A device and method is provided to create an anonymous account to play a wager-based game of chance on a mobile gaming device comprises obtaining a cashless ticket voucher having a unique identifier, the cashless ticket voucher having a monetary value, inputting the unique identifier into the mobile gaming device to expend the monetary value of the cashless ticket voucher, validating the unique identifier, and generating a game of chance on the mobile gaming device if the unique identifier is validated.
FIG. 2

VALIDATOR  I/O DEVICES  CPU  LCD  MEMORY  COMM INT

MASS STORAGE DEVICE  SPEAKER  KEYPAD  CARD READER  NETWORK DEVICE

FIG. 3

PGD  RELAY  TRANSCEIVER

PGD INTERFACE  VALIDATION SERVER  FINANCIAL SERVER  GAME SERVER

RESERVATION SERVER  INTERNET GATEWAY
Begin

Form a cashless ticket voucher on a first gaming machine 400

Input the ticket voucher unique identifier 402

 Transmit the unique identifier to a validation server 404

Is the unique identifier validated? 406

Yes

Generate a game of chance on the second gaming machine 408

No

End
INSTANT ANONYMOUS ACCOUNT CREATION

FIELD OF THE INVENTION

[0001] The present invention relates to portable gaming devices and methods, and more particularly, the present invention relates to creating anonymous accounts for playing wager-based games on portable gaming devices.

BACKGROUND OF THE INVENTION

[0002] Gaming is an increasingly popular industry, with casinos and other gaming establishments continually seeking new and exciting ways to present games for play. Many games are generally presented on large free-standing gaming devices, such as the well known slot machines, video poker machines and the like. Other games can be presented at something other than a gaming device, such as the table games of craps, blackjack and roulette. In addition, games such as keno and bingo may be played in areas specially configured to present the game to players (e.g., at areas where personnel pick up keno cards and called numbers are displayed on large displays).

[0003] Such wager-based games allow the casino customers to place bets or wagers that result in winnings if the wager is successful, or losses if the wager is unsuccessful. A substantial disadvantage to the way such games are currently presented is that a player may participate in a particular game only at certain specified locations and/or on specific gaming machines or tables. For example, in order to play video poker or a particular slots game, such as “Red White and Blue,” a player may be required to travel through a large hotel and/or casino to a specific gaming area where an actual video poker or “Red White and Blue” gaming machine is located.

[0004] In addition, electronic gaming machines and gaming systems often employ cashless instruments for ease of paying out winnings to users, which can involve the use of ticket printers and other associated hardware and software components. Such cashless instruments can include, for example, paper tickets used in the EZ Pay™ system by IGT of Reno, Nev., among others. Of course, other suitable items or devices can be used as such cashless instruments as well, and it is understood that the present invention is directed to all such items. Paper cashless tickets in particular are printed by a printer at the gaming machine upon the request of a player at the completion of a game or gaming session, and signify a cash amount owed to the player, a portion of which might represent cash winnings owed to the player. Such paper tickets typically include appropriate currency or credit amounts, as well as various identification features printed on them, which can include a unique identifier or code.

[0005] It will be readily understood that such a unique identifier or code can be called a variety of names, such as an identification, verification, and/or authentication number or code, among others, and that any such term or terms can be used where the basic function is to identify a specific cashless instrument that has been issued at a specific time and location. Such a unique identifier or code on a printed ticket is typically used in association with a matching confirmation number or code that is stored on the system, such that a match can be made with a recorded and outstanding number when a ticket is offered or received, whereby the ticket can be determined as valid and thus be accepted. For purposes of consistency within the present disclosure, the term “unique identification” (or code) will be used with respect to printed tickets or other cashless instruments, while the term “confirmation number” (or code) will be used to denote those numbers or codes that are stored on a system.

[0006] Casinos and other gaming operators generally desire to provide to their customers greater accessibility to gaming devices and the opportunity to play games such as through the use of a personal gaming device (PGD). However, it is inconvenient and cumbersome to add additional funds to the PGD. Players typically must bring the PGD to a cashier and give the cashier cash prior to being able to play wager based games on the PGD. Players do not have the option to simply insert additional funds or the cashless tickets directly into the PGD similar to fixed gaming machines using a bill/ticket acceptor. There is no equivalent bill/ticket acceptor that is small enough to be used with a PGD. Even a simple scanner may add too much size and cost to a PGD.

SUMMARY OF THE INVENTION

[0007] A device and method is provided to create an anonymous account to play a wager-based game of chance on a mobile gaming device comprises obtaining a cashless ticket voucher having a unique identifier, the cashless ticket voucher having a monetary value, inputting the unique identifier into the mobile gaming device to expend the monetary value of the cashless ticket voucher, validating the unique identifier, and generating a game of chance on the mobile gaming device if the unique identifier is validated.

[0008] In another embodiment, a method for creating an anonymous account to play a game of chance on a mobile gaming device comprises obtaining a cashless ticket voucher having a unique identifier, the cashless ticket voucher having a monetary value, inputting the unique identifier into the mobile gaming device to expend the monetary value of the cashless ticket voucher, validating the unique identifier, and generating a game of chance on the mobile gaming device if the unique identifier is validated.

[0009] The portable gaming device to play at least one wager-based game may have a communication interface adapted to communicate with a remote gaming server, a display, an input mechanism to receive a unique identifier of a cashless ticket voucher, a controller operatively coupled to the display, communication interface, and the input mechanism, and a validator operatively coupled to the controller to transmit the unique identifier to the remote gaming server for validation, the validator to receive an approval or a rejection message from the remote gaming server. The controller is programmed to cause the display to generate a game display relating to the at least one wager-based game and display an outcome of the at least one wager-based game if an approval message is received by the validator.

[0010] The validation server may have an interface to receive a cashless ticket voucher unique identifier, and a confirmation number database having a list of confirmation numbers of distributed cashless ticket vouchers wherein the unique identifier is matched to a confirmation number, and wherein an approval message is transmitted to a remote gaming server if a match is found.

[0011] A mobile gaming network may have a validation server, comprising an interface to receive a cashless ticket voucher unique identifier, and a confirmation number data-
base having a list of confirmation numbers of distributed cashless ticket vouchers, wherein the unique identifier is matched to a confirmation number. The network may also have at least one portable gaming device to play at least one wager-based game, comprising a communication interface adapted to communicate with a remote gaming server, a display, an input mechanism to receive the unique identifier, a controller operatively coupled to the display, communication interface, and the input mechanism, and a validator operatively coupled to the controller to transmit the unique identifier to the remote gaming server for validation, the validator to receive an approval or a rejection message from the remote gaming server wherein an approval message is relayed from the validation server to the remote gaming server if a match is found, and wherein the controller is programmed to cause the display to generate a game display relating to the at least one wager-based game and display an outcome of the at least one wager-based game if an approval message is received by the validator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments and, together with the detailed description, serve to explain the principles and implementations of the invention.

[0013] In the drawings:

[0014] FIG. 1 is a perspective view of an exemplary PGD in accordance with an embodiment of the invention.

[0015] FIG. 2 is a block diagram of a component arrangement of the PGD illustrated in FIG. 1.

[0016] FIG. 3 is a schematic of an exemplary gaming system including a PGD in accordance with the invention.

[0017] FIG. 4 is a block diagram illustrating a method for creating an anonymous account to play a wager-based game of chance.

[0018] FIG. 5 is a diagram illustrating an exemplary gaming machine in accordance with an embodiment of the invention.

[0019] FIG. 6 is a block diagram illustrating an exemplary network topology in accordance with an embodiment of the invention.

[0020] FIG. 7 is a block diagram illustrating a simplified communication topology in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0021] Embodiments are described herein in the context of an instant anonymous account creation. Those of ordinary skill in the art will realize that the following detailed description is illustrative only and is not intended to be in any way limiting. Other embodiments will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0022] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer’s specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0023] In general, the present invention is directed to creating an anonymous account to play a wager-based game of chance on an individual or mobile gaming unit such as a PGD. The use of a cashless ticket voucher does not require a player to input personal information thereby remaining anonymous. The ability to use cashless ticket vouchers with a mobile gaming unit is also addressed.

[0024] Personal Gaming Device

The individual gaming unit may be a PGD that is adapted to present a wager-based game for play by a player. An example is described in co-pending patent application Ser. No. 11/155,702, filed Jun. 16, 2005, entitled “Virtual Leash For Personal Gaming Device” and co-pending patent application Ser. No. 10/672,307, filed Sep. 26, 2003, entitled “Personal Gaming Device and Method Of Presenting a Game” which are incorporated herein in their entirety for all purposes. FIG. 1 illustrates an exemplary PGD, generally numbered 20, in accordance with one embodiment of the invention. In general, the PGD 20 includes a body or housing 22. The body 22 may be constructed from a wide variety of materials and in a wide variety of shapes. In one embodiment, the body 22 is constructed from one or more molded polypropylene or other plastic components. The body 22 may be constructed of metal or a wide variety of other materials. As illustrated, the body 22 is generally rectangular in shape, having a front side or face 24, a rear side or face (not visible), a top end 26, a bottom end 28, a first side 30 and a second side 32. Preferably, the body 22 defines an enclosed interior space (not shown) in which a variety of components are located.

