, or by taking the person's identity and matching the stored on biometric data on the server with their identity. The person's identity may be determined using a driver's license, other personal identification, a player-tracking card issued by the casino that also includes a confirmed identity, etc. The server copy of encrypted biometric data permits validation of the portable gaming instrument—without requiring the person redeeming the ticket to once again have their fingerprint or other biometric information captured. The biometric data obtained at redemption is then compared to the biometric data stored on the ticket. In this manner, a person can walk up to any gaming machine within a gaming establishment and have their locally captured and encrypted biometric input authenticated.

[0014] The present invention is concerned with the redemption of value on portable gaming instrument. Many portable gaming instruments, such as paper tickets and magnetic card devices, can be redeemed at a gaming machine.

[0015] In one aspect, the present invention relates to a method of providing a portable gaming instrument for use with gaming machines. The method includes assigning a value to the portable gaming instrument. The method also includes obtaining biometric data for a person that has interacted with a gaming machine. The method further includes encrypting the biometric data representative to produce encrypted biometric data. The method additionally includes storing the value and the encrypted biometric data on the portable gaming instrument.

[0016] In another aspect, the present invention relates to a method of redeeming value on a portable gaming instrument. The method includes receiving a request to redeem the value on the portable gaming instrument. The method also includes decrypting encrypted biometric data stored on the portable gaming instrument. The encrypted biometric data includes biometric data used to produce the encrypted biometric data and identifies a person who received the portable gaming instrument. The method further includes obtaining biometric data for a person trying to redeem the value on the portable gaming instrument. The method additionally includes comparing a) the biometric data for the person trying to redeem the value on the portable gaming instrument with b) the biometric data obtained from the portable gaming instrument. When the biometric data for the person trying to redeem the value on the portable gaming instrument matches the biometric data that was encrypted and stored on the portable gaming instrument, then the value on the portable gaming instrument is awarded to the person trying to redeem the value on the portable gaming instrument

[0017] In yet another aspect, the present invention relates to a gaming machine. The gaming machine includes an external cabinet defining an interior region of the gaming machine. The gaming machine also includes a display device adapted to display game play information. The gaming machine further includes a biometric reader located within or about the external cabinet and configured to read biometric information from a person. The gaming machine additionally includes a portable gaming instrument reader that is configured to read encrypted biometric data stored on a portable gaming instrument. The encrypted biometric data includes biometric data used to produce the encrypted biometric data and identifies a person who received the portable gaming instrument. The gaming machine also includes a gaming machine controller designed or configured to i) provide a game play sequence comprising a presentation of one or more games of chance on the gaming machine, ii) decrypt the encrypted biometric data stored on a portable gaming instrument, iii) compare a) the biometric data for the person with b) the biometric data obtained from the portable gaming instrument, and iv) award the value on the portable gaming instrument to the person when the biometric information for the person matches the biometric information that was encrypted and stored on the portable gaming instrument.

[0018] In yet another aspect, the present invention relates to a gaming system for providing portable gaming instruments. The gaming system includes a plurality of portable gaming instruments. Each portable gaming instrument includes encrypted biometric data that identifies a person that received the portable gaming instrument. The gaming system also includes a plurality of gaming machines. Each gaming machine includes a biometric reader configured to read biometric information from a person, a portable gaming instrument reader configured to read the encrypted biometric data stored on a portable gaming instrument, and a network interface that permits communication across a network. The gaming system further includes a server including a network interface that permits communication across the network and configured to distribute a private key to each of the gaming machines.

[0019] Another aspect of the invention pertains to computer program products including a machine-readable medium on which are stored program instructions for implementing any of the methods described above. Any of the methods of this invention may be represented as program instructions and/or data structures, databases, etc. that can be provided on such computer readable media.

[0020] These and other features and advantages of the invention will be spelled out in more detail below with reference to the associated drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] **FIG. 1** shows an exemplary video gaming machine suitable for use with the present invention.

[0022] **FIG. 2** illustrates a process flow for providing a portable gaming instrument for use with a gaming machine in accordance with one embodiment of the present invention.

[0023] **FIG. 3** illustrates a process flow for redeeming value on a portable gaming instrument in accordance with one embodiment of the present invention.

[0024] **FIG. 4** illustrates a process flow for storing encrypted biometric data on a player tracking card and server in accordance with one embodiment of the present invention.

[0025] **FIG. 5A** illustrates a process flow for redeeming value on a portable gaming instrument in accordance with one embodiment of the present invention.

[0026] **FIG. 5B** illustrates a process flow for redeeming value on a portable gaming instrument that uses a network architecture in accordance with another embodiment of the present invention.

[0027] **FIG. 6** is a flow chart depicting a method for validating information stored on a portable gaming instrument at a validation site connected to a network in accordance with one embodiment of the present invention.

[0028] **FIG. 7** is a block diagram of the components of a portable gaming instrument system for one embodiment of the present invention.

[0029] **FIGS. 8A-8D** illustrate exemplary printed portable gaming instruments and data formats of the present invention.

[0030] **FIGS. 9A-9C** illustrate RFID tags and RFID readers of the present invention.

[0031] **FIGS. 10A-10B** show simplified illustrations of input mechanisms with a non-physical contact data interface of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0032] The present invention will now be described in detail with reference to a few preferred embodiments thereof as illustrated in the accompanying drawings. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps and/or structures have not been described in detail in order to not unnecessarily obscure the present invention.

[0033] The present invention increases the integrity of portable gaming instruments. More specifically, the systems and methods described herein bolster redemption integrity for portable gaming instruments and value associated with the portable gaming instruments. In one embodiment, biometric data is encrypted and stored on a portable gaming instrument and used to verify the identity of a person attempting to redeem any value on a portable gaming instrument.

[0034] The portable gaming instrument refers to any device used to carry value or convey value in a gaming establishment. This may include a paper ticket or voucher, a smart card or debit card, for example. Other portable gaming instruments (also often referred to as 'credit devices') are suitable for use herein. A printed credit device generally refers to any portable gaming instrument suitable for interaction with a gaming machine that includes some form of printing thereon. Exemplary printed credit devices include printed-paper tickets and printed plastic cards. A paper ticket may comprise any card stock or gloss covering as determined by a desired quality for the ticket and/or by a scanner included in a gaming machine that receives the ticket. Printing on plastic cards is becoming increasingly popular, less expensive and is suitable for use with the present invention. Plastic cards that include a magnetic strip that stores information are also suitable for use herein. Some casinos issue player identification or player tracking cards that furnish a person awards for frequent patronage. Before beginning play, a player presents the card to a magnetic card reader that communicates with the gaming machine. The reader detects the card, and software on the gaming machine or network notes the card value and verifies player identity, as will be discussed in further detail below. The credit device is often portable. A person may carry the portable gaming instrument until redemption at a gaming machine, cash-out station or another location in a gaming establishment that redeems portable credit devices. Although the present invention will now primarily be described with respect to printed tickets to ease description and discussion, it is understood that secure redemption techniques discussed herein are applicable to any portable gaming instruments and not just printed tickets.

[0035] A gaming establishment refers to any business or organization that operates at least one gaming machine on its premises and/or offers gaming machine services to potential customers. Exemplary establishments that currently operate gaming machines on their premises include casinos, hotels, airports, restaurants, nightclubs, grocery stores, gas stations and convenience stores. A gaming machine services provider may include a gaming machine manufacturer or a business that offers gaming machine services (such as progressive pools or financial services for ticket redemption). The same portable gaming instrument may be offered and redeemed by one or multiple establishments. For example, a portable gaming instrument may have been generated at one property, redeemed at that property, or redeemed at another property, such as a second casino.

[0036] When a person attempts to redeem value on a ticket, the present invention uses multiple security techniques to verify that the correct person is awarded value on the ticket. Generally, security can be classified into: a) what a person has, b) what a person knows, and c) who a person is. The first measure of security provided by the present invention relates to "what a person has"—a portable gaming instrument carried by the person. The present invention employs additional security measures. In one embodiment, biometric authentication ("who the person is") uses personal information to validate that the person redeeming the ticket is the person who received the ticket from a gaming machine. In another embodiment, a "what a person knows" redemption requirement prompts a person to enter a password or PIN number associated with the portable gaming instrument. Another layer of security encrypts biometric and other data on the ticket.

[0037] Biometric systems and methods described herein employ a combination of biometric data and encryption of the biometric data on a ticket. Before redeeming any value on the ticket, validation of the person trying to redeem the value includes a comparison of biometric data for the person that received the ticket (and stored on the ticket in an encrypted manner) with biometric data for the person trying to redeem the ticket.

[0038] Biometrics uses biological information to establish and verify identity. The basic idea behind biometrics is that each person's body contains unique properties that can be used to distinguish the person from others. 'Biometric data' refers to data used to identify a person based on a person's physical trait or behavioral characteristics. 'Biometric authentication' refers to the process of verifying the identity of a person based on his or her biometric data. Fingerprint identification is one example of biometric authentication. Retina scans, hand-written signatures, voice patterns and/or palm prints are all forms of biometric authentication that are suitable for use herein. Other forms of biometric authenti-

cation may also be used. In addition, there exists a wide number of specific techniques and technologies for each form of biometric authentication, and the present invention is not limited by any specific technique or technology of biometric data capture, biometric authentication, and/or data storage.

[0039] Most fingerprint validation systems compare specific features of a fingerprint, generally known as minutiae. Typically, the comparison concentrates on points where ridge lines end or where one ridge splits into two (bifurcations). Fingerprint validation software uses one or more algorithms to recognize and analyze these minutiae from a fingerprint image. The algorithm measures the relative positions of minutiae, and to get a match, the scanner system does not have to find the entire pattern of minutiae both in the sample and in the print on record, it simply has to find a sufficient number of minutiae patterns that the two prints have in common. The exact number varies according to the algorithm and user design. There a wide variety of fingerprint validation systems and algorithms known to those skilled the art and suitable for use with the present invention.

[0040] Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare a person's face to a stored image. To validate someone's identity, facial recognition software compares information from a newly captured image with information from a stored image on the ticket. In a specific embodiment, facial recognition includes the following steps: alignment, normalization, and representation. Alignment turns a face toward a camera for recognition (e.g., at least 35 degrees or some other threshold angle). Normalization scales and rotates a head so that it can be registered and mapped into an appropriate size and pose. Representation translates the facial data into a unique code. This coding process allows for comparison of the acquired facial data to the stored facial data obtained from the ticket. The newly acquired facial data is then compared to the stored data for biometric authentication. Facial recognition may use one or more algorithms or mathematical techniques to encode a face, such as the Local Feature Analysis (LFA) algorithm. This algorithm maps a face and creates a faceprint, or a unique numerical code for that face. Exemplary facial features that may be quantified and used for comparison include a distance between eyes, wit of knows, depth of eye sockets, cheekbones, jaw line, chin, etc.

[0041] As mentioned above, the biometric data is encrypted or otherwise protected when stored on a portable gaming instrument. For instance, fingerprints, scanned signatures and voice authorization records may be stored in a 2-D bar-code (see **FIGS. 8A-8D**). The encryption prevents open access to the biometric data. As will be described in further detail below, data protection and storage on the credit device will vary with the credit device. Printed tickets may include 1-D and/or 2-D barcode printing that stores voice authorization data recorded at a gaming machine, for example. Wireless identification cards may include digital memories that store encrypted biometric data.

[0042] In one embodiment, public and private keys are used to provide encryption. The keys may be distributed to gaming machines in a network. In this case, a gaming machine in the network obtains biometric data of a person that has interacted with the gaming machine. The gaming machine then encrypts and signs the biometric data with a private key assigned to the gaming machine or to a portable gaming instrument output by the gaming machine. The gaming machine then stores the encrypted biometric data on a ticket, and provides the ticket to the person.

