

PLAYING CARD DEALING SHOE ACTIVATION DEVICE**CROSS-REFERENCE TO RELATED APPLICATIONS**

The present application claims priority to US Provisional Patent Application No.
5 62/318,881, filed April 6, 2016 titled PLAYING CARD DEALING SHOE ACTIVATION
CARD, the entirety of which is hereby incorporated by reference.

FIELD OF INVENTION

The present disclosure relates to playing card dealing shoes for use in casinos, and
10 more particularly to an activation device for use in the playing card dealing shoe.

BACKGROUND OF INVENTION

Security of playing cards is a major concern for casino properties. From leaving the
factory to destruction, there are various methods and scams used to gain information on or
15 tamper with cards to defraud casinos, causing massive financial losses. Damage to the brands
of both the casino and the playing card manufacturer also occurs when these losses occur.

Players use any perceived instance of breach of game integrity to request money from
a casino. Gaming regulatory agencies may also institute penalties against a casino for a
breach of game integrity.

20 Playing card manufacturers use various coding, packaging, storage and tracking
means to ensure integrity throughout the manufacturing process. Examples include using
random number generators to randomly shuffle cards together so the casino doesn't have to.

Casinos use various procedures to try and ensure the security and integrity of the
playing cards using a combination of human beings, machinery and procedures. Every
25 interaction with human beings actually creates an additional point of risk in the case of

unscrupulous individuals; and a point susceptible to human error or oversight. Procedures rely on human intervention and control, so provide limited security. Machinery, such as automated deck checkers and shufflers are also susceptible to failure and introduce human intervention.

5 This invention eliminates the security risks that occur throughout the playing card value chain. One example is the ability for cards to be replaced and/or reordered in the pack without the casino's knowledge. The invention also prevents a card from being used more than once or from being transferred from one pack or table and used on another. The invention also eliminates the need for expensive and labor intensive management of cards
10 before and after game play and the need for physical destruction of them.

SUMMARY OF THE INVENTION

By using known methods of printing individual playing cards, applying unique individual identifiers, storing, encrypting and reading data together in a unique way with
15 electronic table gaming devices such as dealing shoes and automatic shufflers, security can be ensured. The concepts disclosed herein can be applied to deck sizes containing any number of cards, including but not limited to deck sizes of 52, 104, 208, and up to 520 or more.

Individual cards receive a unique mark or code referred to as a serial code, allowing each to be tracked thru multiple systems both in manufacturing and game play. The unique
20 individual identifiers could be numbers, letters, bar codes, QR codes, 2D or 3D codes or any other marks to make each card unique. The individual identifiers can be stand alone or can be combined with other information that is desired such as card rank and suit, casino property, card color or design, production details etc.

The individual identifiers on each card are read as the cards are assembled into the
25 decks. The various identifiers are captured to a data source and encrypted into a deck

identification number, code or mark, and associated file. The encryption can be done via a private key (Kpriv). There are multiple methods or algorithms for encryption, including but not limited to AES256 and SHA256. The deck identification file or data is then associated with the physical deck of cards using a smart card, RFID chip, SD card, or any other
5 electronic data storage device or file. For example, a dual-interface card, a contactless card, a CR-80 8-pin card, a SIM/SAM card, or a keychain card may be used. This is referred to as the activation device. The activation device will be discussed herein in the context of a data card, although it should be recognized that other forms of activation devices could be used.

The data card travels with the deck of cards. It could be inside the deck in the form of
10 a cut card or special card, or in or on the pack in any manner. Once at the casino, the data card is queried by a central server, or a device at the point where integrity of the cards needs to be verified. Such points could include an inventory management scanner, dealing shoe, shuffler, storage device or other piece of equipment.

When encrypted, the data card file is queried using a Device Key (Kdev). The device
15 key works to read the data and determine if a match to the expected information exists. As cards are examined or read by a device such as a playing card dealing shoe, there is a check for the individual identifiers and the data card is queried to validate a match. If a match is not found, the device would stop, lock, alarm, send a signal or alert or the like to indicate a mismatch. Thus, as each card is pulled, the system verifies the information on the playing
20 card to a matching serial number from the data card before the value of the card is considered or identified by the device.