[0025] In a preferred embodiment, the PGD 20 is adapted to present video and sound game data to a player. As illustrated, the PGD 20 includes a display 34. The display is located in the front face 24 of the body 22, thus facing upwardly towards a player. In a preferred embodiment, the display 34 comprises a liquid crystal display (“LCD”), and in particular, an LCD permitting touch-screen input. It will be appreciated that other types of displays may be provided. PGD 20 also includes a sound generating device in the form of at least one speaker 36. In one embodiment, the speaker 36 is positioned beneath a top or cover portion of the body 22 having one or more perforations or apertures therein through which the sound may readily travel. As illustrated, the speaker 36 is located near the bottom end 28 of the body 22, generally opposite the display 34. It will be appreciated that the speaker 36 or additional speakers may be provided in a wide variety of locations, such as at one or both sides 30, 32 of the body 22.

[0026] In a preferred embodiment, the PGD 20 is adapted to send and/or receive data from another device. As such, the PGD 20 includes one or more data input and/or output devices or interfaces. In one embodiment, the PGD 20 includes an RS-232 data port 38 for transmitting and accepting data, such as through a cable extending between the PGD 20 and another device, such as a computer. In one embodiment, the PGD 20 includes a USB data port 40 for
transmitting and accepting data, also through a cable. In one embodiment, the PGD 20 includes an infrared data transmitter/receiver 42 for transmitting information in wireless, infrared light form. In a preferred embodiment, the PGD 20 includes another wireless communication device 44, such as a wireless communication device/interface operating at radio frequency, such as in accordance with the IEEE-802.11 or the Bluetooth™ standard.

[0027] Preferably, a player is permitted to provide input to the PGD 20, such as for playing a game. As stated above, one means of input may be through the display 34. The display 34 may also be arranged to accept input via a touch screen, stylus or other device. In one embodiment, the PGD 20 includes a keypad 46. In one or more embodiments, the keypad 46 is a sealed keypad having one or more keys or buttons which may be activated by a player, such as by depressing the button with their finger. The PGD 20 can include a microphone 48 arranged to accept voice input from a player. Other input devices may alternatively be provided or be provided in addition to those input devices described. For example, a player may be permitted to provide input through a joystick (not shown). The joystick may comprise a control element associated directly with the body 22 of the PGD 20. Alternatively, the joystick may be separate from the PGD 20, and then be placed in communication therewith, such as by plugging in the joystick to a data port of PGD 20. A smart card reader, optical reader, memory card slot, or other input device may be provided for reading information from another element, such as a card, magnetic stripe, flash memory cards, ticket or the like. For example, in some embodiments of the invention PGD 20 includes a scanner for scanning a cashless ticket voucher. Some such embodiments are made for use with cashless ticket vouchers having a light-sensitive coating or the like; these embodiments may illuminate such a cashless ticket voucher with light of a sufficient intensity (and/or within a proper frequency range) to darken and void the cashless ticket voucher. PGD 20 may also include a keyboard or mouse.

[0028] In one embodiment, the PGD 20 includes an image collection device 41, such as a camera. The image collection device 41 may be used, for example, to capture the image of a user or player of the PGD 20. This image information may be used for security or authentication purposes, as set forth in greater detail below. The PGD 20 may also include a biometric sensor or device, such as a fingerprint scanner 49. In one embodiment, as illustrated, the fingerprint scanner 49 may be located behind or beneath a user input button, such as a “spin” or “draw” button. In this manner, a player’s fingerprint may be obtained without the user or player having to consciously participate. As described below, a player’s scanned fingerprint information may be used for authentication purposes. The biometric sensor may be a fingerprint imager, a retina print imager, a voice pattern imager, a facial component imager, handwriting sensor, and other similar devices to recognize and identify the player. The biometric sensor offers a reliable and inexpensive way to authenticate the identity of a player, which is more secure than personal identification numbers (PINs) or passwords, which are subject to being compromised or forgotten.

[0029] The PGD 20 may include a card reader 50. As illustrated, the card reader 50 is located on the side 30 of the body 22 of the PGD 20. In a preferred embodiment, the card reader 50 comprises a magnetic stripe reader for reading information from a magnetic stripe of a card. The card reader may also be adapted to write or store data to a smart card or portable memory module.

[0030] As illustrated, the card reader 50 includes a slot that is positioned in the side 30 of the PGD 20. The PGD 20 may be battery-powered, such as with a rechargeable battery pack. An ON/OFF button 47 may be provided for controlling the power to the PGD 20. The PGD 20 may be docked at or otherwise associated with a free-standing gaming machine or other gaming device. At such times that the PGD 20 is docked, the internal battery of the device can be recharged for later use in an undocked or “remote” mode, as will be readily appreciated. Appropriate detection provisions, warnings and safeguards for a low battery status in PGD 20 while in such a remote mode can also be provided.

[0031] Preferably, PGD 20 includes control means for controlling the operation of the device, including accepting input and providing output. One embodiment of such a control means is illustrated in FIG. 2, a block diagram of an exemplary component arrangement of the PGD illustrated in FIG. 1. As illustrated, PGD 20 preferably includes a computing environment serving as the control means. The computing environment includes a central processing unit 52. The central processing unit 52 preferably comprises a microprocessor. The central processing unit 52 is associated with a bi-directional system bus 54. The system bus 54 may contain, address lines for addressing a video memory or main memory. In addition, the system bus 54 includes a data bus for transferring data between and among components associated with the bus 54. Alternatively, multiplex data/address lines may be used instead of separate data and address lines.

[0032] The display 34 is coupled to the bus 54. In one embodiment, a video memory (not shown) is provided in association with the bus 54. The video memory may be dual-ported video random access memory. The video memory is preferably coupled to and arranged to drive the LCD display 34. Of course, the video memory might be coupled to a cathode ray tube (CRT) or other suitable display device. A memory 56 is associated with the system bus 54. In one embodiment, the memory 56 comprises dynamic random access memory (“DRAM”), synchronous DRAM or other forms of random access memory. The memory 56 may have other forms as well, such as electronically erasable programmable read-only memory (“EEPROM”). Preferably, the memory 56 is of the type that permits data to be written thereto and read therefrom. A mass storage device 58 is preferably also accessible via the bus 54. The mass storage device 58 may be of the read-only type (such as a CD or DVD optical drive) or may be of the read-and-write variety such as flash memory, compact flash, or CD/DVD-ROM drives.

[0033] A validator 80 may also be coupled to the bus 54. The validator 80 may send the unique identifier received by the central processing unit 52 to the remote gaming server to be validated. If the unique identifier is validated, as further described below with reference to the validation server, the validator may receive an approved message. If the unique identifier is not validated, a rejected message may be received. As such, the validator 80 emulates or acts as the bill or ticket validator/acceptor for the PGD.

[0034] As illustrated, the variety of input and output devices can be associated with the system bus 54, and thus the other components associated with the bus. As illustrated,
the speaker 36, keypad 46 and card reader 50 are associated with the system bus 54. A variety of data input/output devices ("I/O Devices") may also associated with the system bus 54, such as, though not specifically illustrated, the RS-232 port 38, the USB 40, and the infrared communication transmitter/receiver 42. As will be appreciated, these devices/elements may operate in accordance with different protocols and have different architectures, and have appropriate interfaces provided for communicating with the system bus 54. For example, the infrared transmitter/receiver may have different layers, including a physical layer including the light-emitting device, and link and other layers which include software and/or hardware, as is known. A variety of other input/output devices may be associated with the PGD 20, as now known or later developed.

[0035] As stated above, the PGD 20 may include a wireless, radio frequency, and communication interface. The architectures/protocols of such wireless communication interfaces are well known and thus will not be described in detail herein. In general, however, such an interface 44 permits two-way data communication. The PGD 20 may be permitted to communicate with a wide variety of devices/systems, including at least one device associated with a gaming network. The PGD 20 may send and receive data, including program code, through the communication interface 44 (or the other input/output devices, such as the infrared transmitter/receiver). As one example described in more detail below, a gaming server may transmit requested code for an application via a transceiver to the communication interface 44 of the PGD 20. The received code may be executed by the central processing unit 52 as it is received and/or stored in the memory 56 for later execution. In one embodiment, the PGD 20 may include a mass data storage device (not shown) such as a hard drive, CD-ROM or the like. In one or more embodiments, the memory 56 may comprise a smart card or similar easily removable (and replaceable) device. In such event, data, such as operating code, may be associated with the PGD 20 via a CD-ROM placed in a CD-ROM drive or by insertion of a coded smart card or portable memory device.