[0043] As the term is used herein, 'value' on a portable gaming instrument refers to any monetary worth, player incentive or attraction, and/or other quantity stored a portable gaming instrument or otherwise conveyed with a portable gaming instrument. Cash value is very common, such as an amount of money won by a person at a gaming machine after playing a game and awarded by the gaming machine to a printed ticket output by the gaming machine. The value may also include player tracking quantities, incentive awards offered by gaming establishments, loyalty program points, and the like. In general, the value may refer to any quantity that is redeemed by a person in a gaming establishment. 'Redemption value' refers to the value on a portable gaming instrument when a person attempts to redeem any value on the instrument, whether the person chooses to redeem full or partial value conveyed with a ticket.

[0044] Incentive awards may include any prize, item or services items offered by a casino or gaming establishment that have monetary value or otherwise attract patrons to the gaming establishment. Such incentives may include meals and food service, rooms and room service, entertainment shows, promotional game play, or concerts and events at which tickets, vouchers or the like that may be issued and redeemed or used at selected events. Other incentive awards are suitable for use herein.

[0045] Loyalty points refers to any type of points accrued for participating in designated activities at a gaming establishment. Designated activities include, but are not limited to, gaming activity such as playing gaming machines, card games such as black jack, pai gow poker, baccarat and poker, betting on public event outcomes, table games such as roulette, craps, keno and lotteries, etc. Other patronage activities at gaming establishments may accrue loyalty points. In one sense, loyalty points represent a form of credit accrued for patronage. The points can be stored on a ticket and redeemed for a variety of goods or services (or translated to other forms of credit) within a gaming establishment or affiliated establishment. Player tracking points are a typical example of "loyalty points."

[0046] Loyalty point sessions are sessions during which a person is performing the designated activity and during which loyalty points accrue. Examples of events that trigger accrual of loyalty points include a player beginning to play a particular gaming machine, a player providing cash or indicia of credit to a gaming machine, a user actuating a mechanism allowing anonymous gaming activity, etc. Examples of events that can indicate the end of a loyalty points session include winning a jackpot or other conventional gaming award, a user actuating a mechanism indicating an end to the gaming activity, detecting that a particular period of inactivity has elapsed, etc.

[0047] In one embodiment, loyalty point sessions are triggered or initiated by events that need not involve conventional player tracking initiation events (e.g., insertions of player tracking cards). Thus, the person can begin accruing loyalty points even if he/she forgets to insert his/her player

tracking card or otherwise fails to initiate a conventional player tracking session. Further description of wireless and anonymous loyalty point sessions are described in commonly owned and co-pending U.S. patent application Ser. No. 10/214,936 entitled "FLEXIBLE LOYALTY POINTS PROGRAMS," filed Aug. 6, 2002, which was incorporated herein by reference above. Because loyalty point sessions may begin without a conventional player tracking initiation event, a more general concept may be applied to initiation of loyalty points sessions. In a specific embodiment, such initiation can be automatically detected by a gaming machine or other mechanism at a gaming establishment. Some activities such as black jack may require that a dealer or other person manually initiate the session.

[0048] The present invention finds wide use with gaming machines. **FIG. 1** shows an exemplary video gaming machine **2** suitable for use with the present invention. Machine **2** includes a main cabinet **4**, which generally surrounds the machine interior and is viewable by users. The main cabinet includes a main door **8** on the front of the machine, which opens to provide access to the interior of the machine. Attached to the main door are player-input switches or buttons **32**, a coin acceptor **28**, and a bill validator **30**, a coin tray **38**, and a belly glass **40**. Viewable through the main door is a video display monitor **34** and an information panel **36**. The display **34** may comprise a cathode ray tube, high resolution flat-panel LCD, or other electronically controlled video display. The information panel **36** may be a back-lit, silk screened glass panel with lettering to indicate general game information including, for example, the number of coins played. The bill validator **30**, player-input switches **32**, video display monitor **34**, and information panel are devices used to play a game on the gaming machine **2**. The devices are controlled by circuitry housed inside the main cabinet **4** of the machine **2**.

[0049] The gaming machine **2** includes a top box **6**, which sits on top of the main cabinet **4**. The top box **6** houses a number of devices, which may be used to add features to a game being played on the gaming machine **2**, including speakers **10**, **12**, **14**, a ticket printer **18** which may print bar-coded tickets **20** used as loyalty point instruments or cashless instruments, a key pad **22** for entering player tracking information or PIN numbers, a florescent display **16** for displaying player tracking information, and a card reader **24** for entering a magnetic striped card containing player tracking information. Further, the top box **6** may house different or additional devices than shown in **FIG. 1**. For example, the top box may contain a bonus wheel or a back-lit silk screened panel which may be used to add bonus features to the game being played on the gaming machine. During a game, these devices are controlled and powered, in part, by circuitry, such as a master gaming controller housed within the main cabinet **4** of the machine **2**.

[0050] Understand that gaming machine **2** is but one example from a wide range of gaming machine designs on which the present invention may be implemented. For example, not all suitable gaming machines have top boxes or player tracking features. Further, some gaming machines have two or more game displays—mechanical and/or video. And, some gaming machines are designed for bar tables and have displays that face upwards. Still further, some machines may be designed entirely for cashless systems. Such machines may not include such features as bill validators, coin acceptors and coin trays. Instead, they may have only ticket readers, card readers and ticket dispensers. Those of skill in the art will understand that the present invention, as described below, can be deployed on most any gaming machine now available or hereafter developed.

[0051] Gaming machine **2** includes a main processor, or gaming machine controller. When acting under the control of appropriate software or firmware, the processor (or CPU) implements game play and biometric authentication functions as described herein. The gaming machine controller may include one or more commercially available processors such as a processor from the Motorola family of microprocessors or the MIPS family of microprocessors. In an alternative embodiment, the processor is specially designed hardware for controlling the operations of a gaming machine. In one embodiment, one or more memories (such as non-volatile RAM and/or ROM) also forms part of the gaming machine controller. However, there are many different ways in which memory could be coupled to the processing system. To implement biometric authentication features of the present invention, the controller is designed or configured to i) provide a game play sequence comprising a presentation of one or more games of chance on the gaming machine, ii) decrypt the encrypted biometric data stored on a portable gaming instrument, iii) compare a) the biometric data for the person with b) the biometric data obtained from the portable gaming instrument, and iv) award the value on the portable gaming instrument to the person when the biometric information for the person matches the biometric information that was encrypted and stored on the portable gaming instrument. The gaming machine controller may also be configured to perform other duties described in the methods provided below.

[0052] To permit network communications, the gaming machine also include one or more interfaces that control the sending and receiving of data to and from a network and to support other peripherals such as a biometric reader. Suitable hardware interfaces and their respective protocols may include USB interfaces, Ethernet interfaces, cable interfaces, wireless interfaces, dial up interfaces, and the like. For example, the USB interfaces may include a direct link to an infrared camera as described above and a direct link to a host processor in a gaming machine.

[0053] Gaming machine **2** includes one or more biometric readers. As shown in this instance, machine **2** includes a fingerprint reader **27** configured to receive a person's finger and read and digitize a person's fingerprint information. Communications between fingerprint reader **27** and a processor for gaming machine **2** may use a USB or RS232 port on the computer system, for example. In one embodiment, fingerprint reader **27** includes an optical type system. Built inside an optical fingerprint reader is a small digital camera that captures a static picture of a player's fingerprint. The outer surface of this reader often includes a thin soft plastic membrane that can be scratched. Because of the physical isolation of the digital camera and the outer surface of the fingerprint reader, this system has high electrostatic isolation. The digital photograph is input into the fingerprint program and it creates a fingerprint template. In another embodiment, fingerprint reader **27** includes a capacitive fingerprint reader whose reading surface includes a series of small capacitors. A finger is placed on a thin insulating material that isolates the surface of the reader. Each of the

small capacitors provides a voltage change and this information is input into the fingerprint program that creates a fingerprint template. In one embodiment, fingerprint reader **27** produces fingerprint minutiae that are characterized and stored as an individual's fingerprint template. In a specific embodiment, the fingerprint template requires approximately 1000 bytes of stored information. Other sizes may be used.

[**0054**] Gaming machine **2** also includes a camera **31**. Retinal scan technology employs optical technology to map capillary patterns of a retina of the eye. Camera **31** may operate as a retinal scanner by assuming that a person's head remains relatively stationary during game play and in a known location relative to the display. Camera **31** may also be used for facial feature authentication.

[**0055**] Gaming machine **2** may also include a hand reader. Hand geometry systems employ optical systems to "map" key geometric features of the topography of a hand to verify an individual's identity. The hand geometry template often requires little data, such as only 10 bytes of data. In a specific embodiment, a hand geometry reader is built into an LCD monitor thus reducing space and cost.

[**0056**] Gaming machine **2** may also include a microphone for voice authentication. In this case, verification is accomplished by comparing a spoken PIN number or spoken password to the individual's digitally stored voice-print. The voice-print may be the same spoken PIN number or spoken password. Voice is a convenient biometric authentication system for use in telephonic transactions. The microphone may be built into a front panel of gaming machine **2** in a position that receives person's voice. When activated, first by game software, then by the player's voice, the received data is digitized into a voice-print for processing. Filtering may be used to separate the voice information from occasional background noises on the floor of a casino.

[**0057**] A signature reader may also be included, which includes any suitable signature pad for receiving handwritten input. A feature in automated signature identification systems is the ability to differentiate between aspects of the signature that are habitual (consistent) and aspects that change nearly every time the person signs their name.

[**0058**] Many possible games, including traditional slot games, video slot games, video poker, mechanical slot games, video blackjack, video keno, video pachinko, lottery games and other games of chance as well as bonus games may be provided with gaming machines of this invention. In general, the present invention is not limited to a specific game played on a gaming machine.

[**0059**] When a user wishes to play a game on the gaming machine **2**, he or she inserts cash through the coin acceptor **28** or bill validator **30**. Alternatively, the player may use a portable credit instrument of some type to register credits on the gaming machine **2**. For example, the bill validator **30** may accept a printed ticket voucher, including **20**, as an indicia of credit. As another example, the card reader **24** may accept a debit card or a smart card containing cash or credit information that may be used to register credits on the gaming machine. In addition, the player may use a loyalty program instrument, such as smart card, ticket voucher, or debit card, to register previously accumulated loyalty points on the gaming machine. Typically, the gaming machine validates information contained on the portable gaming instrument or loyalty point instrument, such as validating the redemption value against a stored value for the ticket on a database server. Using biometric data, gaming machine **2** also verifies the identity of the person to ensure that the original recipient of the printed ticket voucher, debit card or smart card is the same as the person currently providing it to the gaming machine.

[**0060**] During the course of a game play session, a player may be required to make a number of decisions, which affect the outcome of one or more games played during the game play session. For example, a player may vary his or her wager on a particular game, select a prize for a particular game, or make game decisions which affect the outcome of a particular game. The player may make these choices using the player-input switches **32**, the video display screen **34** or using some other device which enables a player to input information into the gaming machine. During certain game events, the gaming machine **2** may display visual and auditory effects that can be perceived by the player. These effects add to the excitement of a game, which makes a player more likely to continue playing. Auditory effects include various sounds that are projected by the speakers **10**, **12**, **14**. Visual effects include flashing lights, strobing lights or other patterns displayed from lights on the gaming machine **2** or from lights behind the belly glass **40**.

[**0061**] The present invention increases the integrity of portable gaming instruments used with gaming machines by encrypting and storing biometric data on a portable gaming instrument; and subsequently uses the stored biometric data to verify the identity of a person attempting to redeem any value on a portable gaming instrument. **FIG. 2** illustrates a process flow **200** for providing a portable gaming instrument for use with a gaming machine in accordance with one embodiment of the present invention. Processes in accordance with the present invention may include up to several additional steps not described or illustrated here in order not to obscure the present invention.

[**0062**] Process flow **200** may begin in response to a request to finish interaction with a gaming machine. When a player is ready to cash out and leave a gaming machine, he or she typically wants to take any accrued value. This is called cashing out. The person often presses a 'Cash Out button' on the gaming machine and the gaming machine starts a Cash Out sequence.

[**0063**] At this point, a processor or central controller within the machine assigns a value to the portable gaming instrument (**202**). This includes calculating one or more transaction elements associated with the transaction, including a cash out value and/or loyalty program information. The cash out value after interaction with the gaming machine may include winnings from the gaming machine. Other transaction elements may also be assigned to the ticket, such as a ticket number, time of printing, gaming machine number, etc. The value and transaction elements may also be sent to a central server via a network associated with the gaming machine.