For additional security the data card can be set to read each individual serial code only once to ensure the cards can only be used once. However, if cards are to be reused, the card deactivation features can be adjusted accordingly. For yet another level of security, the data
25 card can contain the exact sequence of the deck.

A casino may destroy the data card or the device may erase the data card, making the reading of the associated playing cards by the device impossible.

In view of the above, in accordance with an aspect of the present disclosure, there is provided a method comprising the steps of: generating and assigning a random number to
5 each playing card in a deck of playing cards, wherein the said random number for a playing card contains no indication of the rank or suit of the playing card; applying the random number associated with a said playing card on said playing card; recording, to a digital memory device associated with the deck, each random number associated with each said playing card in the deck, with the order in which each playing card appears in the deck, to
10 create a data file thereof; and providing the data file to a purchaser of the deck.

In accordance with another aspect of the present disclosure, there is provided a method comprising the steps of: placing a deck of playing cards in a playing card handling device, wherein each playing card in the deck is printed with a randomly generated number thereon; associating, with the deck in the playing card handling device, a data file containing
15 the random numbers associated with each playing card in the playing card handling device, along with order information of an order in which each playing card appears in the deck; reading the random number printed on a said playing card as the playing card is drawn from the playing card handling device; determining whether drawn playing card is expected based on the random number read from the drawn playing card as compared to the order
20 information stored in the data file; allowing play to continue normally when the drawn playing card is expected; and signaling an alert when the drawn playing is not expected.

In accordance with yet another aspect of the present disclosure, there is provided a system comprising: a deck of playing cards, wherein a randomly generated number is applied on each said playing card in the deck; an activation device containing a data file of each
25 randomly generated number of the playing cards in the deck, and the order of each playing

card in the deck; a playing card handling device for receiving the deck of cards therein, wherein the playing card handling device includes a sensor for detecting the randomly generated number on a said playing card as the said playing card is drawn from the playing card handling device; and wherein the playing card handling device is associated with a processor, wherein said processor: is in communication with the sensor and the activation device to receive information therefrom; determines whether a playing card drawn from the playing card handling device is expected an expected playing card based on the information from the sensor and the activation device; and disables the playing card handling device when the drawn playing card is not the expected playing card.

10

DESCRIPTION OF THE DRAWINGS

For a better understanding of the various embodiments of the present invention, reference may be made to the accompanying drawings in which:

Fig. 1 is a perspective view of a playing card dealing shoe and deck of cards, with an example data card in accordance with one embodiment;

15

Fig. 2 is an example playing card showing one or more example position(s) for a data track thereon in accordance with one embodiment;

Fig. 3. is a chart showing an example set of data for inclusion on a data card in accordance with an example embodiment.

Fig. 4A is a flow diagram of an example method for encrypting data to be saved to a data card in an example embodiment.

20

Fig. 4B is a flow diagram of an example method for decrypting data read from a data card in an example embodiment.

Fig. 5 is a flow diagram of an example method for creating and using playing cards and a data card in an example embodiment.

25

While the disclosure is susceptible to various modifications and alternative forms, a specific embodiment thereof is shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that the drawings and detailed description presented herein are not intended to limit the disclosure to the particular
5 embodiment disclosed, but to the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present disclosure as defined by the appended claims.

DETAILED DESCRIPTION OF THE INVENTION

The invention will now be described with reference to the drawing figures, in which like reference numerals refer to like parts throughout. For purposes of clarity in illustrating the characteristics of the present invention, proportional relationships of the elements have not necessarily been maintained in the drawing figures.