[0036] Although the foregoing exemplary PGD 20 is fairly specific with respect to many details, it will be readily appreciated that a wide variety of similarly suitable devices can also be used as a PGD. For example, the PGD may be a specialized unit carried by casino personnel to only provide mobile gaming service functions. As discussed herein, it will be understood that use of the term "PGD" can refer to the exemplary PGD 20 disclosed above, as well as any other suitable device that can serve as a PGD for any purpose of the present invention, and that such a device or devices may or may not be portable or hand-held. Further, while use of the terms "portable" and "mobile" gaming device are used, it is understood that use of other suitable non-portable PGDs may be substituted in relevant instances.

[0037] FIG. 3 is a schematic of an exemplary gaming system including a PGD in accordance with the invention. As illustrated therein, the gaming system, generally numbered 60, includes a PGD interface 62. This PGD interface 62 serves as a gateway to data communications between the PGD 20 and various networks, servers and other devices. In one embodiment, data communications between the PGD 20 and the PGD interface 62 is via a transceiver 64 associated with the PGD interface 62. In general, the transceiver is arranged to receive information from the PGD interface 62 and transmit it to the PGD 20 and/or receive information from the PGD 20. As illustrated, a PGD 20 may communicate directly with the transceiver 64. It will be appreciated, however, that limitations may exist as to the range over which such data can be accurately transmitted. Therefore, in one or more embodiments, one or more relays 66 may be provided for receiving and re-transmitting the data to the appropriate location.

[0038] As stated above, in a preferred embodiment, the PGD interface 62 serves as a gateway or interface between the one or more PGDs 20 and one or more other devices, systems or networks. The interface 62, whether in the form of a wireless interface or a docking station, may be associated with or reside in a kiosk, slot or other type of gaming machine, a point of sale device, a personal computer or the like. As illustrated, in one embodiment, the PGD interface 62 is associated with a financial server 68 either via a direct link (as illustrated in FIG. 3) or via a network. The financial server 68 may be a computer or be associated with a computer having a processing unit and one or more data files. The financial server 68 is preferably arranged to confirm financial transaction data. For example, in order for a player to be permitted to play a game using the PGD 20, the player may be required to place a bet. In one embodiment, the portable memory device may be updated using a credit card. In such event, the player may swipe their credit card using the card reader 50 associated with the PGD 20. This data may be transmitted to the financial server 68 for confirmation (and as is known in the art, the generation of financial transaction data, such as a transaction date, time and value).

[0039] In one embodiment, the system 60 includes a game server 70. As illustrated, the game server 70 is associated with the PGD interface 62, either directly or via a network. In one or more embodiments, the game server 70 is, or is associated with, a computing device, such as a processor adapted to execute game code. Preferably, the game server 70 is arranged to provide game data to the PGD 20 via the interface 62. This game data may comprise video data for generating an image on a display 34 of the PGD 20, and sound data for generating sound emitted by the speaker 36. The game server 70 is preferably also adapted to receive input from a player, such as a player selection during the play of a game. In one embodiment, a reservation server 72 is connected to the PGD interface 62, either directly or via a network. The reservation server 72 may be arranged to accept reservation selections, and provide information regarding available hotel rooms, rates, shows, restaurants and the like for use by a player of the PGD 20 in making a reservation selection.

[0040] The system may also include a validation server 82 having a confirmation number database with a list of confirmation numbers of distributed cashless ticket vouchers. The validation server 82 may have an interface to receive the unique identifier of a cashless ticket voucher. The unique identifier may then be compared with the list of confirmation numbers in the confirmation number database. If there is a match, an approved message may be relayed to the remote gaming server and/or PGD and the unique identifier and confirmation number is subsequently marked as used or deleted. This ensures that the cashless ticket voucher cannot be reused if reinserted. Otherwise, a rejection message may be relayed if no match was found.
While the PGD 20 may communicate with other devices via direct network links as illustrated in FIG. 2, the PGD 20 may communicate with a variety of other devices (via a wired or wireless connection) such as the portable memory device, a printer, kiosk, cell phone, slot machine, another computer, and the like. Internet gateway 74 may also be used to allow the PGD 20 to connect to other services available on the Internet.

Anonymous Account Creation

FIG. 4 is a block diagram illustrating a method for creating an anonymous account to play a wager-based game of chance. A cashless ticket voucher may be formed at 400 via a remote gaming server. The remote gaming server may be, but is not limited to, a personal computer, slot machine, a kiosk, remote gaming device, another PGD such as a used limited to a cell phone, a personal digital assistant, and a wireless game player, or any other gaming machine that may be used to generate a cashless ticket voucher. For example, a player may input credit card information into a personal computer to generate a cashless ticket voucher for use on a PGD. Alternatively, the player may input cash into a bill validator on a slot machine to obtain the cashless ticket voucher. In some implementations, a player may use a portable device, such as a cellular telephone, a personal digital assistant, a PDG, etc., to communicate directly with a gaming machine for the purpose of obtaining the cashless ticket voucher. For example, an infrared, Bluetooth™ or other interface of the portable device may use a system comparable to that of NTT DoCoMo’s i-mode mobile Internet service, Sanyo’s i-PS system, or the like, which facilitate purchases from vending machines using cellular telephones. User ID and age could be verified by reference to cellular phone registration data, e.g., by using a system such as that developed by Matsushita Refrigeration Co. for ensuring that alcoholic beverages and cigarettes are sold only to adults from vending machines. Through whatever means, the cashless ticket voucher formed may have a unique identifier and a monetary value associated with it. This allows a user to remain anonymous when playing a wager-based game of chance since no identifying or personal information is needed to generate and/or use the cashless ticket voucher. The unique identifier may be any combination of words, number, and/or symbols as described below to identify and provide security to the cashless ticket voucher. The ticket voucher may be printed with any template desired. For example, the ticket voucher may not indicate the monetary value, may state that it is valid for PGD use only, etc.

The ticket voucher unique identifier may be inputted into the second gaming device, such as a PGD, at 402 to expend the monetary value of the cashless ticket voucher. The unique identifier may be inputted using any means available. For example, the player may manually input the unique identifier into the PGD using an interactive display, keyboard, or any other similar means. In another embodiment, the PGD may be placed in a docking station where the unique identifier may be download onto the device. In yet another embodiment, a camera on the PGD may be used. An image of the ticket voucher may be taken and transmitted to the PGD and/or remote gaming server.

In still another embodiment, the unique identifier may be obtained via a scanner, such as a barcode or magnetic stripe scanner, or ticket acceptor. The scanner or ticket acceptor may be coupled to the PDG and/or remote gaming server. If coupled to the remote gaming server, a docking station, transceiver, or wireless or non-wireless means may be used to download the unique identifier to the PGD.

Alternatively, the unique identifier does not have to be downloaded to the PGD. Rather, the scanner or ticket acceptor may be in communication with the validation server and forwards the unique identifier directly to the validation server for validation. In any of the above examples, an additional security code may be associated with the unique identifier. The security code may be any known security codes such as a personal identification number or password, a biometric identifier obtained from a biometric device as described above, and any other similar security means. The player may be required to input the security code before the unique identifier is forwarded to the validation server.

The unique identifier may be transmitted to the validation server at 404. The validation server may have a confirmation number database with a list of confirmation numbers of distributed cashless ticket vouchers. The unique identifier may then be compared with the list of confirmation numbers in the confirmation number database. If there is a match at 406, an approved message may be relayed to the remote gaming server or direction to the PGD and the unique identifier and confirmation number is subsequently marked as used or deleted. This ensures that the cashless ticket voucher cannot be reused if reinserted. Otherwise, a rejection message may be relayed if no match was found.

A game of chance may be generated on the PGD if the unique identifier is validated at 408. This may be signified by an approval message received from the validation server and/or a transfer of monetary funds to the PGD. In one embodiment, the PGD may require the user to acknowledge that use of the monetary funds to play the game of chance will void the cashless ticket voucher.

The use of cashless ticket vouchers requires that certain security measures be taken. For example, players may attempt to redeem the same voucher ticket a second time. Thus, efforts should be taken to notify players that a ticket voucher has been redeemed and is no longer valid. One embodiment to void a redeemed ticket may be to print a written indicium on the cashless ticket voucher to indicate the ticket voucher is void, such as a dark line, “X”, the word “VOID”, or any other written indicium.

In another embodiment, the ticket voucher may be coated with a light sensitive coating so that when the redeemed ticket is scanned or inserted into a ticket accepter, the ticket voucher may be exposed to light, thereby voiding the ticket voucher.