[**0064**] In this case, value assigned to the ticket is assessed at the time of cash-out from the gaming machine. In one embodiment, a single instrument stores both cash transaction information and/or loyalty program information. For instance, a smart card may store credits for a gaming

machine and an award of some type. Also, the smart card may be used to store loyalty program information generated during one or more of a player's game playing activities. Further, a smart card may store prize information for a prize redeemed at a gaming machine using loyalty points accrued by the game player.

[0065] Prior to issuing the instrument, the value awarded to the player may be displayed on a main display **34** (see **FIG. 1**), the secondary display **42** or the player tracking display **16**. Also, a prize menu may be displayed on one or more displays on the gaming machine **2** such as the main display **34**, the secondary display **42** or the player tracking display **16**. The prize menu may include one or more goods and services items. To acquire a particular prize, a particular amount of loyalty points is needed. As service items, the game player may be able to convert the awarded loyalty points to frequent flyer miles, obtain a free meal with the loyalty points or obtain a free nights lodging. As an example of goods items, a player may be able to redeem loyalty points for clothes, food items, electronic goods, concert tickets, etc. If the person selects such a prize, it is added to the ticket as assigned value for subsequent redemption.

[0066] Process flow **200** then obtains biometric data for a person that has interacted with the gaming machine (**204**). From the gaming machine perspective, a Cash Out sequence operated by the main controlled may prompt a player for their biometric data, and reading data according to a biometric reader included in the gaming machine. The biometric data may include fingerprint data, retina data, handwritten data, voice pattern data and/or palm print data, for example. Other forms of biometric data may also be obtained. The method and devices used to obtain the biometric data will vary with the type of biometric data. Fingerprint data may be obtained by prompting the person to put their finger on a fingerprint reader included with the gaming machine. There are a number of different ways to obtain an image of somebody's finger; the most common methods used today are optical scanning and capacitance scanning. A camera included with the gaming machine may obtain face recognition data—at any time during a game play session. The biometric data may thus be obtained by the gaming machine during a game play session, or obtained from a server that stores the biometric data and references the biometric data according to player tracking information that correlates the person and their biometric data (typically according to some player tracking number for the person). In this case, the gaming machine communicates with the remote server (e.g., across a network) using some form of identification for the person to obtain the biometric data. Redeeming any value on this device then requires authentication of encrypted biometric data on the portable gaming instrument, as will be described in further detail below.

[0067] The biometric data is encrypted to produce encrypted biometric data (**206**). The biometric information is encrypted so no one other than the casino is able to decode the stored biometric information taken from the player at the time of cash out. The encryption generally refers to any mathematical algorithm or technique used to protect data from open access. As described with respect to **FIGS. 3 and 4**, public and private keys are well-suited for use to encrypt the biometric data. In this case, authorized users of encrypted fingerprint data must have the private key that was used to encipher the data in order to decrypt it. The encryption algorithm is commonly known. The unique key chosen for use in a particular application makes the results of encrypting data using the algorithm unique. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. Thus, biometric data can be recovered from cipher only by using the same private key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct private key cannot derive the original data algorithmically. However, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

[0068] Other techniques may be used. For example, an encryption algorithm such as DES, "Data Encryption Standard", is suitable for use. DES uses a key of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte.

[0069] The person's encrypted biometric data is also stored on the portable gaming instrument (**208**) for subsequent identity authentication of a person holding the ticket upon redemption of any value on the ticket. After the player has completed a game play session, a gaming machine thus generates the portable gaming instrument with the encrypted biometric data included thereon. The portable gaming instrument may be a printed ticket voucher, a smart card, debit card or other cashless medium. For example, in the case of the ticket voucher, a printer included in the gaming machine prints the ticket voucher on paper or some other medium. The gaming machine records the encrypted and non-encrypted information on the portable gaming instrument when the instrument is generated. A unique 1-D or 2-D bar-code may be printed on the ticket voucher, which may be read with a bar-code scanner to obtain information from the ticket.

[0070] Printer **18** (see **FIG. 1**) prints the ticket voucher **20**. A wide variety of printers are suitable for use with gaming machine **2**. Printer **18** may be selected from the group consisting of a thermal contact printer, an inkjet print and a laser printer. The printer may be configured to print data in a 1-D bar-code format, a 2-D bar-code format and combinations thereof. Further, the printer may be capable of printing in a format that is invisible, such as using an invisible ink.

[0071] In the case of the smart card or debit card, the generation of the smart card or debit card refers to storing or encoding this information on the smart card or debit card. The generation of the debit card or smart card may occur when the smart card or debit card is inserted into the card reader **24** in the gaming machine **2** or at another site where smart cards or debit cards are issued. For example, smart cards or debit cards may be generated at ATM like terminals, at a cashier station when a player cashes out or prepaid smart cards or debits may be purchased within the gaming property (e.g. casino). In a particular embodiment, the printer or another output device is capable of generating an electronic circuit on a printable media used as a portable gaming

instrument. The printable media may be flexible. The electronic circuit may be programmed to store the value, and may be part of an RFID tag. As another example, the gaming machine may transfer cash value and/or loyalty point information to portable wireless device worn by the player via a wireless interface (not shown) on the gaming machine **2**.

[**0072**] The person removes the ticket from the gaming machine. The ticket can be placed back into the same gaming machine at a later time, placed into another gaming machine, or redeemed for any value conveyed on the ticket.

[**0073**] In one embodiment, the present invention uses a public and private key distribution system for encryption of the biometric data on portable gaming instruments. **FIG. 3** illustrates a process flow **220** for providing public and private keys to gaming machines in accordance with one embodiment of the present invention.

[**0074**] Process flow **220** employs a server-based network architecture in a gaming machine environment. One suitable network architecture is described below with respect to **FIG. 7**.

[**0075**] Process flow **220** begins by generating private keys for use in a gaming machine network (**222**). The system server (or 'system computer') generates and stores a set of private keys to be used for biometric template encryption and protection. The private keys may be generated on a per gaming machine basis, a per portable gaming instrument basis, or both. In some cases, the server manages and distributes public and private keys to both gaming machines in a network and to portable gaming instruments accepted in the network.

[**0076**] In one embodiment, the server assigns a private key to each gaming machine in a network (**224**). A gaming machine serial number may be used to reference this assignment. For example, when a gaming machine is installed on the floor in a casino, communications between the gaming machine and the server take place. The server in these initial communications commonly assigns a serial number to the gaming machine. In this case, the server also assigns a private key to the serial number and gaming machine. This may occur weeks, months or years before a specific incident of using the private key to encrypt biometric data on the ticket. The system computer then transmits the private key to the gaming machine with that serial number (**226**). The gaming machine stores the private key.

[**0077**] In one embodiment, process flow **220** verifies the encryption system (**228**). One suitable verification encrypts a known block of data into an encrypted block at the gaming machine. This block is then transmitted to the server. If this known block verifies at the server, then the private key has been transmitted and received correctly. In another embodiment, process flow also updates the private keys (**230**). This is considered an optional step and is not necessary. If it is decided to update the private keys, then process flow **220** returns to step **222**.

[**0078**] As mentioned above, the present invention may also a sign private keys to individual portable gaming instruments, such as loyalty points program or player tracking cards, to permit encryption of biometric data on a personal card. **FIG. 4** illustrates a process flow **240** for storing encrypted biometric data on a personal cards and on a server in accordance with one embodiment of the present invention.

[**0079**] Process flow **240** begins by generating a set of private keys for use with portable gaming instruments (**242**). The system computer will generate and store a series of private keys to be used for this purpose. When a person requests a loyalty points program or player-tracking card, one of these private keys is assigned to their card (**244**).

[**0080**] A person may also be asked to provide one or more forms of biometric information (**246**). This may occur when the person registers for a loyalty points program or a player tracking program, and/or when the person requests a new card for one of these programs. The biometric information may include fingerprint information obtained using a fingerprint reader, face recognition information contained in an image captured by a camera, retinal information contained in an image captured by the camera, hand-written information obtained using a digital signature recorder, voice pattern information stored in an audio file and obtained using a microphone, and/or palm print information obtained using a palm print reader, for example.

[**0081**] Software associated with the biometric authentication converts the biometric information into biometric data representative of the biometric information and the person (**248**). For example, fingerprint information may be converted into a fingerprint template according to an algorithm that generates, analyzes and recognizes minutiae from a fingerprint image. Alternatively, face recognition software may be used to translate facial information included in an image into a unique code (data) representative of a person.

[**0082**] The server then uses a private key assigned to the person's portable gaming instrument to encrypt the biometric data (**250**). This prevents biometric information in data from being opened in unprotected on a player tracking card and similar instruments. It also helps gaming establishments such as casinos reward loyalty infrequent patronage by ensuring that the right person redeems image rewarded for frequent painter to patronage in the casino.

[**0083**] The encrypted biometric data is then stored on the portable gaming instrument (**252**). The encrypted biometric data may be stored as magnetic data, a "spread-spectrum" barcode or the like on a player tracking card. The player tracking card is now ready for use. The server also stores a copy of the encrypted biometric data. This will be used during redemption of any value on the loyalty points program card or player tracking card.

[**0084**] A "spread-spectrum" barcode system permits added security and reliability. The "spread-spectrum" barcode system uses a gray scale (all numbers between 1 and 0 including 1 and 0) to encode the encrypted data onto the surface of the ticket. Each bit of data is encoded pseudo-randomly across the entire barcode. All of the encoded bits are then overlaid to form a grayscale, or an analog barcode image. Because each bit of data is spread redundantly across the barcode, all of the data can be recovered even when some or most of the barcode is missing (providing you know the private key to the pseudo-random code). Further description of barcode and similar systems is provided below.

[**0085**] So far, the present invention has generated portable gaming instruments such as loyalty points program cards, player tracking cards and paper tickets with encrypted biometric information stored thereon. The owners of these instruments may use or hold on to these devices, as desired.

[0086] At some subsequent time, someone will attempt to redeem value on the portable gaming instrument. This may or may not be the same person as the person who received the instrument from the gaming machine. **FIG. 5A** illustrates a process flow **260** for redeeming value on a portable gaming instrument in accordance with one embodiment of the present invention.

[0087] Process flow **260** begins by receiving a request to redeem the value on the portable gaming instrument (**262**). This may occur at a gaming machine, a casino kiosk, a hand-held wireless device, a clerk validation terminal in a networked gaming system, a cash out station in a casino, a cash cage in a casino, a wireless walk around cash out station, another gaming machine that has a built in gash out station, or a cash out station associated with a server or system computer. Collectively, these may be referred to as a gaming device that validates the portable gaming instrument. In one embodiment, value redemption and biometric authentication uses a server (**FIG. 5B**). For process flow **260**, value redemption and biometric authentication may occur solely at the gaming device (**FIG. 5A**). For example, a gaming machine can be constructed such that a cash out Station is part of the gaming machine. This station may not dispense money for a ticket but instead credits the machine from value on the ticket. Thus, the player would receive credits on the gaming machine instead of money.

[0088] Loyalty points may redeemed on a gaming machine for a number of purposes such as to access a special bonus feature available on the gaming machine or to obtain goods and services. The portable gaming instrument contains information used to register loyalty points on the gaming machine and validate the transaction. For example, when a ticket voucher is used as a portable gaming instrument for a loyalty program, the printed ticket voucher may contain information including but not limited to: 1) a ticket value, 2) a ticket issue date, 3) a ticket issue time, 4) a ticket transaction number, 5) a machine ID, 6) a ticket issue location, 7) a ticket sequence number and 8) biometric data. Some or all of the information may be encrypted on the portable gaming instrument. Information such as the ticket value, the ticket issue date, the ticket issue time, the ticket number and the machine ID may be common to loyalty program systems that generate and validate tickets issued at a single property. However, information such as the ticket issue location and other information may be needed to allow multi-site generation and validation of loyalty program instruments. In addition, other types of information, besides the information listed above, may be stored on the loyalty program instrument. For example, the ticket may contain information regarding a promotional prize that may be redeemed for loyalty points by the player when the ticket voucher is utilized in a gaming machine. As another example, the ticket may contain information such as a number of additional loyalty points that are needed to obtain a particular goods or services item.