Referring to the drawings, Fig. 1 illustrates a playing card dealing system 100. This system 100 includes a playing card handling device 105 that contains a deck of playing cards 110. The playing card handling device 105 may be a dealing shoe in an example embodiment. For ease of reference, playing card handling device 105 will be referred to hereinafter as a shoe 105. In addition to illustrating the deck 110 in the shoe 105, Fig. 1 also illustrates the deck 110 exploded from the shoe 105. Deck 110 may be a standard fifty-two card deck. However, as shown, deck 110 is a superdeck comprised of eight standard decks for a total of 416 cards. Other deck sizes are also envisioned as per casino preferences.

As can best be seen in the exploded deck 110, the deck 110 may contain a data card 115. The data card 115 is preferably an electronic memory storage device, which is generated and used for a specific deck 110, as will be further discussed below. The data card 115 itself could be created from various technologies, including smart card technologies or the like. For example, a smart card with RFID technology would allow the data card 115 to be written or read without physical electrical connections. Fig. 1, for example, illustrates an embodiment in which the data card includes RFID technology. The data card 115 merely needs to be in proximity to a reader antenna on the shoe 105 for the shoe 105 to read the data card 115. Therefore, the data card 115 can be used as a cut card or the like. However, the data card 115 need not be associated with actual gameplay.

Wireless read/write functionality is optional. When the data card 115 is written, the card could be put into a fixture that provides electrical connectivity. Similarly, in the casino, the data card 115 could be physically inserted into a shoe 105 or another electronic device associated with the shoe 105, providing electrical connectivity (not shown in Fig. 1). Thus, any type of digital memory device or card could be used, as desired. Alternatively, the contents of the digital memory device could be communicated to the casino electronically, such as via the Internet. In such an embodiment, a physical data card may be avoided.

RFID technology has some advantages, though. The antenna-based coupling of RFID technology is more tolerant of mechanical misalignment than electrical contacts. For example, the data card 115 could be inserted into the shoe 105 in any possible orientation and still be successfully read. Another potential advantage is that an RFID-based data card 115 could be read (or written to) while the data card 115 remains within a factory-sealed box. This could allow for a casino process in which a deck 110 that still has a factory seal intact is loaded into a shoe 105.

There are various types of RFID technologies on the market, each of which have specific advantages and disadvantages as would be recognized in the art. For example, some technologies allow data rates of 106 Kbps. Given data size estimate of less than 4 KB, writing time would be short relative to an example 18 second manufacturing cycle time. Additionally, certain RFID technologies are fairly short in range. Although longer range RFID may have some benefits, shorter range RFID technologies are preferred to help prevent the shoe 105 of an adjacent table from accidentally reading a different table's data card 115. In order to help prevent shoe-to-shoe cross reading, the spacing between the data card 115 and the reader antenna of a shoe 105 should be low. In an example embodiment, the spacing between two shoes 105 ("D") is between about 10 and 100 times greater than the distance between the data card 115 and the reader antenna of the shoe 105 ("d"), such that $D \gg d$.

The deck 110 itself will now be discussed in additional detail in connection with Fig. 2. Fig. 2 illustrates a playing card 200. As with any standard playing card, playing card 200 includes an indicator of rank 205 and suit 210, along with a design 215 on the face of the card 200. However, playing card 200 also includes at least one data track 220. Multiple data
5 tracks 220 may be used for redundancy. A data track 220 may include encoded information that is machine readable and identifiable.

US Patent No. 8,657,287 and related family (the disclosure of which is hereby incorporated by reference) disclose techniques for encoding rank and suit on a playing card, and then reading the encoded information from the playing card when the card is drawn from
10 a shoe. However, a data track 220 in accordance with the teachings hereof may include additional information besides rank and suit information. For example, a random number is preferably included in a data track 220. This number, referred to herein as a serial number or “SN” is not related to the playing card suit or value. Preferably, a new random SN is generated for every playing card 200 upon creation.

15 A SN may, in an example embodiment, be a 32-bit number. The SN on each playing card preferably supports at least 1 billion unique values. A serial number of at least 30 bits is therefore preferred (for at least 1 billion values), but 32 bits is generally easier to implement in a digital memory system. Including the rank and suit generally entails an additional six bits (to account for 52 possibilities). Additional bits may also be included for error detection
20 and/or correction, as well as lead-in or preamble bits.