The tickets may be returned to the establishment where the ticket voucher was formed. Various incentives may be used to entice a player to return redeemed ticket vouchers. One embodiment may be to retain an amount from the monetary value of the ticket voucher from game play, similar to a security deposit. Once the ticket is returned, the retained amount would be returned to the player. This may also be used with player tracking points—points may be deducted and redeemed upon return of the ticket voucher. In another embodiment, the ticket voucher may be used to enter the player into a second game of chance, such as a lottery drawing. It will now be realized that other means to entice a player to return redeemed ticket vouchers may be used.
Secure Validation Numbers and Counterfeit Detection

The cashless instruments or printed tickets described above can in some instances be susceptible to counterfeiting by those that wish to fabricate false cashless instruments and redeem them for money. Typically, the validation number is printed on the printed ticket and a corresponding confirmation number is also stored in a back-end system, such as the confirmation number database of the validation server. When a printed ticket is redeemed, the unique identifier is checked to see if it matches the stored confirmation number in the validation server. If so, the printed ticket amount is paid out. However, such validation numbers are often just number strings that may have predictable portions and/or unpredictable portions.

For example, unique identifiers are often generated as a multiple-digit number or code, such as a 10 digit number “1234567890,” where the first seven digits “1234567” are used for every printed ticket generated at a given location and time frame, while the last three digits “890” are sequentially or randomly generated with each new ticket printed at that location during that time frame. Thus, a printed ticket could be issued with the unique identifier “1234567890,” and 100 tickets later another printed ticket might be printed with the unique identifier “1234567215,” and so forth. As will be readily appreciated, characters other than numbers might also be used in such a number or code validation system, with such characters including letters, dashes, punctuation marks and the like. Alternatively, bar codes or other devices could be used in such a ticket validation system. It will be understood that any and all such alternative uses of other characters and/or devices can be used in conjunction with the methods and systems of the present invention. In yet another specific example, a multiple-digit number or code for a printed ticket might be represented as “1234-ABCD-5678-efgh,” where the first two sets of characters can represent the gaming establishment, gaming machine, time and date, among other items, and thus appear to remain constant and/or can be readily discerned by a thief or other unscrupulous party attempting to decipher printed tickets. The third set of characters might simply involve a sequential numbering system for printed tickets, while the fourth set of characters represents a randomly generated set of numbers or other characters that cannot be predicted.

A potential thief or other unscrupulous party might then discern such a pattern by a simple inspection of several printed tickets, thus guessing that one or more sets of digits remain the same, while others sets or individual digits are varied, perhaps sequentially, perhaps randomly, or in some other manner. The potential thief could then create his or her own printed tickets with the same constant or predictable digits, and guess at the variable or random digits, hoping to get lucky for an “easy” cash out of a fraudulent ticket. To combat such an approach, various methods and systems, such as incorporating the use of hash numbers, codes or values may be used. This and other methods and systems are disclosed in co-pending application Ser. No. 10/938,934, filed Sep. 9, 2004, entitled “Counterfeit Cashless Instrument Detection Methods and Systems”, which is incorporated herein in its entirety for all purposes, and will not be discussed further to prevent obfuscation of the invention.

Exemplary Gaming Machine

As stated above, the remote gaming server may be, but is not limited to, a personal computer, slot machine, remote gaming device, another PGD such as but not limited to a cell phone, a personal digital assistant, and a wireless game player, or any other gaming machine. FIG. 5 illustrates an exemplary gaming machine in accordance with an embodiment of the invention.

Video gaming machine 502 includes a main cabinet 504, which generally surrounds the machine interior (not shown) and is viewable by users. The main cabinet includes a main door 508 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 5032, a coin acceptor 5028, and a bill validator 5030, a coin tray 5038, and a belly glass 5040. Viewable through the main door is a video display monitor 5034 and an information panel 5036. The display monitor 5034 will typically be a cathode ray tube, high resolution flat-panel LCD, or other conventional electronically controlled video monitor. The information panel 5036 may be a back-lit, silk screened glass panel with lettering to indicate general game information including, for example, a game denomination (e.g. $0.25 or $1). The bill validator 5030, player-input switches 5032, video display monitor 5034, and information panel are devices used to play a game on the game machine 502. The devices are controlled by circuitry (e.g. the master gaming controller) housed inside the main cabinet 504 of the machine 502.

Many different types of games, including mechanical slot games, video slot games, video poker, video black jack, video pachinko and lottery, may be provided with gaming machines of this invention. In particular, the gaming machine 502 may be operable to provide a play of many different instances of games of chance. The instances may be differentiated according to themes, sounds, graphics, type of game (e.g., slot game vs. card game), denomination, number of paylines, maximum jackpot, progressive or non-progressive, bonus games, etc. The gaming machine 502 may be operable to allow a player to select a game of chance to play from a plurality of instances available on the gaming machine. For example, the gaming machine may provide a menu with a list of the instances of games that are available for play on the gaming machine and a player may be able to select from the list a first instance of a game of chance that they wish to play.

The various instances of games available for play on the gaming machine 502 may be stored as game software on a mass storage device in the gaming machine or may be generated on a remote gaming device but then displayed on the gaming machine. The gaming machine 502 may execute game software, such as but not limited to video streaming software that allows the game to be displayed on the gaming machine. When an instance is stored on the gaming machine 502, it may be loaded from the mass storage device into a RAM for execution. In some cases, after a selection of an instance, the game software that allows the selected instance to be generated may be downloaded from a remote gaming device, such as another gaming machine.

The gaming machine 502 includes a top box 506, which sits on top of the main cabinet 504. The top box 506 houses a number of devices, which may be used to add features to a game being played on the gaming machine 502, including speakers 5010, 5012, 5014, a ticket printer 5018.
which prints bar-coded tickets 5020, a key pad 5022 for entering player tracking information, a fluorescent display 5016 for displaying player tracking information, a card reader 5024 for entering a magnetic striped card containing player tracking information, and a video display screen 5045. The ticket printer 5018 may be used to print tickets for a cashless ticketing system. Further, the top box 506 may house different or additional devices than shown in FIG. 5. For example, the top box may contain a bonus wheel or a back-lit silk screened panel that may be used to add bonus features to the game being played on the gaming machine. As another example, the top box may contain a display for a progressive jackpot offered on the gaming machine. During a game, these devices are controlled and powered, in part, by circuitry (e.g. a master gaming controller) housed within the main cabinet 504 of the machine 502.

[0059] Understand that gaming machine 502 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 only a single game display—mechanical or video, while others are designed for bars and have displays that face upwards. As another example, a game may be generated in a host computer and may be displayed on a terminal or a remote gaming device. The remote gaming device may be connected to the host computer via a network of some type such as a local area network, a wide area network, an intranet or the Internet. The remote gaming device may be a portable gaming device such as a cell phone, a personal digital assistant, and a wireless game player. Images rendered from 3-D gaming environments may be displayed on portable gaming devices that are used to play a game of chance. Further a gaming machine or server may include gaming logic for commanding a remote gaming device to render an image from a virtual camera in a 3-D gaming environment stored on the remote gaming device and to display the rendered image on a display located on the remote gaming device. Thus, 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.

[0060] Some preferred gaming machines of the present assignee are implemented with special features and/or additional circuitry that differentiates them from general-purpose computers (e.g., desktop PCs and laptops). Gaming machines are highly regulated to ensure fairness and, in many cases, gaming machines are operable to dispense monetary awards of multiple millions of dollars. Therefore, to satisfy security and regulatory requirements in a gaming environment, hardware and software architectures may be implemented in gaming machines that differ significantly from those of general-purpose computers. A description of gaming machines relative to general-purpose computing machines and some examples of the additional (or different) components and features found in gaming machines are described below.

[0061] At first glance, one might think that adapting PC technologies to the gaming industry would be a simple proposition because both PCs and gaming machines employ microprocessors that control a variety of devices. However, because of such reasons as 1) the regulatory requirements that are placed upon gaming machines, 2) the harsh environment in which gaming machines operate, 3) security requirements and 4) fault tolerance requirements, adapting PC technologies to a gaming machine can be quite difficult. Further, techniques and methods for solving a problem in the PC industry, such as device compatibility and connectivity issues, might not be adequate in the gaming environment. For instance, a fault or a weakness tolerated in a PC, such as security holes in software or frequent crashes, may not be tolerated in a gaming machine because in a gaming machine these faults can lead to a direct loss of funds from the gaming machine, such as stolen cash or loss of revenue when the gaming machine is not operating properly.

[0062] For the purposes of illustration, a few differences between PC systems and gaming systems will be described. A first difference between gaming machines and common PC based computer systems is that gaming machines are designed to be state-based systems. In a state-based system, the system stores and maintains its current state in a non-volatile memory, such that, in the event of a power failure or other malfunction the gaming machine will return to its current state when the power is restored. For instance, if a player was shown an award for a game of chance and, before the award could be provided to the player the power failed, the gaming machine, upon the restoration of power, would return to the state where the award is indicated. As anyone who has used a PC, knows, PCs are not state machines and a majority of data is usually lost when a malfunction occurs. This requirement affects the software and hardware design on a gaming machine.