[0089] Upon receiving a request for redemption of value on the portable gaming instrument, either for redemption by a gaming machine or at cash-out, biometric authentication is used to verify identity of the person requesting the redemption. Biometric authentication compares a) biometric data stored and encrypted on the portable gaming instrument with b) a biometric data obtained for the person upon redemption.

[0090] To do so, the gaming device first reads the encrypted biometric data stored on the portable gaming instrument (**264**). For a ticket including a barcode, a reader on the gaming machine reads the printed information on the ticket, which includes the bar code containing any winning information and containing the encrypted biometric data that was printed on the ticket at cash out by a gaming machine.

[0091] The gaming device then decrypts the encrypted biometric data (**264**). The encrypted biometric data includes the biometric data that was used to produce the encrypted biometric data. Decryption employs a public key that corresponds to the private key used to encrypt the biometric data. The biometric data identifies a person who received the portable gaming instrument.

[0092] The gaming device also obtains biometric information for a person trying to redeem the value on the portable gaming instrument (**268**). In this case, the gaming device prompts the user for their biometric data according to the information stored on the ticket. If the ticket includes fingerprint data, then the gaming device obtains fingerprint information using a fingerprint reader included therewith, and converts the fingerprint information to fingerprint data using the algorithm that produced the fingerprint data on the ticket.

[0093] Process flow **260** then compares a) the biometric information for the person trying to redeem the value on the portable gaming instrument with b) the biometric information obtained from the portable gaming instrument (**270**). As mentioned above, the biometric authentication algorithm does need an exact match of the biometric data, such as an exact match of the entire pattern of minutiae both in the sample and in the data from the ticket, it simply has to find a sufficient threshold of biometric data that the two sets of biometric data have in common. The exact threshold varies according to the algorithm and user design.

[0094] When the biometric information for the person matches the biometric information that was encrypted and stored on the portable gaming instrument, then the gaming device awards the value on the portable gaming instrument to the person (**272**). Any discrepancies between the biometric data stored and encrypted on the portable gaming instrument and the biometric data obtained for the person trying to redeem the value on the portable gaming instrument may be investigated. In this manner, anyone other than the ticket recipient may be detected.

[0095] Redemption may also include a transfer of the awarded cash and/or loyalty points to a player tracking account. After providing account information (e.g., by inserting a player tracking card) and biometric authentication according to the present invention, the player tracking points are transferred to a player tracking account for the player. In other embodiments, the player may credit player cash, tracking points and/or loyalty points, stored on a loyalty point instrument, to a player tracking account 1) over the phone, 2) at a clerk validation terminal, 3) at a cashier station, 4) at a casino kiosk, 5) via a web-interface, 6) via mail or 7) through a hand-held wireless device.

[0096] In some embodiments of the present invention, value on a portable credit device may be combined with previously earned loyalty points to redeem a prize. Thus, loyalty points stored in one or more of a player's loyalty

program accounts, such as a player tracking account, or loyalty points earned during other activities stored on one or more loyalty program instruments available to the player may be used to redeem prizes on the gaming machine. For instance, the player may insert five printed tickets containing various amounts of loyalty points into the gaming machine **2** using the bill validator **30**. After the person's identity for each ticket has been validated, the loyalty points stored on each ticket may be added to the amount loyalty points available on the gaming machine. As another example, the player may request that loyalty points be deducted from a loyalty program account such as a player tracking account. In this case, the gaming machine may send a message to remote server storing the loyalty point account information and request that some amount of loyalty points be deducted from the player's account. Assuming the amount of requested points is available, the requested points may be deducted from the player's account and then transferred to the gaming machine. Finally, the method described above, may be implemented when the player has not accrued any loyalty points during a particular game playing session. For instance, the player may desire to redeem a prize using one or more loyalty program instruments storing loyalty points previously earned by the game player.

[**0097**] **FIG. 5B** illustrates a process flow **280** for redeeming value on a portable gaming instrument that uses a network architecture in accordance with another embodiment of the present invention. In this case, value redemption and biometric authentication uses a server. For example, a loyalty point instrument, player tracking card or paper ticket may be validated in a manner consistent with an EZPAY™ cashless system provided by IGT of Reno, Nev.

[**0098**] Details of apparatus and methods used to validate a cashless instruments and that may be applied to the validation of the present invention are described in commonly owned and co-pending U.S. application Ser. No. 09/544,884 by Rowe et al. filed Apr. 7, 2000 entitled "Wireless Gaming Environment" which is incorporated herein in its entirety and for all purposes. Details of apparatus and methods used to validate a cashless instrument across multiple gaming properties and may be applied to the validation of portable gaming instruments across multiple gaming properties are described in co-pending U.S. application Ser. No. 09/684,382 by Rowe filed Aug. 25, 2000 entitled "Cashless Transaction Clearinghouse" which is incorporated herein in its entirety and for all purposes. Details of apparatus and methods of using a smart card as a cashless instrument, at a single gaming property or across multiple gaming properties, that may be applied to the use of a smart card as a loyalty point instrument, at a single gaming property or across multiple gaming properties, are described in co-pending U.S. application Ser. No. 09/718,974 by Rowe filed Nov. 22, 2000 entitled "EZPAY™ Smart Card and Ticket System" which is incorporated herein in its entirety and for all purposes. Details of providing secure transactions for a cashless system which may applied to a loyalty program instrument system are described in co-pending U.S. application Ser. No. 09/660,984 by Espin et al. filed Sep. 13, 2000 entitled "Transaction Signature" which is incorporated herein in its entirety and for all purposes.

[**0099**] Process flow **280** begins similar to process flow **260** and includes: receiving a request to redeem the value on the portable gaming instrument (**262**); reading encrypted biometric data stored on the portable gaming instrument (**264**); and decrypting the encrypted biometric data (**266**). Server and network-based redemption permits more flexible options for patrons of the gaming establishment to redeem value on portable gaming instruments. a player may redeem any value on a credit device at any gaming machine, a designated cash out window or a pay machine. When a credit device is redeemed at a cash out window, the cashier may verify the device by inputting the device number into the cashier station computer. In one embodiment where the credit device is a ticket including a bar-code, the cashier may input the ticket identification by scanning the ticket with a bar-code scanner.

[**0100**] The person's biometric information may also be received (e.g., using a fingerprint scanner or other biometric reader). Alternatively, the player's identity may be determined from a player tracking card inserted into the gaming machine. This identity may then be sent to a remote server that associates the person's biometric data with their identity on the player tracking card.

[**0101**] The request to redeem value on the portable gaming instrument is sent via a network interface on the gaming device validating the instrument to a server for the gaming network (**282**).

[**0102**] The server receives this data and uses it to determine if the person trying to redeem the ticket is the same person that received the ticket or cash to doubt any gaming machine (**270**). To do so, the server first decrypts the encrypted biometric data sent by the gaming device, using a stored public key associated with a private key used to encrypted data. The server may reference an index/number for the portable gaming instrument or gaming machine to determine if the private key used to encrypt the data was assigned to the gaming machine or to the portable gaming device. Process flow **280** then compares a) the biometric information for the person trying to redeem the value on the portable gaming instrument with b) the biometric information obtained from the portable gaming instrument. As mentioned above, a) may come from a gaming device and fresh biometric information provided by a person during redemption or from a stored biometric data for the person who is identified using a player tracking card or some other form of identification received by the gaming device.

[**0103**] If the validation request occurs at a gaming machine, the player will be credited the corresponding amount on the gaming machine (**272**) and the server sends this validation to the requesting gaming device. If the validation request occurs at a cashier's station, the player may be paid with the corresponding amount according to the cash out value stored on the ticket. The system may also print out a verification receipt for each ticket at the cashier's station. The cashier may store the ticket and the verification receipt. If the biometric data does not match, the cash out transaction is prevented, and the discrepancy may be logged and investigated.

[**0104**] Server-based validation may include additional steps. **FIG. 6** is a flow chart depicting a method for validating information stored on a portable gaming instrument at a validation site connected to a cross validation network as described with reference to **FIG. 7**. In **600**, a request for game service transaction information read from a portable gaming instrument is sent via a network interface on the

gaming device validating the instrument to a server. In **605**, the server identifies which gaming device owns the instrument. When a gaming device owns an instrument, the gaming device has stored information regarding the status of a particular instrument issued from a instrument generation site connected to the gaming device. As an example, the gaming device may be a CVT connected to a number of gaming machines that generate loyalty program instruments. In **610**, the server sends a request to validate the instrument to the gaming device identified as the owner of the instrument. Typically, the validation request indicates a service on the instrument has been requested. For instance, for a loyalty program ticket, a validation request may mean a request to access the loyalty points stored on the ticket has been made. For a loyalty program ticket valid for a free meal, a validation request may mean a request to obtain the meal has been made. In **615**, the instrument owner receives the validation request for the instrument and marks the instrument transaction pending. While the instrument transaction is pending, any attempts to validate a loyalty program instrument with similar information is blocked by the instrument owner.

[0105] In **620**, the instrument owner sends back a reply with context information to the server. As an example, the context information may include a request for biometric information or may include the time and place when the instrument was issued. The information from the instrument owner to the server may be sent as one or more date packets according to a communication standard shared by the instrument owner and server. In **625**, after receiving the validation reply from the instrument owner, the server marks the validation request pending and sends a validation order to the gaming device validating the instrument. While the validation request is pending, the server will not allow another instrument with the same information as the instrument with the validation request pending to be validated.

[0106] In **630**, the gaming device may chose to accept or reject the validation order from the server. For instance, using a biometric authentication security protocol, the gaming device may determine the validation order is invalid. As another example, an employee using a gaming device to validate loyalty program instruments may decide not to validate an instrument for some reason. When the gaming device accepts the validation order from the server, in **640**, the gaming device sends a reply to the transaction server confirming that the transaction has been performed. The loyalty program server marks the request validated or completed which prevents another instrument with identical information from being validated. In **645**, the server sends a confirmation to the instrument owner which allows the instrument owner to mark the request from pending to validated. When the gaming device rejects the validation order from the server, in **650**, the gaming device sends a reply to the server to mark the validation request from pending to unvalidated. When the instrument transaction is marked unvalidated, it may be validated by another gaming device at a later time. In **655**, the server sends the reply to the instrument transaction owner to mark the validation request from pending to unvalidated which allows the instrument to be validated later.

[0107] **FIG. 7** is a block diagram of the components of a portable gaming instrument system for one embodiment of the present invention. A portable gaming instrument system is the hardware components and software components needed to generate and validate portable gaming instrument such as loyalty program instruments. Components of the system may include 1) data acquisition hardware, 2) data storage hardware, 3) portable gaming instrument generation and validation hardware (e.g. printers, card readers, ticket acceptors, validation terminals, etc.), 3) auditing software, 4) portable gaming instrument validation software and 5) database software. Many types of portable gaming instrument systems are possible and are not limited to the components listed above. A loyalty program instrument system may be installed at each property utilizing loyalty program instruments. To allow multi-site validations of portable gaming instrument, the systems at each property may be linked via a clearinghouse. The relation of multiple loyalty program instrument systems connected to a loyalty program transaction clearinghouse is described U.S. patent application Ser. No. 10/214,936 entitled "FLEXIBLE LOYALTY POINTS PROGRAMS," filed Aug. 6, 2002, which was incorporated by reference above.

[0108] In some embodiments of the present invention, the portable gaming instrument system may be implemented in conjunction with a cashless system that generates cashless instruments. For example, a single instrument generation site may issue both cashless instruments and loyalty program instruments. For example, a gaming machine may issue printed tickets with a cash value that may be redeemed for cash or gaming credits as part of a cashless system or a gaming machine may issue printed tickets with a loyalty point value or a prize value that may be redeemed for goods and services as part of a loyalty program instrument system. Further, a single generation site may issue a plurality of different instrument types for cashless transaction and loyalty program transaction such as but not limited to smart cards, printed tickets, magnetic striped cards, room keys and portable wireless devices. In addition, a single validation site may accept and validate both cashless instruments and loyalty program instruments such as but not limited to smart cards, printed tickets, magnetic striped cards, room keys and portable wireless devices. An example of a cashless system that may be modified to implement both cashless instruments and loyalty point instruments with the present invention is the EZPAY™ system manufactured by IGT of Reno, Nev.