The data track 220 may be one-dimensional (akin to a barcode), two-dimensional (as in US Patent No. 8,657,287 and related family), three-dimensional codes, or the like. A one-dimensional self-clocking data track 220 may also be used, such as via a Manchester encoding scheme, differential Manchester encoding, or Biphase Mark Code. Such a data
25 track 220 could be printed on the top and/or bottom of a playing card 200 as shown in Fig. 2.

One dimensional data tracks 220 are preferred because they allow for the use of a much simpler camera or sensor to detect the bits as they move past. In Fig. 2, the size of the data track 220 is exaggerated to better show the concept. The data tracks 220 may be much smaller so that the draw speed of the card is fairly constant over the length of the data read.

- 5 When the data tracks 220 are small compared with the width of the card, the speed remains relatively consistent as the card is pulled.

A number of techniques for error detection and data correction could be used, as are known in the art. For example, CRC (cyclic redundancy check/correction) techniques calculated over the entire data track 220 could be used. Similarly, error correction codes
10 exist that allow both detection and correction of one or more bit errors.

Preferably, the data track 220 is applied on the playing card 200. Such application may occur by printing with an ink, or laser etching, or the like. For example, a low visibility ink may be used, such as by using yellow (on a white background), infrared, or ultraviolet ink. Similarly, the data track 220 is preferably printed so as to be small while still achieving
15 reliable detection. The height of a data track 220 is preferably tall enough to compensate for any misalignment and/or slop. Small data tracks 220 also help to preserve the visual aesthetic of playing card 200. Further, making the data track 220 hard to see or discern with the naked eye helps to obfuscate the encoded rank and suit of the card in the data track 220, if present.

Fig. 3 illustrates example data content 300 of a data card 115. As each card 200 in the
20 deck is assigned with a random SN, the data card 115 is loaded with the SN information of each card 200 in its associated deck 110 at the time of factory shuffling. Data card 115 therefore contains a list of the SNs of each card 200 and their order in the deck 110. Fig. 3 illustrates this sequence of SNs as numeral 305. In an example embodiment, the rank and suit information is also loaded into the data card 115, although in a preferred embodiment the
25 rank and suit information is not loaded into the data card 115. In addition, a deck ID 310, a

casino ID 315, a time/date code 320, and/or error detection/correction bits may also be added into the data card 115. In an example embodiment, the data card 115 may hold at least 1.64 KB of data, although 64 bit SNs would lead to a data card 115 that holds at least 3.28 KB of data.

5 A digital signature may also be included as an obstacle against counterfeiting. Other techniques include encryption and other security measures. With random SNs that are independent of the playing card face value, encryption of the SN data is less important because knowledge of the SNs would not give a player an advantage in the game. However, cryptography concepts may still be utilized in the data stored within a data card 115 and the
10 shoe 105. For example, authentication provides the identification of a message originator. This could be used to validate that the data card 115 was created at a proper facility. A security service that can identify any alteration(s) in the message data may also be used. Encrypted data could also make it more difficult to hack the interface between a data card 115 and a shoe 105.

15 If no cryptography is used, data integrity of the data card 115 could be verified using simple CRC data 325 appended to the end of the data in the data card 115, as shown in Fig. 3. However, adding a digital signature to the data card 115 immediately adds capability for authentication and enhanced data integrity checks of the data card 115 data. In an example embodiment, a digital signature is generated by combining the SNs 305, deck ID 310, casino
20 ID 315, time/date code 320, and CRC data 325 into a unique hashed message digest. This digest may then be passed, along with a private key, into a Digital Signature Algorithm (DSA) to generate a unique digital signature. The private key (Kpriv) would remain with the card manufacturer.