[0063] A second important difference between gaming machines and common PC based computer systems is that for regulation purposes, the software on the gaming machine used to generate the game of chance and operate the gaming machine has been designed to be static and monolithic to prevent cheating by the operator of gaming machine. For instance, one solution that has been employed in the gaming industry to prevent cheating and satisfy regulatory requirements has been to manufacture a gaming machine that can use a proprietary processor running instructions to generate the game of chance from an EPROM or other form of non-volatile memory. The coding instructions on the EPROM are static (non-changeable) and must be approved by a gaming regulators in a particular jurisdiction and installed in the presence of a person representing the gaming jurisdiction. Any changes to any part of the software required to generate the game of chance, such as adding a new device driver used by the master gaming controller to operate a device during generation of the game of chance can require a new EPROM to be burnt, approved by the gaming jurisdiction and reinstalled on the gaming machine in the presence of a gaming regulator. Regardless of whether the EPROM solution is used, to gain approval in most gaming jurisdictions, a gaming machine must demonstrate sufficient safeguards that prevent an operator or player of a gaming machine from manipulating hardware and software in a manner that gives them an unfair and some cases an illegal advantage. The gaming machine should have a means to determine if the code it will execute is valid. If the code is not valid, the gaming machine must have a means to prevent the code from being executed. The code validation requirements in the gaming industry affect both hardware and software designs on gaming machines.

[0064] A third important difference between gaming machines and common PC based computer systems is the number and kinds of peripheral devices used on a gaming
machine are not as great as on PC based computer systems. Traditionally, in the gaming industry, gaming machines have been relatively simple in the sense that the number of peripheral devices and the number of functions the gaming machine has been limited. Further, in operation, the functionality of gaming machines were relatively constant once the gaming machine was deployed, i.e., new peripherals devices and new gaming software were infrequently added to the gaming machine. This differs from a PC where users will go out and buy different combinations of devices and software from different manufacturers and connect them to a PC to suit their needs depending on a desired application. Therefore, the types of devices connected to a PC may vary greatly from user to user depending in their individual requirements and may vary significantly over time.

Although the variety of devices available for a PC may be greater than on a gaming machine, gaming machines still have unique device requirements that differ from a PC, such as device security requirements not usually addressed by PCs. For instance, monetary devices, such as coin dispensers, bill validators and ticket printers and computing devices that are used to govern the input and output of cash to a gaming machine have security requirements that are not typically addressed in PCs. Therefore, many PC techniques and methods developed to facilitate device connectivity and device compatibility do not address the emphasis placed on security in the gaming industry.

To address some of the issues described above, a number of hardware/software components and architectures are utilized in gaming machines that are not typically found in general purpose computing devices, such as PCs. These hardware/software components and architectures, as described below in more detail, include but are not limited to watchdog timers, voltage monitoring systems, state-based software architecture and supporting hardware, specialized communication interfaces, security monitoring and trusted memory.

A watchdog timer is normally used in IGT gaming machines to provide a software failure detection mechanism. In a normally operating system, the operating software periodically accesses control registers in the watchdog timer subsystem to “re-trigger” the watchdog. Should the operating software fail to access the control registers within a preset timeframe, the watchdog timer will timeout and generate a system reset. Typical watchdog timer circuits contain a loadable timeout counter register to allow the operating software to set the timeout interval within a certain range of time. A differentiating feature of the some preferred circuits is that the operating software cannot completely disable the function of the watchdog timer. In other words, the watchdog timer always functions from the time power is applied to the board.

IGT gaming computer platforms preferably use several power supply voltages to operate portions of the computer circuitry. These can be generated in a central power supply or locally on the computer board. If any of these voltages falls out of the tolerance limits of the circuitry they power, unpredictable operation of the computer may result. Though modern general-purpose computers include voltage monitoring circuitry, these types of circuits only report voltage status to the operating software. Out of tolerance voltages can cause software malfunction, creating a potential uncontrolled condition in the gaming computer. Gaming machines of the present assignee typically have power supplies with tighter voltage margins than that required by the operating circuitry. In addition, the voltage monitoring circuitry implemented in IGT gaming computers typically has two thresholds of control. The first threshold generates a software event that can be detected by the operating software and an error condition generated. This threshold is triggered when a power supply voltage falls out of the tolerance range of the power supply, but is still within the operating range of the circuitry. The second threshold is set when a power supply voltage falls out of the operating tolerance of the circuitry. In this case, the circuitry generates a reset, halting operation of the computer.

The standard method of operation for IGT slot machine game software is to use a state machine. Different functions of the game (bet, play, result, points in the graphical presentation, etc.) may be defined as a state. When a game moves from one state to another, critical data regarding the game software is stored in a custom non-volatile memory subsystem. This is critical to ensure the player’s wager and credits are preserved and to minimize potential disputes in the event of a malfunction on the gaming machine.

In general, the gaming machine does not advance from a first state to a second state until critical information that allows the first state to be reconstructed is stored. This feature allows the game to recover operation to the current state of play in the event of a malfunction, loss of power, etc. that occurred just prior to the malfunction. After the state of the gaming engine software is restored during the play of a game of chance, game play may resume and the game may be completed in a manner that is no different than if the malfunction had not occurred. Typically, battery backed RAM devices are used to preserve this critical data although other types of non-volatile memory devices may be employed. These memory devices are not used in typical general-purpose computers.

As described in the preceding paragraph, when a malfunction occurs during a game of chance, the gaming machine may be restored to a state in the game of chance just prior to when the malfunction occurred. The restored state may include metering information and graphical information that was displayed on the gaming machine in the state prior to the malfunction. For example, when the malfunction occurs during the play of a card game after the cards have been dealt, the gaming machine may be restored with the cards that were previously displayed as part of the card game. As another example, a bonus game may be triggered during the play of a game of chance where a player is required to make a number of selections on a video display screen. When a malfunction has occurred after the player has made one or more selections, the gaming machine may be restored to a state that shows the graphical presentation at the just prior to the malfunction including an indication of selections that have already been made by the player. In general, the gaming machine may be restored to any state in a plurality of states that occur in the game of chance that occurs while the game of chance is played or to states that occur between the play of a game of chance.

Game history information regarding previous games played such as an amount wagered, the outcome of the game and so forth may also be stored in a non-volatile memory device. The information stored in the non-volatile memory may be detailed enough to reconstruct a portion of the graphical presentation that was previously presented on.
the gaming machine and the state of the gaming machine (e.g., credits) at the time the game of chance was played. The game history information may be utilized in the event of a dispute. For example, a player may decide that in a previous game of chance that they did not receive credit for an award that they believed they won. The game history information may be used to reconstruct the state of the gaming machine prior, during and/or after the disputed game to demonstrate whether the player was correct or not in their assertion.

Another feature of gaming machines, such as IGT gaming computers, is that they often contain unique interfaces, including serial interfaces, to connect to specific subsystems internal and external to the slot machine. The serial devices may have electrical interface requirements that differ from the “standard” EIA 232 serial interfaces provided by general-purpose computers. These interfaces may include EIA 485, EIA 422, Fiber Optic Serial, optically coupled serial interfaces, current loop style serial interfaces, etc. In addition, to conserve serial interfaces internally in the slot machine, serial devices may be connected in a shared, daisy-chain fashion where multiple peripheral devices are connected to a single serial channel.

The serial interfaces may be used to transmit information using communication protocols that are unique to the gaming industry. For example, IGT’s Netplex is a proprietary communication protocol used for serial communication between gaming devices. As another example, SAS is a communication protocol used to transmit information, such as metering information, from a gaming machine to a remote device. Often SAS is used in conjunction with a player tracking system.

IGT gaming machines may alternatively be treated as peripheral devices to a casino communication controller and connected in a shared daisy chain fashion to a single serial interface. In both cases, the peripheral devices are preferably assigned device addresses. If so, the serial controller circuitry must implement a method to generate or detect unique device addresses. General-purpose computer serial ports are not able to do this.

Security monitoring circuits detect intrusion into an IGT gaming machine by monitoring security switches attached to access doors in the slot machine cabinet. Preferably, access violations result in suspension of game play and can trigger additional security operations to preserve the current state of game play. These circuits also function when power is off by use of a battery backup. In power-off operation, these circuits continue to monitor the access doors of the slot machine. When power is restored, the gaming machine can determine whether any security violations occurred while power was off, e.g., via software for reading status registers. This can trigger event log entries and further data authentication operations by the slot machine software.