[0109] Returning to **FIG. 7**, a first group of gaming machines **365**, **366**, **367**, **368**, and **369** is shown connected to a first clerk validation terminal (CVT) **360** and a second group of gaming machines, **375**, **376**, **377**, **378** and **379** is shown connected to a second CVT **370**. The clerk validation terminals are used to store portable gaming instrument transaction information generated when a portable gaming instrument is issued at a generation site such as a gaming machine. The transaction information, which may be stored each time a portable gaming instrument is issued, may include but is not limited to prize information, biometric data, encryption information, loyalty point information, an establishment, a location, a bar code, a instrument type (e.g. ticket, smart card, room key, magnetic card, portable wireless device, etc.), an issue date, a validation number, an issue time, an instrument number, an instrument sequence number and a machine number. Also, the transaction information may include transaction status information such as whether the portable gaming instrument has been validated, is outstanding or has expired. Some of the transaction information

stored in the CVT may also be stored on the portable gaming instrument. When a portable gaming instrument is validated, the information stored in the CVT and the information stored on the portable gaming instrument may be compared as an added means of providing secure redemption.

[0110] All of the gaming machines are designed or configured to offer games, accrue loyalty points during a game play session, award a player some or all of the accrued game credits and loyalty points, and store value and other loyalty program information to a portable gaming instrument, such as a printed ticket, a magnetic striped card, a room key, a portable wireless device or a smart card, which is issued to the game player. The portable gaming instruments may be redeemed for goods and services, pending biometric authorization as described herein. In addition, the gaming machines and other redemption and validation sites at property **300** may accept portable gaming instruments issued at a different property from property **300** where the different property utilizes the same or a different portable gaming instrument system as compared to property **300**. Details of a multi-site loyalty program instrument system are described in commonly owned patent application Ser. No. 10/214,936, which was incorporated by reference above.

[0111] A player may participate in a number of activities at the gaming establishment of property **300** for which the player can earn cash, loyalty points and other value. For instance, loyalty points may be earned while playing a game of chance at pit games **337**, while playing one of the gaming machines, or while making a food purchase, an entertainment purchase, a transportation purchase, a lodging purchase, a merchandise purchase or a service purchase at one of the other venues **338** at property **300**. Further, food purchases, entertainment purchases, transportation purchases, lodging purchases, merchandise purchases and service purchases that earn loyalty points for a patron may be made at venues outside of traditional gaming establishments but in affiliation with a gaming establishment. For instance, a patron may make a food purchase at a restaurant affiliated with a gaming establishment or may make merchandise purchase with a retailer affiliated with the gaming establishment. After their purchase, the patron may be issued a loyalty point instrument with a number of loyalty points that may be redeemed for goods, services and comps or may be later added to a loyalty point account of the patron.

[0112] After each activity, a player may be issued 1) a portable gaming instrument or new loyalty program instrument storing the loyalty points earned for the activity or 2) an existing portable gaming instrument may be updated to store additional loyalty points. For instance, the existing portable gaming instrument may be, a smart card, already storing loyalty points earned from previous activities. The smart card may be modified to store additional loyalty points after each new activity. Accumulated loyalty points earned by a player and stored on a loyalty program instrument may be redeemed for goods, services and comps at various loyalty program validation sites at property **300**, such as but not limited to: i) gaming machines, ii) cashier stations **325**, **330**, **335**, iii) a casino kiosk **359**, iv) from a casino service person with a hand-held wireless device **358** and v) at a clerk validation terminal **360** or **370**.

[0113] A game player may wish to use a portable gaming instrument issued during one activity during another activity at property **300**. For example, a game player may participate in a pit game **337** such as craps, roulette, black jack, etc. and may be issued a portable gaming instrument, such as a printed ticket, with a number of loyalty points based upon the manner in which they participated in the activity such as an amount wagered over a particular amount of time. Next, the player may desire to use the portable gaming instrument during another activity such as a game play session on one of the gaming machines **365**, **366**, **367**, **368**, **369**, **375**, **376**, **377**, **378** and **379**. After the person's identification and the portable gaming instrument have been validated, any value and loyalty points stored on the loyalty point instrument may be used by the player to redeem prizes, goods, or services available on the gaming machine. In one embodiment, for promotional purposes, only particular prizes, goods or services may be available on particular gaming machines to encourage game play of those machines. In another embodiment, a player may redeem loyalty points stored on a loyalty point instrument to access a special bonus features or game play features on a gaming machine. For example, after the play has been issued a printed ticket with loyalty points during one activity, the player may initiate a game play session on a gaming machine by entering the printed ticket into a bill validator on the gaming machine. After the person and ticket has been validated, some or all of the loyalty points stored on the printed ticket may be used to access a special bonus game or a special game play feature available on the gaming machine such as a chance to win a special jackpot. For instance, a player may commit five hundred loyalty points earned from a lodging purchase, stored on a loyalty program instrument, to activate a bonus feature on a gaming machine.

[0114] In **FIGS. 9-10**, apparatus are described for communication between various portable gaming instruments and a gaming machine. The apparatus and methods employ a non-physical contact data interface that allows for data to be read from a portable gaming instrument without physical contact between the data interface and the portable gaming instrument. Examples include a bar-code scanner and a wireless interface.

[0115] A card reader and a magnetic striped card are commonly employed in providing a player tracking session on a gaming machine. The data interface in a card reader includes contact between a magnetic head and the magnetic-stripe on the card to read data from the card. When a magnetic striped card is used in a player tracking session, which is one type of loyalty program session, the session is initiated when physical contact between the magnetic stripe and magnetic reader is detected. Typically, the card is inserted in a card reader. For a successful read of the magnetic stripe, the length of the stripe is moved over a magnetic head in the card reader. The movement of the magnetic stripe over the magnetic head can be supplied by 1) a force supplied by a user (e.g., the act of the user inserting the card forces the stripe over the magnetic head) or 2) a force supplied by servo-mechanisms within the card reader.

[0116] The magnetic head is used to read data stored on a number of tracks on the magnetic stripe. The magnetic stripe may contain a number of tracks, usually three, but all of the tracks may not be used. In most player tracking implementations, the first track is used to store a number, the number is an index to a record in a player tracking database or the

number may include encrypted biometric data stored on the card. The second track may be used to store a name such as the property where the card was issued. The third track is optionally used. In a specific embodiment, the first track contains up to 80 characters of data and the second track contains up to 40 characters of data.

[0117] For the generation of a player tracking session, the striped card is inserted in the card reader, the index number is read from the magnetic striped card and then is transmitted to a remote server. As part of the validation process for the player tracking session, a player is required to enter biometric data and/or a PIN number. After the session is validated, parameters from game play performed on the gaming machine, such as an amount bet, is converted to player tracking points by the remote server. The player tracking session ends when the player removes the magnetic striped card from the card reader.

[0118] **FIGS. 8A-8D** illustrate exemplary printed portable gaming instruments and data formats of the present invention. In **FIG. 8A**, a substrate **900** with a 1-D bar-code is shown. The 1-D bar-code may be used to encode an index to a record in a database or store an encrypted number. A standard Universal Product Code (UPC) symbol provides a 12 digit number. However, longer or shorter numbers may be encoded in a 1-D bar-code format.

[0119] In **FIG. 8B**, a substrate with a 1-D bar-code and a 2-D bar-codes **904** are shown. The 2-D bar-codes may be used to encode a much large amount of data than a 1-D bar code. In **FIGS. 8A and 8B**, the 1-D bar-codes and 2-D bar-codes may be read with a bar-code reader, such as a LS 6800 series bar-code reader from Symbol Technologies (Holtsville, N.Y.).

[0120] In **FIG. 8A**, the substrate **900** is printed with three **1**-D bar-codes **902**. The 1-D bar-codes encode the same number or different numbers. For instance, the bar-codes at the edge of the substrate **8**A may encode one number while the large bar-code in the center of the substrate **900** may encode a different number than then number at the edges. The size and orientations of the 1-D barcodes allow the bar-codes to be read at different orientations and distances from the bar-code reader.

[0121] In one embodiment, the bar-codes (1-D/2-D) may be printed on a substrate, such as a plastic wallet sized rectangular shaped card (e.g., credit card sized), a printed ticket and a plastic device designed to be attached to a key ring. In this case, the bar-codes may be printed on the top-side of the substrate, the bottom side of the substrate or both. The information encoded on the top-side and the bottom side of the substrate **900** may be the same or may be different. When the information is on the top-side and the bottom-side is the same, the information may be read from the substrate when either top-side or the bottom side is orientated toward the reader. In another embodiment, different information may be optionally encoded on the top-side and the bottom-side of the substrate. For instance, a 1-D bar-code may be printed on a top-side of the substrate **900** and an optional 2-D bar-code may be printed on the bottom side of the substrate. In this case, information may be read from a first side of the substate and the substrate may be optionally flipped to read information from the second side of the substrate.

[0122] In one embodiment of the present invention, the 1-D/2-D bar-codes may be printed on a substrate with an adhesive backing. Thus, the substrate may be attached to a plurality of devices that may be carried by the player. For instance, the substrate may be attached to a credit card carried by the player, a magnetic striped room key, a cell phone, a person digital assistant, a watch band, a purse, a wallet, an item of clothing, etc. The surface on which the printed substrate is attached does not necessarily have to be flat. Many bar-code readers are capable of reading bar-codes placed on curved surfaces. A player may be issued a sheet of bar-codes with adhesive backing so that the bar-codes may be placed on a plurality of devices.

[0123] In another embodiment, the bar-code may be printed on a bracelet that may be worn by the player, similar to a hospital bracelet. The player may place the bracelet near the bar-code reader to have it read. After the player is finished with the bracelet, it may be discarded.

[0124] In another embodiment, the gaming machine or another gaming device may be capable of scanning a plurality of 1-D bar-codes and 2-D bar-codes and combining them on a single instrument. For example, a plurality of 1-D bar-codes providing index numbers for a plurality of player tracking clubs may be read by the bar-code reader or the index numbers may be read by another input device on the gaming machine. Then, the all of the 1-D bar-codes may be formatted and printed on a single instrument, such as a printable media with an adhesive backing or a printed ticket. In another example, the plurality of 1-D bar-codes may be combined into a single 2-D bar-code. The 2-D bar-code may be printed on a single instrument, such as a printable media with an adhesive backing or a printed ticket, that may be carried by the player. In yet another embodiment, all of the index may be combined in a single RFID tag.

[0125] As described above, 1-D/2-D bar-codes may be used with the present invention. In an ordinary (1-D) bar-code, the data is encoded in a vertically redundant format, i.e., the same information is repeated vertically. This allows the heights of the bars to be truncated without any loss of information. The vertical redundancy also permits a symbol with printing defects, such as spots or voids, to still be read. The higher the bar heights, the greater probability that at least one path along the bar-code will be readable.

[0126] A 2-D bar-code symbol stores information along the height as well as the length of the symbol. Since both dimensions contain information, some of the vertical redundancy is lost. To insure accurate reading, most 2-D bar-codes use check words to insure accurate reading. An advantage of a 2-D bar-code symbol is that significantly more data may be encoded and encrypted compared a 1-D bar-code symbol. With a 2-D bar-code symbol, an entire record of a database can be stored on a single 2-D bar-code symbol rather than just an index to a record.

[0127] When a 2-D bar-code is employed, data processing, such as but not limited to parsing, editing, formatting, re-ordering, optical character recognition, encrypting/decrypting, format conversion, may be utilized to process the data read from the 2-D bar-code by the bar-code reader. The data processing may be performed by a logic device located in the bar-code reader, a logic device in communication with the bar-code reader and combinations thereof. Thus, the bar-code reader may include a communication interface for communicating with processors located on other gaming devices, such as a processor located in a player tracking unit,

the master gaming controller on the gaming machine or a processor on a remote server.