 Later, when put into use, the casino could also then take the SNs 305, deck ID 310,
25 casino ID 315, time/date code 320, and CRC data 325 and perform a hash operation to

generate a digest. The casino would then use a corresponding public key and the same DSA to verify that the digital signature was created at an authorized facility. If the digital signature is valid and/or the CRC data is validated, the casino knows that the data in the data card 115 is legitimate.

- 5 Encryption may also or alternatively be used to add confidentiality to the data card 115 data. It is possible to encrypt (at the factory) and decrypt (in the casino) the original plaintext message. In any example embodiment, this process could use a symmetric key to both encrypt and decrypt the message. This encryption would make it harder for hackers to generate their own data cards 115 because it would require knowledge of the symmetric key.
- 10 The symmetric key (K_{sym}) known to the casino in the shoe would not be made available to the general public, and would need to be protected. Figs. 4A and 4B illustrate example methods 400A and 400B for implementing digital signature and encryption/decryption techniques for the data 300 on a data card 115.

- In Fig. 4A, the original plaintext message 305 (which, again, includes the SNs 305 and any deck ID 310, casino ID 315, time/date code 320, and CRC data 325) is designated "M." The original plaintext message 305 is sent to an encryption system 405 that uses a symmetric key " K_{2sym} " to encrypt the original plaintext message 305 into an encrypted plaintext message "E." The encrypted plaintext message E then becomes part of the data 300 on data card 115. The original plaintext message 305 is simultaneously sent to a hash
- 15 function 410 to create a digest 415. Hash function 410 may be a one-way function that takes variable length data to create a fixed length output in the form of digest 415. Changing the input data in any way would change the output 415 of the hash function 410. The digest 415 is then sent to a Digital Signature Algorithm "DSA" that uses a private key " K_{1priv} " to create digital signature "DS." The digital signature is then added to the encrypted plaintext message
- 20 E as data 300 on the data card 115.

In Fig. 4B, the data 300 on data card 315 is decrypted to validate the contents. The encrypted plaintext message E is sent to for decryption at 425 using the symmetric key “ K_{2sym} ” back into original plaintext message 305 (“M”). The original plaintext message 305 can then be passed again to a hash function 430 to create a digest 435. This digest 435, along
5 with the digital certificate DS are passed to another Digital Signature Algorithm “DSA” 440 that uses a public key “ K_{1pubv} ” to validate the digital signature DS at step 445.

In another example embodiment, digital certificates and Public Key Infrastructure (PKI) may be used to authenticate both sides of a communication link. PKI utilizes a network connection to a Certificate Authority (CA), which is used during a handshake
10 process to identify and verify the other end of a communication link. For example, the casino would communicate to a server to validate a deck ID 310. The casino would use PKI to create that communication connection. It will be understood that present and future encryption techniques are envisioned, including techniques not yet created.

Fig. 5 illustrates a process 500 for validating playing cards according to an example
15 embodiment. At step 502, a sheet of playing cards 200 is printed. At step 504, a random SNs is generated and assigned to each card 200, as discussed above. Each respective SN is printed on its respective card 200. At step 506, the SNs on the cards 200 are verified. Cards with bad SNs are rejected. At step 508, the cards 200 are cut and punched from the sheet. At step 510, the cards 200 are shuffled and collected into a deck 110. At this point, the cards
20 200 may again be checked for bad SNs, using a sensor. The sensor may, in an example embodiment, be a vision system such as a high speed camera, or a barcode scanner or the like. At step 512, the SNs from all cards in the deck are read, and at step 514 the number of cards in the deck is verified. Simultaneously, at step 516, the SN numbers and any other selected information are sent through a digital certificate and/or encryption system (e.g., a
25 system operating method 400A above) if such a step is desired.