Trusted memory devices are preferably included in an IGT gaming machine computer to ensure the authenticity of the software that may be stored on less secure memory subsystems, such as mass storage devices. Trusted memory devices and controlling circuitry are typically designed to not allow modification of the code and data stored in the memory device while the memory device is installed in the slot machine. The code and data stored in these devices may include authentication algorithms, random number generators, authentication keys, operating system kernels, etc. The purpose of these trusted memory devices is to provide gaming regulatory authorities a root trusted authority within the computing environment of the slot machine that can be tracked and verified as original. This may be accomplished via removal of the trusted memory device from the slot machine computer and verification of the secure memory device contents is a separate third party verification device. Once the trusted memory device is verified as authentic, and based on the approval of the verification algorithms contained in the trusted device, the gaming machine is allowed to verify the authenticity of additional code and data that may be located in the gaming computer assembly, such as code and data stored on hard disk drives. A few details related to trusted memory devices that may be used in the present invention are described in U.S. Pat. No. 6,685,567 from U.S. patent application Ser. No. 09/925,098, filed Aug. 8, 2001 and titled “Process Verification,” which is incorporated herein in its entirety and for all purposes.

Mass storage devices used in a general purpose computer typically allow code and data to be read from and written to the mass storage device. In a gaming machine environment, modification of the gaming code stored on a mass storage device is strictly controlled and would only be allowed under specific maintenance type events with electronic and physical enablers required. Though this level of security could be provided by software, IGT gaming computers that include mass storage devices preferably include hardware level mass storage data protection circuitry that operates at the circuit level to monitor attempts to modify data on the mass storage device and will generate both software and hardware error triggers should a data modification be attempted without the proper electronic and physical enablers being present.

Returning to the example of FIG. 5, when a user wishes to play the gaming machine 502, he or she inserts cash through the coin acceptor 5028 or bill validator 5030. Additionally, the bill validator may accept a printed ticket voucher that may be accepted by the bill validator 5030 as indicia of credit when a cashless ticketing system is used. At the start of the game, the player may enter playing tracking information using the card reader 5024, the keypad 5022, and the florescent display 5016. Further, other game preferences of the player playing the game may be read from a card inserted into the card reader. During the game, the player views game information using the video display 5034. Other game and prize information may also be displayed in the video display screen 5045 located in the top box.

During the course of a game, a player may be required to make a number of decisions, which affect the outcome of the game. For example, a player may vary his or her wager on a particular game, select a prize for a particular game selected from a prize server, or make game decisions that affect the outcome of a particular game. The player may make these choices using the player-input switches 5032, the video display screen 5034 or using some other device which enables a player to input information into the gaming machine. In some embodiments, the player may be able to access various game services such as concierge services and entertainment content services using the video display screen 5034 and one or more input devices.

During certain game events, the gaming machine 502 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 5010, 5012, 5014. Visual effects include flashing lights, strobing lights or other patterns displayed from lights on the gaming machine 502 or from lights behind the belly glass 5040. After the player has completed a game, the player may receive game tokens from the coin tray 5038 or the ticket 5020 from the printer 5018, which may be used for further games or to redeem a prize. Further, the player may receive a ticket 5020 for food, merchandise, or games from the printer 5018.

Exemplary System Architecture

One example of a network topology for implementing some aspects of the present invention is shown in FIG. 6. Those of skill in the art will realize that this exemplary architecture and the related functionality are merely examples and that the present invention encompasses many other such embodiments and methods. Here, for example, a single gaming establishment 1205 is illustrated, which is a casino in this example. However, it should be understood that some implementations of the present invention involve multiple gaming establishments.

Gaming establishment 1205 includes 16 gaming machines 2, each of which is part of a bank 1210 of gaming machines 2. In this example, gaming establishment 1205 also includes a bank of networked gaming tables 1100. It will be appreciated that many gaming establishments include hundreds or even thousands of gaming machines 2 and/or gaming tables 1100, not all of which are included in a bank. However, the present invention may be implemented in gaming establishments having any number of gaming machines, gaming tables, etc.

Various alternative network topologies can be used to implement different aspects of the invention and/or to accommodate varying numbers of networked devices. For example, gaming establishments with very large numbers of gaming machines 2 may require multiple instances of some network devices (e.g., of main network device 1225, which combines switching and routing functionality in this example) and/or the inclusion of other network devices not shown in FIG. 6. For example, some implementations of the invention include one or more middleware servers disposed between gaming machines 2 and server 1230. Such middleware servers can provide various useful functions, including but not limited to the filtering and/or aggregation of data received from bank switches 1215, from individual gaming machines and from other player terminals. Some implementations of the invention include load balancing methods and devices for managing network traffic.

Each bank 1210 has a corresponding bank switch 1215, which may be a conventional bank switch. Each bank switch is connected to server-based gaming (“SBG”) server 1230 via main network device 1225, which combines switching and routing functionality in this example. Although various floor communication protocols may be used, some preferred implementations use IGT’s open, Ethernet-based SuperSAS® protocol, which IGT makes available for downloading without charge. However, other protocols such as Best of Breed (“BOB”) may be used to implement various aspects of SBG. IGT has also developed a gaming-industry-specific transport layer called CASH that rides on top of TCP/IP and offers additional functionality and security.

SBG server 1230, License Manager 1231, Arbiter 133, servers 1232, 1234, 1236 and 1238, and main network device 1225 are disposed within computer room 1220 of gaming establishment 1205. In practice, more or fewer servers may be used. Some of these servers may be configured to perform tasks relating to player tracking, bonusing/progressives, etc. Some servers may be configured to perform tasks specific to the present invention. License Manager 1231 may also be implemented, at least in part, via a server or a similar device. Some exemplary operations of License Manager 1231 are described in detail in U.S. patent application Ser. No. 11/225,408, entitled "METHODS AND APPARATUS FOR AUTHENTICATION AND LICENSING IN A GAMING NETWORK" by Kinsley et al., which is hereby incorporated by reference.

SBG server 1230 can also be configured to implement, at least in part, various aspects of the present invention. Some preferred embodiments of SBG server 1230 and the other servers shown in FIG. 6 include (or are at least in communication with) clustered CPUs, redundant storage devices, including backup storage devices, switches, etc. Such storage devices may include a redundant array of inexpensive disks (“RAID”), back-up hard drives and/or tape drives, etc. Preferably, a Radius and a DHCP server are also configured for communication with the gaming network. Some implementations of the invention provide one or more of these servers in the form of blade servers.

In some implementations of the invention, many of these devices (including but not limited to License Manager 1231, servers 1232, 1234, 1236 and 1238, and main network device 1225) are mounted in a single rack with SBG server 1230. Accordingly, many or all such devices will sometimes be referenced in the aggregate as an “SBG server.” However, in alternative implementations, one or more of these devices is in communication with SBG server 1230 and/or other devices of the network but located elsewhere. For example, some of the devices could be mounted in separate racks within computer room 1220 or located elsewhere on the network. For example, it can be advantageous to store large volumes of data elsewhere via a storage area network (“SAN”).

In some embodiments, these components are SBG server 1230 preferably has an uninterruptible power supply (“UPS”). The UPS may be, for example, a rack-mounted UPS module.

Computer room 1220 may include one or more operator consoles or other host devices that are configured for communication with SBG server 1230. Such host devices may be provided with software, hardware and/or firmware for implementing various aspects of the invention; many of these aspects involve controlling SBG server 1230. However, such host devices need not be located within computer room 1220. Wired host device 1260 (which is a laptop computer in this example) and wireless host device 1270 (which is a PDA in this example) may be located elsewhere in gaming establishment 1205 or at a remote location.

Arbiter 133 may be implemented, for example, via software that is running on a server or another networked device. Arbiter 133 serves as an intermediary between different devices on the network. Some implementations of Arbiter 133 are described in U.S. patent application Ser. No. 10/948,387, entitled "METHODS AND APPARATUS FOR NEGOTIATING COMMUNICATIONS WITHIN A GAMING NETWORK" and filed Sep. 23, 2004 (the “Arbiter Application”), which is incorporated herein by reference and
for all purposes. In some preferred implementations, Arbiter 133 is a repository for the configuration information required for communication between devices on the gaming network (and, in some implementations, devices outside the gaming network). Although Arbiter 133 can be implemented in various ways, one exemplary implementation is discussed in the following paragraphs.

Fig. 7 is a block diagram of a simplified communication topology between a gaming unit 21, the network computer 23 and the Arbiter 133. Although only one gaming unit 21, one network computer 23 and one Arbiter 133 are shown in Fig. 7, it should be understood that the following examples may be applicable to different types of network gaming devices within the gaming network 12 beyond the gaming unit 21 and the network computer 23, and may include different numbers of network computers, gaming security arbiters and gaming units. For example, a single Arbiter 133 may be used for secure communications among a plurality of network computers 23 and tens, hundreds or thousands of gaming units 21. Likewise, multiple gaming security arbiters 46 may be utilized for improved performance and other scalability factors.