[0128] A 2-D bar-code is one example of a 2-D symbol encoding format. In general there are many types of 2-D symbol formats that may be employed with the present invention. Often the term 2-D bar-codes and the term 2-D symbols are used interchangeably to describe a 2-D symbol encoding information. These 2-D symbol formats include but not are limited to, 3-DI, ArrayTag, Aztec Code, Small Aztec Code, Codablock, Code 1, Code 16K, Code 49, CP-Code, DataGlyphs, Data Matrix, Data Strip Code, Dot Code A, hueCode, Intacta.Code, MaxiCode, Mini code, PDF 417, Micro PDF 417, QR Code, Smart Code, Snowflake Code, Supercode and Ultracode.

[0129] Data Matrix is a high density 2-D matrix style bar code symbology that can encode up to 3116 characters from the entire 256 byte ASCII character set. The symbol is built on a square grid arranged with a finder pattern around the perimeter of the bar code symbol. There are two types of Data Matrix symbols each using a different error checking and correction scheme (ECC). The different types of Data Matrix symbols are identified using the terminology "ECC" followed by a number representing the type of error correction that is used by the encoding software. The ECC 200 version of Data Matrix is well suited for use herein.

[0130] MaxiCode is a fixed size matrix style symbology made up of offset rows of hexagonal modules arranged around a unique bulls-eye finder pattern. Each MaxiCode symbol has 884 hexagonal modules arranged in 33 rows with each row containing up to 30 modules. The maximum data capacity for a MaxiCode symbol is 93 Alphanumeric characters or 138 Numeric characters. The United Parcel Service designed the symbology for package tracking applications.

[0131] Aztec Code is a high density 2 dimensional matrix style bar code symbology that can encode up to 3750 characters from the entire 256 byte ASCII character set. The symbol is built on a square grid with a bulls-eye pattern at its center. Data is encoded in a series of "layers" that circle around the bullseye pattern. Each additional layer completely surrounds the previous layer thus causing the symbol to grow in size as more data is encoded yet the symbol remains square. Aztec's primary features include: a wide range of sizes allowing both small and large messages to be encoded, orientation independent scanning and a user selectable error correction mechanism. The smallest element in an Aztec symbol is called a "module" (i.e. a square dot). The module size and the amount of error correction are the only "dimensions" that can be specified for an Aztec symbol and both are user selectable.

[0132] Spread-spectrum barcode systems are suitable for use herein and can read an entire message when a significant fraction of the barcode is occluded or damaged in contrast to localized-data barcodes, are tolerant of overprinting, require no clear zone bordering the barcode and provide data capacities in the range of 100 B-1 kB. They also permit the storage of multiple independent data sets stored in same image, can be read from any "reasonable" viewing angle, and can be read with significant interference (dust, dirt, particles, etc.).

[0133] These codes may be black and white codes, i.e., use only black and white elements. However, some codes may also utilize color elements or gray scale elements which allow the information density encoded in the 2-D symbol to be increased. The use of a color elements or gray scale elements in a symbol may require different types of scanners to read the symbol than are used for symbols encoded only with black and white elements.

[0134] Varying amounts of data may be encoded in a 2-D symbol depending on the format and the capabilities of the reader. As described above, the data may be encrypted. For instance, Code 16K printed at 7.5 mils may be used to encode **208** alphabet characters per square inch or 417 numeric characters per square inch. Data Strip Code may be used to encode 150 to 1000 Bytes of digital data per square inch. PDF417 (portable data format) may be used to encode 1.1 kilobytes of machine readable data in the space of a standard bar-code. Also, PDF417 (Symbol Technologies) may be used to encode ASCII, numeric or binary data. The data densities may vary according encoding format of the data. With maximum error correction in PDF417, data may be correctly read from a symbol with half of the symbol damaged.

[0135] The 2-D bar-codes may be used to encode gaming machine and interaction data, text, graphics, biometric data, sounds and voice records. For instance, fingerprints, scanned signatures and voice authorization records may be encrypted and stored in a 2-D bar-code. The scanned signature and the voice authorization record may be recorded at the gaming machine, encrypted and printed in a 2-D bar-code format on a ticket that is carried by the player. The encoded information on the ticket may be later used to validate/authenticate the printed ticket and the person trying to redeem the ticket.

[0136] In one voice authentication embodiment, prior to issuing a ticket, the player may be asked to speak a short phrase of their choosing or specified by the gaming machine into a microphone located on the gaming machine. The short phrase may or may not be encoded on the ticket in the player's voice. For instance, a digital sound signature may be generated from the message, encrypted and stored on a ticket. Later, to validate the ticket, the encoded information may be read from the ticket and played back to an operator validating the ticket, such via as in an earpiece worn by the operator. The operator may ask the player to repeat the short phrase encoded on the ticket. The operator may use the manner in which the phrase is said, the information contained in the phrase or combinations thereof to validate the ticket. In another embodiment, the short phrase may be repeated into a microphone and a digital sound signature generated from the short phrase may be compared with a digital sound signature of the message originally stored on the ticket.

[0137] In other embodiments, the 2-D bar-code may be used to encode a record in a loyalty program database such as a 1) a player identification number, 2) a social security number, 3) a name, 4) an address, 5) a credit number, 6) a player rating, 7) complimentary (comp.) information, 8) a player preference tracking number and 9) a casino preference tracking number. In general, the 2-D barcodes may be used to encode one of a) loyalty program information, b) biometric information, c) player preferences for games, game features, gaming machine settings, prizes, promotions and food/beverage services, d) promotional information, e) gaming machine configuration settings, f) prize information,

g) cashless transaction information and h) and combinations thereof. Further, equipment calibrations used for maintenance as well as gaming machine settings preferred by the player may be encoded in a 2-D bar-code format.

[0138] The 2-D bar-codes provide a number of advantages. One advantage is that gaming services may be provided to the player when contact with a remote server is unavailable because a record rather than an index may be encoded in the 2-D bar-code. Another advantage is that the PIN code may be eliminated when biometric information is encoded in the 2-D bar-code. For instance, in one embodiment, a player's fingerprint may be encoded in a 2-D symbol. Thus, rather than entering a PIN number, the player simply places their finger on a finger printer reader. Therefore, the player can initiate a secure session without having to remember a PIN number.

[0139] In general, by providing an entire record on the loyalty program instrument (e.g., encoded in a 2-D bar-code format or encoded in an RFID tag), a gaming service, such as a player tracking session, a preferred gaming machine configuration or other customized gaming machine service, that requires a record to be retrieved from a remote server to generate the service on the gaming machine, may be provided by the gaming machine without first contacting the remote server. For example, in a traditional player tracking programs, a remote server is contacted after the player inserts their player tracking card because the player tracking card only stores an index to a record stored on the remote server. Via a communication on the gaming machine, the index number is sent to the remote server to retrieve the player tracking record corresponding to the index number. The player tracking record provides information necessary to implement the player tracking session. With the present invention, the player tracking session may be implemented using the player tracking record stored on the loyalty program instrument without contacting the remote server. After the player tracking session has been completed, the gaming machine may contact the remote server to provide a history of the player tracking session that has been implemented on the gaming machine.

[0140] Bar-code readers include a bar-code scanner and a decoder. The bar-code scanner is the optoelectronic part of the reader which transforms for the optical image of the bar-code into electrical signals. The electrical signal may be converted by a decoder within the reader into ASCII (American Standard Code for Information Interchange). The readers of the present invention are not limited to reading data only encoded in a 1-D bar-code format (there are also a wide variety of 1-D formats). For instance, information on a loyalty program instrument may be encoded in a 1-D bar-code format, a 2-D bar-code format (there are wide variety of 2-D bar-code symbol formats), other symbol formats, alpha-numeric formats and combinations thereof. Therefore, the reader of the present invention, including a scanner and a decoder, may be capable of scanning and decoding information encoded in a wide variety of formats. For instance, on a substrate **900**, a casino's name in an alpha-numeric format, a symbol for a casino, a 1-D bar-code and a 2-D bar-code may all be printed on the same substrate and all of this information in the different formats may be processed by the same reader.

[0141] The bar-code reader may be used to read 1-D bar-codes and 2-D bar-codes using a laser scanner. The laser scanner used in the bar-code reader is one example of a non-physical data interface. The laser in the scanner may be generated using a laser diode. The wavelength of the light used in the scanner may vary from the visible to the infrared spectrum. In some embodiments, the bar-code may be printed in an invisible format. For example, some invisible inks and dyes are fluorescent in the near infrared spectrum and thus may be read with infrared scanner. These symbols are not visible under UV light.

[0142] The scanning rate for the laser scanner may be between 40 and 800 times a second. Since self-scanning laser readers, scan at a high rate, they are able to read poorly printed bar code that may require several scan attempts without the user noticing. Many bar-code readers and symbols formats provide for error correction that allow damaged or misprinted symbols to be read. Typically, laser scanner use coherent light, which limits the amount of beam spreading. This allows the diameter of the beam to remain small enough to resolve wide and narrow bars of the bar-code even when the reading distances vary over the bar-code symbol. This property allows bar-codes printed on curved surfaces to be read. Depending on the symbol width, printing technology and ambient conditions, data may be read from bar-codes in a range of about 2 inches to 30 inches from the reader. These distances may vary depending on the employed technology. For instance, an ArrayTag 2-D bar-code format may be read from a distance as great as 50 meters.

[0143] Another example of a non-physical contact data interface that may be used to read 1-D and 2-D bar-codes in a bar-code reader is a charged coupled device (CCD) scanner. In CCD scanner, the bar-code may be illuminated by a photoflash or by another type of light source. The image of the bar-code is focused on to an array of photodetectors (i.e., CCD). The images of the dark bars of the symbol will fall on some of the photodetectors, while the light spaces fall on other detectors. An electrical signal is applied to the CCD array and the light value at each detector is read. This signal may be processed to determine the information encoded in the symbol. With a bright light, the depth of focus for a CCD array is several inches and generally the symbol must be placed closer to the scanner as compared to a laser scanner. Although, depending on the size of the symbols, the information may be read up to several feet away.

[0144] The density of the symbol that can be read is a function of the number of photodetectors in the CCD array. Instead of a CCD scanner, a CCD video camera may be also be used to read bar-code symbols. The laser and CCD scanners may be operated continuously, may be activated when a sensor detects an object is in the vicinity of the scanner, may be activated in response to a gaming event, such as a player depositing money into a gaming machine and combinations thereof.

[0145] In the present invention, a loyalty program instrument with an RFID tag is another type of device that may be utilized with an input mechanism using a non-physical contact data interface. In **FIG. 8C**, a substrate **900** with an embedded RFID tag **906** is shown. In its simplest form, an RFID tag **906** may comprise a logic device **907** and an antenna **908** without a power supply. When the RFID tag without a power supply is interrogated by a RFID tag reader operating at the right radio frequency, the antenna picks up

a small amount of electromagnetic energy that is used to power logic device **907**. After receiving power, the logic device **907** broadcasts via the antenna **908** data that is stored in the logic device to the RFID tag reader. Additional details regarding RFID tag readers and RFID tags are described with respect to **FIGS. 9A-9C**.

[**0146**] The RFID tags **906** may be of varying sizes. For instance, the logic device **907** may be 1 mm square and ½ mm thick and embedded in a flexible substrate such as paper. The RFID devices may also incorporated into a substrate **900** with an adhesive backing and placed on various objects carried by a gaming machine user at the casino in the manner as was described for the 1-D/2-D bar-codes. RFID devices that may be used with the present invention are produced by companies, such as Texas Instruments (Dallas, Tex.), Hitachi (Japan), Infeon Technologies (Germany). Another type of RFID tag by Samoff (Princeton, N.J.) is as small as 250 micrometers wide. The RFID tag includes photocells, logic, memory for 50 bits and an antenna etched in silicon. The logic device receives power through a burst of laser light that is received by the photocells.