At step 518, a data card 115 is created containing the SNs and any other data as discussed above, either as encrypted data or otherwise as desired. At step 520, the data card 115 is placed with the deck 110, and at step 522 it is verified that the data card 115, deck 110, and box match. At step 524 the box is sealed, labeled, and shrink-wrapped with the data card 115 inside. At step 526, after shipping to the casino, the sealed box is stored securely. At step 528, the box is opened and the deck 110 and data card 115 are loaded into a device such as a dealing shoe 105. The shoe 105 reads the data card 115 at step 530, which effectively “activates” the deck 110 for play. The contents of the data card 115 are validated and/or unencrypted at step 532 (e.g., as shown above in method 400B). This validation step may occur within the shoe 105 if onboard processing is sufficient. Alternatively or in addition, the shoe 105 may be in communication with a casino server, and the casino server may perform any necessary processing steps. Once validated, at step 534, the shoe 105 erases the data card 115 to kill it. In an alternative embodiment where the data card 115 acts as the cut card and is inserted with the deck 110 into the shoe 105, the shoe 105 may detect the data card 115 at the effective end of the deck 110, and may deactivate the deck and/or data card 115 at that time.

At step 536, as a card 200 is pulled from the shoe 105, the SN is read in addition to any rank and suit information on the card 200. At step 538, the shoe 105 or casino server check the SN against the card SN and order data read from the data card 115. At step 540, if the SN itself contains bad data, an alert, alarm, or other signal is activated or the shoe locks at step 542 because of an invalid card. However, if the SN contains valid data, the process advances to step 544 at which point the shoe 105 or casino server determines whether the drawn card 200 is in the correct order. If not, the shoe 105 again locks at step 542 because of an invalid sequence. If the sequence is correct, play continues at step 546. By tracking each pulled card by SN, the cards 200 in the deck 110 may be “activated” for a single use or

multiple uses as desired by the casino. The order of the playing cards 200 drawn from the shoe 105 may be captured and stored electronically. A casino may use such a digital record to resolve game disputes. Alternatively, a manufacturer of the deck 110 may utilize the digital record to audit or prove randomness of the playing cards 200.

5 From the foregoing, it will be seen that the various embodiments of the present invention are well adapted to attain all the objectives and advantages hereinabove set forth together with still other advantages which are obvious and which are inherent to the present structures. It will be understood that certain features and sub-combinations of the present embodiments are of utility and may be employed without reference to other features and sub-
10 combinations. Since many possible embodiments of the present invention may be made without departing from the spirit and scope of the present invention, it is also to be understood that all disclosures herein set forth or illustrated in the accompanying drawings are to be interpreted as illustrative only and not limiting. The various constructions described above and illustrated in the drawings are presented by way of example only and are not
15 intended to limit the concepts, principles and scope of the present invention.

As is evident from the foregoing description, certain aspects of the present invention are not limited by the particular details of the examples illustrated herein, and it is therefore contemplated that other modifications and applications, or equivalents thereof, will occur to those skilled in the art. The terms “having” and “including” and similar terms as used in the
20 foregoing specification are used in the sense of “optional” or “may include” and not as “required.”

Many changes, modifications, variations and other uses and applications of the present constructions will, however, become apparent to those skilled in the art after considering the specification and the accompanying drawings. All such changes,
25 modifications, variations and other uses and applications which do not depart from the spirit

and scope of the invention are deemed to be covered by the invention which is limited only by the claims which follow.

CLAIMS

What is claimed is:

1. A method comprising the steps of:

generating and assigning a random number to each playing card in a deck of playing
5 cards, wherein the said random number for a playing card contains no indication of the rank
or suit of the playing card;

applying the random number associated with a said playing card on said playing card;

recording, to a digital memory device associated with the deck, each random number
associated with each said playing card in the deck, with the order in which each playing card
10 appears in the deck, to create a data file thereof; and

providing the data file to a purchaser of the deck.
2. The method of claim 1 wherein the random number is a 32-bit number.
3. The method of claim 1 wherein each random number is printed on its respective
playing card in the form of a one-dimensional data track.
- 15 4. The method of claim 3 wherein a said one dimensional data track associated with a
playing card also includes the rank and suit of the playing card.
5. The method of claim 3 wherein a said one dimensional data track associated with a
playing card also includes at least one of: a deck ID, a casino ID, a time/date code, and data
CRC bits.
- 20 6. The method of claim 3 wherein each one dimensional data track is printed using a low
visibility ink and in a low visibility size.
7. The method of claim 1 wherein the digital memory device is a data card, and the data
file is provided to the purchaser of the deck by physically providing the data card to the
purchaser.
- 25 8. The method of claim 1 wherein the digital memory device is a server, and the data file
is provided to the purchaser of the deck electronically via the Internet.