Referencing Fig. 7, the Arbiter 133 may include an arbiter controller 121 that may comprise a program memory 122, a microcontroller or microprocessor (MP) 124, a random-access memory (RAM) 126 and an input/output (I/O) circuit 128, all of which may be interconnected via an address/data bus 129. The network computer 23 may also include a controller 131 that may comprise a program memory 132, a microcontroller or microprocessor (MP) 134, a random-access memory (RAM) 136 and an input/output (I/O) circuit 138, all of which may be interconnected via an address/data bus 139. It should be appreciated that although the Arbiter 133 and the network computer 23 are each shown with only one microprocessor 124, 134, the controllers 121, 131 may each include multiple microprocessors 124, 134. Similarly, the memory of the controllers 121, 131 may include multiple RAMs 126, 136 and multiple program memories 122, 132. Although the I/O circuits 128, 138 are each shown as a single block, it should be appreciated that the I/O circuits 128, 138 may include a number of different types of I/O circuits. The RAMs 126, 136 and program memories 122, 132 may be implemented as semiconductor memories, magnetically readable memories, and/or optically readable memories, for example.

Although the program memories 122, 132 are shown in Fig. 7 as read-only memories (ROM) 122, 132, the program memories of the controllers 121, 131 may be a read/write or alterable memory, such as a hard disk. In the event a hard disk is used as a program memory, the address/data buses 129, 139 shown schematically in Fig. 7 may each comprise multiple address/data buses, which may be of different types, and there may be an I/O circuit disposed between the address/data buses.

As shown in Fig. 7, the gaming unit 21 may be operatively coupled to the network computer 23 via the data link 25. The gaming unit 21 may also be operatively coupled to the Arbiter 133 via the data link 47, and the network computer 23 may likewise be operatively coupled to the Arbiter 133 via the data link 47. Communications between the gaming unit 21 and the network computer 23 may involve different information types of varying levels of sensitivity resulting in varying levels of encryption techniques depending on the sensitivity of the information. For example, communications such as drink orders and statistical information may be considered less sensitive. A drink order or statistical information may remain encrypted, although with moderately secure encryption techniques, such as RC4, resulting in less processing power and less time for encryption. On the other hand, financial information (e.g., account information, winnings, etc.), game download information (e.g., game software and game licensing information) and personal information (e.g., social security number, personal preferences, etc.) may be encrypted with stronger encryption techniques such as DES, AES, or 3DES to provide increased security.

As disclosed in further detail in the Arbiter Application, the Arbiter 133 may verify the authenticity of each network gaming device. The Arbiter 133 may receive a request for a communication session from a network device. For ease of explanation, the requesting network device may be referred to as the client, and the requested network device may be referred to as the host. The client may be any device on the network 12 and the request may be for a communication session with any other network device. The client may specify the host, or the gaming security arbiter may select the host based on the request and based on information about the client and potential hosts. The Arbiter 133 may provide encryption keys (session keys) for the communication session to the client via the secure communication channel. Either the host and/or the session key may be provided in response to the request, or may have been previously provided. The client may contact the host to initiate the communication session. The host may then contact the Arbiter 133 to determine the authenticity of the client. The Arbiter 133 may provide affirmation (or lack thereof) of the authenticity of the client to the host and provide a corresponding session key, in response to which the network devices may initiate the communication session directly with each other using the session keys to encrypt and decrypt messages.

Alternatively, upon receiving a request for a communication session, the Arbiter 133 may contact the host regarding the request and provide corresponding session keys to both the client and the host. The Arbiter 133 may then initiate either the client or the host to begin their communication session. In turn, the client and host may begin the communication session directly with each other using the session keys to encrypt and decrypt messages. An additional explanation of the communication request, communication response and key distribution is provided in the Arbiter Application.

Wireless devices are particularly useful for managing a gaming network. Such wireless devices could include, but are not limited to, laptops, PDAs or even cellular telephones. Referring once again to Fig. 6, one or more network devices in gaming establishment 1205 can be configured as wireless access points. For example, a casino manager may use a wireless handheld device to revise and/or schedule gaming machine configurations while roaming the casino floor. Similarly, a representative of a regulatory body could use a PDA to verify gaming machine configurations, generate reports, view activity logs, etc., while on the casino floor.

If a host device is located in a remote location, security methods and devices (such as firewalls, authentication and/or encryption) should be deployed in order to prevent the unauthorized access of the gaming network.
Similarly, any other connection between gaming network 1205 and the outside world should only be made with trusted devices via a secure link, e.g., via a virtual private network ("VPN") tunnel. For example, the illustrated connection between SBG 1230, gateway 1250 and central system 1263 (here, IGT.com) that may be used for game downloads, etc., is advantageously made via a VPN tunnel.

0100 An Internet-based VPN uses the open, distributed infrastructure of the Internet to transmit data between sites. A VPN may emulate a private IP network over public or shared infrastructures. A VPN that supports only IP traffic is called an IP-VPN. VPNs provide advantages to both the service provider and its customers. For its customers, a VPN can extend the IP capabilities of a corporate site to remote offices and/or users with intranet, extranet, and dial-up services. This connectivity may be achieved at a lower cost to the gaming entity with savings in capital equipment, operations, and services. Details of VPN methods that may be used with the present invention are described in the reference, “Virtual Private Networks: Technologies and Solutions,” by R. Yueh and T. Strayer, Addison-Wesley, 2001, ISBN#0-201-70209-6, which is incorporated herein by reference and for all purposes.

0101 There are many ways in which IP VPN services may be implemented, such as, for example, Virtual Private Lines, Virtual Private Routed Networks, Virtual Private Dial Networks, Virtual Private LAN Segments, etc. Additionally, VPNs may be implemented using a variety of protocols, such as, for example, IP Security (IPSec) Protocol, Layer 2 Tunneling Protocol, Multiprotocol Label Switching (MPLS) Protocol, etc. Details of these protocols, including RFC reports, may be obtained from the VPN Consortium, an industry trade group (http://www.vpn.com, VPNC, Santa Cruz, Calif.).

0102 For security purposes, any information transmitted to or from a gaming establishment over a public network may be encrypted. In one implementation, the information may be symmetrically encrypted using a symmetric encryption key, where the symmetric encryption key is asymmetrically encrypted using a private key. The public key may be obtained from a remote public key server. The encryption algorithm may reside in processor logic stored on the gaming machine. When a remote server receives a message containing the encrypted symmetric encryption key, the symmetric encryption key is decrypted with a private key residing on the remote server and the symmetrically encrypted information sent from the gaming machine is decrypted using the symmetric encryption key. A different symmetric encryption key is used for each transaction where the key is randomly generated. Symmetric encryption and decryption is preferably applied to most information because symmetric encryption algorithms tend to be 100-10,000 times faster than asymmetric encryption algorithms.

0103 As mentioned elsewhere herein, U.S. patent application Ser. No. 11/225,408, entitled “METHODS AND DEVICES FOR AUTHENTICATION AND LICENSING IN A GAMING NETWORK” by Kinsley et al., describes novel methods and devices for authentication, game downloading and game license management. This application has been incorporated herein by reference.

0104 Providing a secure connection between the local devices of the SBG system and IGT’s central system allows for the deployment of many advantageous features. For example, a customer (e.g., an employee of a gaming establishment) can log onto an account of central system 1263 (in this example, IGT.com) to obtain the account information such as the customer’s current and prior account status.

0105 Moreover, such a secure connection may be used by the central system 1263 to collect information regarding a customer’s system. Such information includes, but is not limited to, error logs for use in diagnostics and troubleshooting. Some implementations of the invention allow a central system to collect other types of information, e.g., information about the usage of certain types of gaming software, revenue information regarding certain types of games and/or gaming machines, etc. Such information includes, but is not limited to, information regarding the revenue attributable to particular games at specific times of day, days of the week, etc. Such information may be obtained, at least in part, by reference to an accounting system of the gaming network(s), as described in U.S. patent application Ser. No. 11/225,407, by Wolf et al., entitled “METHODS AND DEVICES FOR MANAGING GAMING NETWORKS,” which has been incorporated herein by reference.

0106 Automatic updates of a customer’s SBG server may also be enabled. For example, central system 1263 may notify a local SBG server regarding new products and/or product updates. For example, central system 1263 may notify a local SBG server (or another device associated with a gaming establishment) that an additional theme-specific data set and/or updates for a previously-downloaded global payout set are available. Alternatively, such updates could be automatically provided to the local SBG server and downloaded to networked gaming machines.

0107 After the local SBG server receives this information, it can identify relevant products of interest. For example, the local SBG server may identify gaming software that is currently in use (or at least licensed) by the relevant gaming entity and send a notification to one or more host devices, e.g., via email. If an update or a new software product is desired, it can be downloaded from the central system. Some relevant downloading methods are described elsewhere herein and in applications that have been incorporated herein by reference, e.g., in U.S. patent application Ser. No. 11/078,966. Similarly, a customer may choose to renew a gaming software license via a secure connection with central system 1263 in response to such a notification.