[**0147**] The memory storage capacities of the RFID tags used in the present invention may vary. In one embodiment, the RFID tag may be used to store a number that is an index to record in database like a 1-D bar-code symbol. In another embodiment, the RFID tag may be used to store encrypted biometric data.

[**0148**] In one embodiment of the present invention, a combination of 1-D/2-D bar-codes and RFID tags may be used. In **FIG. 8D**, a substrate **900** including an RFID tag **906**, 1-D bar-code symbol **902** and a 2-D bar-code symbol **904** is shown. The RFID tag **906** may be embedded in a media, such as paper or plastic, and the 1-D/2-D barcodes may be printed on the media. In particular embodiments, the media may be credit card size plastic substrate, a thermal printing media with an embedded RFID tag, any type of printable media with an embedded RFID tag and a printable label with an embedded RFID tag and an adhesive backing. Since the RFID tags may be quite small a plurality of tags may be embedded in the same media. Input mechanisms of the present invention may be designed to read information stored in RFID tags, read bar-codes or read both formats. For instance, a bill validator may be capable of scanning information encoded in the 1-D/2-D bar-code formats printed on a ticket inserted in the bill validator and interrogating an RFID tag embedded in the inserted ticket.

[**0149**] In **FIG. 8D**, the different information formats (i.e., RFID and bar-code) may be stored the same information or different information. For instance, in one embodiment, the 1-D bar-code **902** may store an index to a record while the RFID tag **906** stores the encrypted biometric data that is used to validate the instrument and its carrier. In another embodiment, the RFID tag and a 1-D bar-code may be used to store the same index number and/or encrypted biometric data. Thus, if the RFID tag is damage, the index number may be read from the 1-D bar-code or if the 1-D bar-code is damaged the index number may be read from the RFID tag.

[**0150**] **FIGS. 9A-9C** illustrate RFID tags and RFID tag readers of the present invention. In **FIGS. 9A and 9B**, the use of inductive coupling and propagation coupling to read RFID tags. In **FIG. 9C**, an RFID tag for one embodiment of the present invention is described.

[**0151**] In **FIG. 9A**, a reader antenna **912** connected to a reader/programmer **910** is used to communicate with an RFID tag **908**, including a logic device **907** and antenna **908**, which is located on a substrate **900**. The RFID tag **906** is a passive RFID tag and does not include a power supply. Although, as described with respect to **FIG. 10C**, active RFID tags with a power supply may be used in the present invention. The logic device may be a silicon microprocessor, which may vary in size. The antenna is typically a metal coil made of a conductive metal such as copper or aluminum.

[**0152**] Power is supplied to the RFID tag **906** via the air interface **914** through inductive coupling **915** to the metal coil which is the tag's antenna **908**. Inductive RFID tags are powered by a magnetic field generated by the reader. The antenna **908** picks up magnetic energy. The magnetic energy is then used to power the logic device **907**. The logic device **907** modulates the magnetic field in order to retrieve and transmit data back to the reader **910**. The data transmitted back to the reader then may be communicated to another gaming device, such as but not limited to, a logic device on a player tracking unit, a master gaming controller on a gaming machine and a remote server.

[**0153**] An RFID tag using capacitive coupling or propagation coupling **916** is shown in **FIG. 9B**. In a typical RFID tag using propagation coupling, the logic device **907** is a silicon microprocessor. The RFIG tag's antenna **908** is generated using a conductive ink. By printing the antenna structure on a media, such as paper, using the conductive ink, the antenna may be formed. Carbon-ink electrodes on the paper, which may be integrated into an adhesive label, may be used to connect the antenna to the microprocessor. The capacitively coupled RFID tag **906** is powered by electric fields generated by the reader antenna **912** attached to the reader/programmer **910**.

[**0154**] In another embodiment of the present invention, the RFID tag **906** may include one or more photocells. The photocells may be used to power the RFID tag by shining light energy, such as a generated by a laser, onto the photocell. The photocell then transmits the energy received from the laser to the logic device.

[**0155**] Typically, the RFID tags may use three frequency ranges, low, medium and high to communicate information. Low frequency range is from 100-500 Khz. The medium frequency range is from 10-15 Mhz and the high frequency range is from 850-850 Mhz and 2.4 to 5.8 GHz. In general, the reading speed for data and the reading range increases as the frequency used with the RFID tag increases. The range of the RFID system is a function of the power available at the reader/programmer **910** and the power available by the RFID tag to respond and the environmental conditions in which the RFID tag is used, such as a casino environment.

[**0156**] The function of the reader portion of the reader/programmer **910** is to provide a means of communicating with the tags and facilitating data transfer. The reader may include a logic device designed to perform signal conditioning and parity error checking and correction. RFID readers, such as **910**, may probe simultaneously a plurality of RFID tags. Once a signal from an RFID tag has been correctly received and decoded, algorithms may be applied to decide whether the signal is a repeat transmission. When the reader **910** determines the transmission has been repeated, the reader may instruct the RFID tag to stop transmitting. This

process, often referred to as "Command Response Protocol," is used to circumvent the problem of reading multiple tags in a short period of time during batch processing. In another approach, the reader **910** may look for RFID tags with specific identities and interrogate them in turn.

[**0157**] Batch processing may be applied when a plurality of RFID tags are within the range of the RFID reader. For example, batch processing may be applied when a player is carrying a plurality of instruments where each instrument may include one or more RFID tags. In this example, the reader may be able to interrogate each of the RFID tags to determine the function of each instrument carried by the player. In one embodiment, when the player is carrying a plurality of RFID tags where a portion of the RFID tags encode index numbers corresponding to different player tracking programs, then the RFID reader located on the gaming machine may be able to read each of the index numbers stored on the tags and determine if any of the read index numbers are valid for a player tracking program implemented on the gaming machine. The interrogation of the different RFID tags by the reader may be initiated when a game play session is initiated on the gaming machine.

[**0158**] In one embodiment, the player may carry portable gaming instruments with RFID tags issued for a number of purposes, such as player tracking programs, anonymous loyalty instruments, cashless instruments, promotional credits, coupons and comps. These RFID tags may have been issued at different locations and at different times. Thus, the RFID tags may store information regarding but not limited to, a purpose, where they were issued, the time they were issued and when they expire. When a game play session is initiated on the gaming machine by a player or in response to some other game event, the reader may interrogate the RFID tags that are within range of the reader such as the RFID tags carried by the player initiating the game play session. With this information, the gaming machine may be able to determine 1) what types of tags the player is carrying, 2) what is their purpose and 3) where the player has been. The gaming machine may also be able to determine where the RFID tag was issued, when the instrument with the RFID tag was issued and whether the instrument has an expiration date. This process may be carried out at other locations frequented by the player. For instance, RFID readers may be located at cashier stations, ATM machines, casino kiosk, hotel registration desks as well as gaming machines.

[**0159**] Using information read from RFID tags carried by the player, a gaming device, such as a gaming machine, or a casino employee that has access to the read information, may send targeted information to the player. For instance, if the player is carrying a coupon for promotional credits, the gaming machine may remind the player of the coupon and encourage them to use it. In another embodiment, if the gaming machine determines the player is carrying cashless instruments with a cash value above a certain threshold, then the gaming machine may offer the player promotional offers to entice them to spend it. The promotional offer may be displayed on a display screen on the gaming machine or may be made via a printed ticket issued by the gaming machine. In another embodiment, based upon information read from the RFID tags, such as the value of cashless instruments carried by the player, the gaming machine may notify an attendant to provide the player special service.

[**0160**] In another embodiment, if the gaming machine determines that any of the instruments carried by the player are about to expire, the gaming machine may generate and display a notification message. For instance, cashless instruments are only redeemable for a limited time period. Thus, if the gaming machine determines that a cashless instrument is about to expire, the gaming machine may generate a notification message with this information and display the message. In another example, promotions, such as promotional credits, may only be valid for a limited time period. Therefore, if the gaming machine determines the promotion is about to end, then the gaming machine may generate a notification message with this information and display the message.

[**0161**] A person carrying the RFID tags may not know what information is stored on the tags or in what instruments the tags are located. Further, the information on the RFID tags may be gathered without any active participation by a person carrying the RFID tag, i.e., the information gathering process is passive in regards to participation by the player. With an RFID tag, the player may only have to be in a location within the range of the RFID reader to have the information on all the RFID tags they are carrying to be read.

[**0162**] Returning to **FIGS. 9A and 9B**, the reader/programmer **910** may be used to store information to an RFID tag **906**. In one embodiment, the programming process may involve a write-once read many (WORM) RFID tag. For this type of tag, the information programming may be carried out when the instrument with the RFID tag is issued. For example, a printable media with an embedded RFID tag may be programmed by the reader/programmer **910** during the process of generating a printed ticket with the RFID tag. In another embodiment, the embedded RFID tag may be pre-programmed and the information stored on RFID tag may only be read when the printed ticket is issued. The data read from the RFID tag may be stored in a database located on one of the gaming machine, a remote server and combinations thereof. As described with respect to **FIG. 9C**, more complicated RFID tags may be read/write capable, i.e., the memory on the tags may be written to and over written a plurality of times.

[**0163**] In one embodiment of the present invention, a portion or all of the electronic circuitry for an RFID tag used in an instrument may be generated by printing the circuitry directly to a printable media. The printing process may be carried out by a printer located in a gaming device, such as a gaming machine as part of the process of issuing the instrument from the gaming machine. For example, circuitry may be printed on a cashless instrument when the cashless instrument is issued from the gaming machine. The circuitry may be used to store information about the cashless instrument, such as a value of the ticket.

[**0164**] In one embodiment, the printed circuitry may be memory circuitry used to store information used on the RFID tag **906**. The printed circuitry may be generated when the instrument is issued i.e., "on the fly." As an example, the memory circuitry may be generated using conductive ink transferred to a suitable media, such as paper, using an inkjet printer. Paper is one example of a flexible media that may be used with the present invention. In another example, a thermal printer may be used to activate electronic pathways on a thermally activated media to create the electronic

circuitry. The memory circuitry printed on the media used for the instrument may be capable of storing a number of bits of information, such as an index number for a loyalty program instrument. The memory circuitry may be connected to an RFID microprocessor embedded in the printable media, such as the logic device **907**. Therefore, the stored information in the memory circuitry may be later read by an RFID reader **910**.

[**0165**] The printers used in the present invention may also be capable of printing information, such as encrypted biometric data, in other formats, such as 1-D/2-D bar-codes and alpha-numeric symbols, as described with respect to **FIGS. 9A-9D**. The printer may be one of a laser printer, inkjet printer and thermal contact printer. Further, the printer may be capable of printing information, such as a bar-code symbols, in an invisible format.

[**0166**] **FIG. 9C** shows an RFID tag **906** according to one embodiment of the present invention. The RFID tags of the present invention may be passive or active tags. Active tags are powered by an internal battery and are typically read/write devices. Passive tags operate without an internal battery source, deriving the power to operate from the field generated by the reader.

[**0167**] The RFID tag memory may comprise one or more of ROM **924**, Non-volatile memory **922** (e.g., EEPROM or flash memory) and RAM **926**. The ROM memory may be used to accommodate security data and the RFID tag operating system instructions. The operating system instructions may be used by the logic device **920** to perform internal functions, such as response delay timing, data flow control, encryption/decryption and power supply switching. The RAM memory **926** may be used for temporary data storage during interrogation and response between the RFID tag **906** and the reader **910**.

[**0168**] The NV-RAM is used to store RFID tag data. NV-RAM is used to ensure the RFID tag data is not lost when the device is in its quiescent or power-saving sleep state. The NV-RAM used in the present invention may vary in storage capacity. The NV-RAM may be capable of storing a number of bits of information used to store a number that is an index to a record in a database or may be large enough to store a portable data file which may be a record in a database. As described with respect to **FIGS. 8A-8D**, gaming services may be provided using the record stored in a portable data file without contacting a remote server.