9. The method of claim 1 wherein the random number associated with each playing card is listed in the data file in an order of the playing cards in the deck.
10. The method of claim 1 wherein information stored in the digital memory device is encrypted.
- 5 11. The method of claim 1 wherein the digital memory device includes a digital certificate.
12. A method comprising the steps of:
- placing a deck of playing cards in a playing card handling device, wherein each playing card in the deck is printed with a randomly generated number thereon;
- 10 associating, with the deck in the playing card handling device, a data file containing the random numbers associated with each playing card in the playing card handling device, along with order information of an order in which each playing card appears in the deck;
- reading the random number printed on a said playing card as the playing card is drawn from the playing card handling device;
- 15 determining whether drawn playing card is expected based on the random number read from the drawn playing card as compared to the order information stored in the data file;
- allowing play to continue normally when the drawn playing card is expected;
- signaling an alert when the drawn playing is not expected.
13. The method of claim 12 wherein the playing card handling device is a dealing shoe.
- 20 14. The method of claim 13 wherein association of the data file with the deck in the shoe occurs by inserting a data card containing the data file into the shoe.
15. The method of claim 14 wherein the data card is plugged into the shoe, wherein physical contacts on the data card engage with physical contacts in the shoe to allow for electronic communication therebetween.
- 25 16. The method of claim 13 wherein association of the data file with the deck in the shoe occurs by inserting a data card containing the data file into an electronic device associated

with the shoe, wherein physical contacts on the data card engage with physical contacts of the electronic device to allow for electronic communication therebetween.

17. The method of claim 14 wherein the data card is placed into proximity with the shoe and communicates wirelessly with the shoe via an RFID device in the data card.

5 18. The method of claim 17 wherein the data card is used as a cut card among the playing cards in the deck.

19. The method of claim 12 wherein the data file is received electronically from a manufacturer of the playing card.

10 20. The method of claim 13 wherein each random number is printed on its respective playing card in the form of a one-dimensional data track.

21. The method of claim 20 wherein a sensor in the shoe reads the data track on a playing card as the playing card is drawn from the shoe.

22. A system comprising:

15 a deck of playing cards, wherein a randomly generated number is applied on each said playing card in the deck;

an activation device containing a data file of each randomly generated number of the playing cards in the deck, and the order of each playing card in the deck

20 a playing card handling device for receiving the deck of cards therein, wherein the playing card handling device includes a sensor for detecting the randomly generated number on a said playing card as the said playing card is drawn from the playing card handling device; and

wherein the playing card handling device is associated with a processor, wherein said processor:

25 is in communication with the sensor and the activation device to receive information therefrom;

determines whether a playing card drawn from the playing card handling device is expected an expected playing card based on the information from the sensor and the activation device; and

5 disables the playing card handling device when the drawn playing card is not the expected playing card.

23. The system, of claim 22 wherein the playing card handling device is a dealing shoe.

24. The system of claim 23 wherein the activation device is a data card packaged with the deck.

10 25. The system of claim 24 wherein the data card includes at least one wireless communication component.

26. The system of claim 25 wherein the at least one wireless communication component is an RFID chip.

15 27. The system of claim 23 wherein the activation device is a server in communication with the processor for providing the processor with the information from the activation device.

28. The system of claim 23 wherein the processor is positioned within the shoe.

29. The system of claim 23 wherein the processor is remote from the shoe.

30. The system of claim 24 wherein the processor is further operable to delete the data file from the data card to deactivate the deck of playing cards.