0108 Secure communication links allow notifications to be sent securely from a local SBG server to host devices outside of a gaming establishment. For example, a local SBG server can be configured to transmit automatically generated email reports, text messages, etc., based on predetermined events that will sometimes be referred to herein as “triggers.” Such triggers can include, but are not limited to, the condition of a gaming machine door being open, cash box full, machine not responding, verification failure, etc. In addition, providing secure connections between different gaming establishments can enable alternative implementations of the invention. For example, a number of gaming establishments, each with a relatively small number of gaming machines, may be owned and/or controlled by the same entity. In such situations, having secure communications between gaming establishments makes it possible for
a gaming entity to use a single SBG server as an interface between central system 1263 and the gaming establish-
ments.

[0109] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

What is claimed is:
1. A portable gaming device adapted to play at least one wager-based game, comprising:
a communication interface adapted to communicate with a remote gaming server;
a display;
an input mechanism to receive a unique identifier of a cashless ticket voucher;
a controller operatively coupled to the display, communication interface, and the input mechanism; and
a validator operatively coupled to the controller to transmit the unique identifier to the remote gaming server for validation, the validator to receive an approval or a rejection message from the remote gaming server;
wherein the controller is programmed to cause the display to generate a game display relating to the at least one wager-based game and display an outcome of the at least one wager-based game if an approval message is received by the validator.
2. The device of claim 1, wherein the input mechanism is a user interface on the portable gaming device.
3. The device of claim 1, wherein the input mechanism is a transceiver.
4. The device of claim 1, wherein the unique identifier is associated with a security code.
5. The device of claim 1, wherein the security code is a biometric data obtained from a biometric sensor coupled to the portable gaming device.
6. The device of claim 1, wherein the remote gaming server is a gaming machine configured for providing wager-based games of chance.
7. A validation server, comprising:
an interface to receive a cashless ticket voucher unique identifier;
and
a confirmation number database having a list of confirmation numbers of distributed cashless ticket vouchers;
wherein the unique identifier is matched to a confirmation number;
and at least one portable gaming device to play at least one wager-based game, comprising:
a communication interface adapted to communicate with a remote gaming server;
a display;
an input mechanism to receive the unique identifier;
a controller operatively coupled to the display, communication interface, and the input mechanism;
and
a validator operatively coupled to the controller to transmit the unique identifier to the remote gaming server for validation, the validator to receive an approval or a rejection message from the remote gaming server;
wherein the approval message is relayed from the validation server to the remote gaming server if a match is found; and
wherein the controller is programmed to cause the display to generate a game display relating to the at least one wager-based game and display an outcome of the at least one wager-based game if an approval message is received by the validator.
13. The network of claim 12, wherein the remote gaming server is a gaming machine configured for providing games of chance.
14. The network of claim 12, wherein the validation server relays a rejection message to the remote gaming server if the unique identifier is not matched to a confirmation number.
15. The network of claim 12, wherein the interface and wager input mechanism is a wireless transceiver.
16. The network of claim 12, wherein the wager input mechanism is a user interface on the portable gaming device.
17. The network of claim 12, wherein the unique identifier is associated with a security code.
18. The network of claim 17, wherein the security code is a biometric data obtained from a biometric sensor coupled to the portable gaming device.
19. The network of claim 17, wherein the security code is a personal identification number.
20. A method for creating an anonymous account to play a game of chance, comprising:
forming a cashless ticket voucher via a first device, the cashless ticket voucher having a unique identifier and a monetary value;
inputting the unique identifier into a second device to expend the monetary value of the cashless ticket voucher;
forwarding the unique identifier to a validation server to validate the cashless ticket voucher; and
generating the game of chance on the second device if the unique identifier is validated.
21. The method of claim 20, wherein the first device is a gaming machine configured for providing games of chance.
22. The method of claim 20, wherein the first device is a personal computer.
23. The method of claim 20, wherein the second device is a mobile gaming device.
24. The method of claim 20, wherein the forming further comprises entering credit card information.
25. The method of claim 20, wherein the generating further comprises associating a security code with the unique identifier.

26. The method of claim 25, wherein the security code is a personal identification number or password.

27. The method of claim 25, wherein the security code is a biometric identifier obtained from a biometric device.

28. The method of claim 20, wherein the inputting further comprises wirelessly inputting the unique identifier to the second gaming machine.

29. The method of claim 20, wherein the inputting further comprises:

- inserting the second device in a docking station; and
- downloading the unique identifier to the second device.

30. The method of claim 20, wherein the inputting further comprises reading the unique identifier with a scanner coupled to the second device.

31. The method of claim 20, wherein the inputting further comprises:

- reading the unique identifier with a scanner coupled to the first device; and
- downloading the unique identifier to the second device.

32. The method of claim 31, wherein the downloading occurs in a docking station.

33. The method of claim 31, where the downloading occurs wirelessly.

34. The method of claim 20, wherein the forwarding comprises:

- comparing the unique identifier to a list of confirmation numbers; and
- marking the unique identifier as used if the unique identifier matches a confirmation number.

35. The method of claim 20, wherein the forming further comprises coating the ticket voucher with a light sensitive coating.

36. The method of claim 35, further comprising the step of exposing the ticket voucher to light, thereby voiding the ticket voucher.

37. The method of claim 20, wherein the inputting further comprises inserting the ticket voucher into a ticket reader in communication with a validation server.

38. The method of claim 37, wherein the ticket reader is coupled to the first device.

39. The method of claim 37, wherein the ticket reader is removably coupled to the second device.

40. The method of claim 37, further comprising printing a written indicia on the cashless ticket voucher to indicate the ticket voucher is void.

41. The method of claim 20, wherein the inputting further comprises manually inputting the unique identifier into the second device.

42. The method of claim 20, further comprising:

- returning the validated cashless ticket voucher to a third party; and
- redeeming a retained amount from the value of the cashless ticket voucher.

43. The method of claim 20, further comprising:

- returning the validated cashless ticket voucher to a third party; and
- entering the validated ticket voucher into a second game of chance.

44. The method of claim 43, wherein the second game of chance is a lottery drawing.

45. A method for creating an anonymous account to play a game of chance on a mobile gaming device, comprising:

- forming a cashless ticket voucher having a unique identifier, the cashless ticket voucher having a monetary value;
- inputting the unique identifier into the mobile gaming device to expend the monetary value of the cashless ticket voucher;
- validating the unique identifier; and
- generating a game of chance on the mobile gaming device if the unique identifier is validated.

46. The method of claim 45, further comprising voiding the validated ticket voucher.

47. The method of claim 45, wherein the forming further comprises entering credit card information.

48. The method of claim 45, wherein the cashless ticket voucher is obtained from a remote gaming machine.

49. The method of claim 48, wherein the remote gaming machine is a gaming machine configured for providing games of chance.

50. The method of claim 45, wherein the inputting further comprises reading the unique identifier with a scanner.

51. The method of claim 50, wherein the scanner is removably coupled to the mobile gaming device.

52. The method of claim 50, wherein the scanner is coupled to a gaming machine.

53. The method of claim 52, further comprising wirelessly inputting the unique identifier to the mobile gaming device.

54. The method of claim 45, wherein the inputting further comprises inserting the cashless ticket voucher into a ticket reader in communication with a validation server.

55. The method of claim 54, wherein the ticket reader is coupled to a gaming machine.

56. The method of claim 55, further comprising wirelessly downloading the value of the ticket voucher to the mobile gaming device if the unique identifier is validated.

57. The method of claim 54, wherein the ticket reader is removably coupled to the mobile gaming device.

58. The method of claim 46, wherein the voiding further comprises printing a written indicia on the ticket voucher to indicate the ticket voucher is void.

59. The method of claim 46, wherein the voiding further comprises:

- coating the ticket voucher with a light sensitive coating; and
- exposing the ticket voucher to light.

60. The method of claim 45, wherein the inputting further comprises manually inputting the unique identifier into the mobile gaming device.

61. The method of claim 45, wherein the validating further comprises:

- forwarding the unique identifier to a validation server; and
- matching the unique identifier to a list of confirmation numbers.

62. The method of claim 61, further comprising marking the unique identifier as used if there is a match.

63. The method of claim 45, wherein the forming further comprises associating a security code with the unique identifier.

64. The method of claim 63, wherein the security code is a personal identification number or password.

65. The method of claim 63, wherein the security code is a biometric identifier obtained from a biometric device.
66. The method of claim 45, wherein the forming further comprises deducting a retained amount from the monetary value.

67. The method of claim 66, further comprising: returning the ticket voucher to a third party; and redeeming the retained amount.

68. The method of claim 67, further comprising: entering the validated ticket voucher into a second game of chance.

69. The method of claim 68, wherein the second game of chance is a lottery drawing.

70. The method of claim 45, further comprising: returning the validated ticket voucher to a third party; and entering the validated ticket voucher into a second game of chance.

71. The method of claim 70, wherein the second game of chance is a lottery drawing.

* * * * *