[**0169**] The data transfer circuitry **926** may be used as a data buffer to temporarily hold incoming data following demodulation and outgoing data for modulation and may be used to interface with the reader antenna. The data transfer circuitry **926** may also be used to direct and accommodate the interrogation field energy for powering purposes and triggering of the transponder response. Circuitry (not shown) may also be provided to allow for programming of the RFID tag **906**. Power supply **930** is optional. Active tags require a power supply while passive tags derive power remote sources such as the from field energy provided by the reader antenna or a laser light source used to transfer energy to the tag via a photocell.

[**0170**] **FIGS. 10A-10B** show simplified illustrations of input mechanisms with a non-physical contact data interface of the present invention. The input mechanisms are provided for illustrative purposes and the present invention is not limited to these two designs. The input mechanisms may be mounted directly to a gaming machine or may be located within a player tracking device mounted to the gaming machine.

[**0171**] In **FIG. 10A**, an input mechanism **950** with an interior non-physical contact data interface **952** is shown. The non-physical contact data interface **952** may be one of a bar-code scanner, a RFID tag reader and combinations thereof. The input mechanism **950** comprises a rectangular housing **955**. The rectangular housing has an exterior surface **959** that is designed to form an exterior surface of the gaming machine. Thus, most of the housing **955** is located within the interior of the gaming machine. The exterior surface **959** may be located on a horizontal surface, a vertical surface or on a surface with an inclination between horizontal and vertical located on a gaming machine.

[**0172**] The housing **955** is designed for accepting a relatively planar substrate **900**, such as a ticket or a plastic card. The substrate **900** may include 1-D bar-codes **902**, 2-D bar-codes **904**, RFID tags (not shown) and combinations thereof. The exterior surface **959** includes a slot **956**. The slot is designed to receive the substrate **900**. Guides **958** may be located in the interior of the housing. The guides **958** may be used to constrain the orientation of the substrate **900** after it is inserted in the slot **956**. The top of the non-physical contact data interface **952** may be located at a distance below the guides **958**. After the substrate **900** is inserted in the slot, information on the substrate may be read by the non-physical contact data interface **952**.

[**0173**] In **FIG. 10B**, an input mechanism **951** with an exterior mounted non-physical contact data interface **952**. The top of the non-physical contact data interface **952** is surrounded by an exterior surface **960**. The non-physical contact data interface **952** may be mounted below a translucent material. The non-physical contact data interface **952** and the exterior surface by connected to a housing (not shown) extending below the exterior surface **960**. The exterior surface **959** may be located on a horizontal surface, a vertical surface or on a surface with an inclination between horizontal and vertical located on the gaming machine.

[**0174**] The non-physical contact data interface may read information from the substrate **900** when it is moved through or within an active volume **970** above the reader **952**. The shape and size of the substrate **900** is not limited to a rectangular shape shown in the figure. Information may be read from the substrate **900** at one of a plurality of distances between the substrate **900** and the reader **952** and with one of a plurality of orientations between the substrate **900** and the reader. For example, when bar-code data is read from the substrate **900** using a bar-code reader, the side of the substrate **900** facing the top of the reader **952** may be parallel to the top of the reader or inclined at one of a plurality relative to the top of the reader. When RFID data is read from the substrate **900**, in some embodiments, the RFID data may be read independently of the orientation of the substrate relative to the reader **952**. In other embodiments, when the RFID tag receives power from the reader **952** via light energy received from photocells on the tag, the substrate may have to be oriented in one of a plurality of orientations that allows the photocells to receive light energy from the reader **952**.

[0175] During the read process, the substrate **900** may be stationary or at a time varying position relative to the reader **952**. Further, the orientation of the substrate relative to the reader **952** during the read process may be fixed or may be time varying during the read process. For example, for a substrate **900** with a 2-D bar-code, the substrate **900** may be moving and changing orientation in the volume above the reader **952** during reading as the reader **952** scans the 2-D bar-code on the substrate a plurality of times.

[0176] The input mechanism **951** may optionally include guides **962** for aligning the substrate **900** in a preferred orientation. By placing the substrate **900** within the guides, the substrate **900** may be aligned relative to the reader **952**. If the substrate **900** is placed above the guides, but somewhat aligned with the guides or the substrate **900** is smaller than the guides, the substrate may still be sufficiently aligned. In one embodiment, the guides **962** may include slots for inserting the substrate **900**. An advantage of using a "free" read where the substrate **900** is simply placed within the active volume **970** for the read and then removed that the substrate **900** can't be left in the device like a magnetic striped card can be left in a card slot. Therefore, this design may reduce the probability of the substrate **900** being lost.

[0177] The input mechanisms **950** and **951** may include a loyalty program session status interface comprising one of a status light **954**, a sound projection device **955** and combinations thereof. The light may be located at any location on the exterior surfaces **959** and **960**. For input mechanism **950**, the light may be a strip with one or more lighting elements and may surround the slot. For input mechanism, the light may be a strip with one or more lighting elements. Further, the guides **962** may be translucent and back-lit. The sound device **955** may be located on the exterior surfaces **959** and **960**. The sound device **955** and status light **954** may be located or at other locations on the gaming machine and are not limited to exterior surfaces **959** and **960**. In general, the sound device **955** and status light **954** may be used to provide information regarding the functioning of the input mechanisms in **950** and **951** in any application for which they are used.

[0178] Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, while the gaming machines of this invention have been depicted as having top box mounted on top of the main gaming machine cabinet, the use of gaming devices in accordance with this invention is not so limited. For example, gaming machine may be provided without a top box.

What is claimed is:

1. A method of providing a portable gaming instrument for use with gaming machines, the method comprising:

assigning a value to the portable gaming instrument;

obtaining biometric data for a person that has interacted with a gaming machine;

encrypting the biometric data representative to produce encrypted biometric data; and

storing the value and the encrypted biometric data on the portable gaming instrument.

2. The method of claim 1 further comprising receiving a request from a person to produce the portable gaming device.

3. The method of claim 1 wherein the biometric data is obtained from biometric information that is obtained from the person using a biometric reader associated with the gaming machine.

4. The method of claim 1 wherein obtaining the biometric data includes accessing the biometric data from a database according to a known identity of the person.

5. The method of claim 4 wherein obtaining the identity of the person is known from a player tracking card that the person has used with the gaming machine.

6. The method of claim 1 wherein the biometric data includes fingerprint data.

7. The method of claim 1 wherein the portable gaming instrument includes a printed ticket or a printed surface.

8. The method of claim 7 wherein the encrypted biometric data is printed in black and white on the portable gaming instrument.

9. The method of claim 7 wherein the encrypted biometric data is printed in gray scale on the portable gaming instrument.

10. The method of claim 7 wherein the encrypted biometric data is printed in two dimensions.

11. The method of claim 7 wherein the encrypted biometric data is redundantly printed on the portable gaming instrument such multiple portions of the ticket each store the encrypted biometric data.

12. The method of claim 7 wherein the encrypted biometric data is hidden within other information printed on the ticket.

13. The method of claim 1 wherein the value includes one of: cash value, player tracking points, and loyalty program points.

14. A method of redeeming value on a portable gaming instrument, the method comprising:

receiving a request to redeem the value on the portable gaming instrument;

decrypting encrypted biometric data stored on the portable gaming instrument, wherein the encrypted biometric data includes biometric data used to produce the encrypted biometric data and identifies a person who received the portable gaming instrument;

obtaining biometric data for a person trying to redeem the value on the portable gaming instrument;

comparing a) the biometric data for the person trying to redeem the value on the portable gaming instrument with b) the biometric data obtained from the portable gaming instrument; and

awarding the value on the portable gaming instrument to the person trying to redeem the value on the portable gaming instrument when the biometric data for the person trying to redeem the value on the portable gaming instrument matches the biometric data that was encrypted and stored on the portable gaming instrument.

15. The method of claim 14 wherein obtaining the biometric data for the person includes receiving biometric information from the person.

16. The method of claim 15 wherein obtaining the biometric data for the person includes receiving a fingerprint from the person.

17. The method of claim 16 wherein the fingerprint is received at a gaming machine.

18. The method of claim 16 wherein the fingerprint is received at a payout station in a casino.

19. The method of claim 14 wherein obtaining the biometric data for the person includes communicating with a server that stores the biometric data for the person.

20. The method of claim 19 wherein obtaining the biometric data includes accessing the biometric data from a database according to a known identity of the person.

21. The method of claim 20 wherein the person is identified using person tracking information.

22. The method of claim 14 wherein the portable gaming instrument includes a printed ticket or a printed surface.

23. The method of claim 22 wherein the encrypted biometric data is printed in gray scale on the portable gaming instrument.

24. The method of claim 22 wherein the encrypted biometric data is printed in two dimensions.

25. The method of claim 22 wherein the encrypted biometric data is redundantly printed on the portable gaming instrument such multiple portions of the ticket each store the encrypted biometric data.

26. The method of claim 14 wherein the value includes one of: cash value, player tracking points, and loyalty program points.

27. A gaming machine comprising:

an external cabinet defining an interior region of the gaming machine;

a display device adapted to display game play information, the display device being located within or about the external cabinet;

a biometric reader located within or about the external cabinet and configured to read biometric information from a person;

a portable gaming instrument reader, located within or about the external cabinet, configured to read encrypted biometric data stored on a portable gaming instrument, wherein the encrypted biometric data includes biometric data used to produce the encrypted biometric data and identifies a person who received the portable gaming instrument; and

a gaming machine controller designed or configured to i) provide a game play sequence comprising a presentation of one or more games of chance on the gaming machine, ii) decrypt the encrypted biometric data stored on a portable gaming instrument, iii) compare a) the biometric data for the person with b) the biometric data obtained from the portable gaming instrument, and iv) award the value on the portable gaming instrument to the person when the biometric information for the person matches the biometric information that was encrypted and stored on the portable gaming instrument.

28. The gaming machine of claim 27 further including a network communications link that is configured to communicate with a server that stores biometric data for a plurality of people to obtain the biometric data for the person.

29. The gaming machine of claim 28 wherein the person is identified using personal identification information stored on the portable gaming instrument.

30. The gaming machine of claim 27 wherein the biometric reader includes a fingerprint reader configured to read a fingerprint from the person.

31. The gaming machine of claim 27 wherein the value includes one of: cash value, player tracking points, and loyalty program points.

32. The gaming machine of claim 27 further including a printer configured to print the encrypted biometric data on the portable gaming instrument.

33. The gaming machine of claim 32 wherein the encrypted biometric data is printed on the portable gaming instrument using one of: a 1-D bar-code, a 2-D bar-code, a symbol.

34. The gaming machine of claim 1 wherein the portable gaming instrument is selected from the group consisting of an RFID tag, a portable wireless device, a cell phone, a portable computation device and a portable communication device.

35. The gaming machine of claim 27 wherein the portable gaming instrument reader is a bar-code reader.

36. A gaming system for providing portable gaming instruments, said gaming system comprising:

a plurality of portable gaming instruments, each portable gaming instrument including encrypted biometric data that identifies a person that received the portable gaming instrument;

a plurality of gaming machines, each gaming machine including

a biometric reader located within or about the external cabinet and configured to read biometric information from a person,

a portable gaming instrument reader configured to read the encrypted biometric data stored on a portable gaming instrument,

a network interface that permits communication across a network; and

a server including a network interface that permits communication across the network and configured to distribute a private key to each of the gaming machines.

37. The gaming system of claim 36 wherein the server is configured to assign a private key to each of the gaming machines.

38. The gaming system of claim 36 wherein the server is configured to assign a private key to each of the portable gaming instruments.

39. The gaming system of claim 36 wherein the biometric reader includes a fingerprint reader configured to read a fingerprint from the person.

40. The gaming system of claim 36 wherein the value includes one of: cash value, player tracking points, and loyalty program points.

41. The gaming system of claim 36 further including a printer configured to print the encrypted biometric data on the portable gaming instrument.

42. The gaming system of claim 41 wherein the encrypted biometric data is printed on the portable gaming instrument using one of: a 1-D bar-code, a 2-D bar-code, a symbol.

43. The gaming system of claim 36 wherein the portable gaming instrument is selected from the group consisting of an RFID tag, a portable wireless device, a cell phone, a portable computation device and a portable communication device.

44. The gaming system of claim 36 wherein the portable gaming instrument reader is a bar-code reader.

* * * * *