

METHOD FOR A PREPAID, DEBIT AND CREDIT CARD SECURITY CODE GENERATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to and the benefit of, U.S. Application No. 15/231,069, filed on August 8, 2016, herein incorporated by reference in its entirety.

1. Field of the Invention.

[001] This invention provides a system for generating and updating security codes for use with prepaid, debit and credit cards. Specifically, prepaid, debit and credit card security codes can be updated by a server connected to a network or by an on card algorithm such that when the card is used with a Delivery Device, new security code(s) are generated for future transactions.

2. Background.

[002] Some payment transactions are made without a payment card, such as a debit or credit card, being read by a payment device. For example, this can happen when purchasing goods from an electronic retailer. Cardholders make these so-called Card-Not-Present (“CNP”) transactions by giving their payment credentials, such as the Primary Account Number (“PAN”), Expiration Date, and security code, to a merchant (e.g., an electronic retailer) without physically presenting the card to that merchant, as opposed to Card-Present transactions where a card is swiped, dipped, or tapped (typically by the cardholder) on a payment device to read the card data and initiate an electronic payment transaction.

[003] CNP fraud can occur when valid credentials of a payment card are stolen from the genuine cardholder and then used by an unauthorized person to perform a payment transaction. These credentials can be stolen when computer systems (e.g.,

merchant accounts systems) are hacked. Theft of card credentials can also occur when unscrupulous individuals record card data while processing a payment and before returning the card to the cardholder. For example, an employee of a restaurant could write down the information printed on the plastic card of a patron while processing the payment.

[004] Payment card companies use various security codes to combat fraud. Security codes, such as the Card Validation Code 2 (CVC2) and the Card Verification Value 2 (CVV2), were introduced by payment card companies specifically to address CNP fraud. These security codes are used as simple static passcodes to help ensure the genuine card is present at the moment of a CNP transaction. These codes can be printed on the back of a card (e.g., on the card's signature panel), but they can also be printed on the front of the card.

[005] Although thieves are now forced to copy an additional piece of information to be able to perform fraudulent transactions, the last few years have seen ever growing levels of CNP fraud. This happened despite the attempts of most of the payment card companies to secure these security codes (e.g., by printing them on the back of the card to force thieves to copy both side of the card, by making the imprint difficult to read from a certain distance, or by forbidding merchants from storing those security codes on their systems, even temporarily).

[006] In addition to the direct cost of fraudulent transactions, CNP fraud generate additional costs related to the management of fraud cases by issuers and merchants, and also by forcing issuers to issue new cards as a replacement for the counterfeited ones.

[007] There already exist cards that can change their security code on a regular basis. These time-based products use a built-in electronic circuit with a real-time clock and a battery to calculate a new security code after a pre-determined length of time and show it on an electronic display embedded in the card. However, these solutions have a number of drawbacks: the real-time clock and the battery make the cards more fragile, the battery makes the card more expensive and limits its lifetime, and the time-based mechanism using the on-card clock makes it prone to de-synchronization with the server.

Therefore, a need exists for a solution that allows for the security codes on cards to be changed during the lifetime of the cards that is cheaper, more robust, and more reliable than existing solutions.

[008] The benefits of such a solution would be two-fold: first, keeping a solution based on security codes would avoid the need to change or replace the existing card payment infrastructure; second, changing the value of these security codes significantly decreases the possibility of fraudulent activity.

SUMMARY

[008a] According to a first aspect of the present invention, there is provided a method for generating a security code for a card on a transaction event basis, the card having a display and no internal electrical battery power, comprising the steps of:

- (a) during each transaction using the card, performing at least the following:
 - (1) interfacing the card with an external electrical power source associated with a delivery device;
 - (2) after and while providing electrical power to the card from the external electrical power source, performing at least the following:
 - (i) transmitting a request for transaction authorization approval from the card to the delivery device connected to a network;
 - (ii) transmitting the request for transaction authorization approval from the delivery device to the network;
 - (iii) validating the request for transaction authorization approval by the network;
 - (iv) generating a new security code at a generator server and inserting the new security code into a transaction script;
 - (v) transmitting the transaction script from the network to the delivery device;
 - (vi) transmitting the transaction script from the delivery device to the card; and
 - (vii) retrieving the new security code from the script in the card.

[008b] According to a second aspect of the present invention, there is provided a method for generating a plurality of security codes for a card on a transaction event basis, the card having a display and no internal electrical battery power source, comprising the

steps of:

- (a) during each transaction using the card, performing at least the following:
 - (1) interfacing the card with an external electrical power source associated with a delivery device;
 - (2) after providing electrical power to the card from the external electrical power source, performing at least the following:
 - (i) transmitting a request for transaction authorization approval from the card to the delivery device connected to a network;
 - (ii) transmitting the request for transaction authorization approval from the delivery device to the network;
 - (iii) validating the request for transaction authorization approval by the network;
 - (iv) generating a plurality of security codes from a generator server and inserting the plurality of security codes into a transaction script;
 - (v) transmitting the transaction script from the network to the delivery device;
 - (vi) transmitting the transaction script from the delivery device to the card; and
 - (vii) retrieving the new security codes from the script in the card.

[008c] According to a third aspect of the present invention, there is provided a method for generating a security code for a card on a transaction event basis, the card having a display and no internal electrical battery power source, comprising the steps of:

- (a) during each transaction using the card, performing at least the following:
 - (1) interfacing the card with an external electrical power source associated with a delivery device;
 - (2) while interfaced, performing at least the following:
 - (i) receiving electrical power from the external electrical power source;
 - (ii) after receiving the electrical power from the external electrical power source, transmitting a request for transaction authorization approval from the card to the delivery device, thereby causing the request for transaction authorization approval to be transmitted from the delivery device to a remote generator server;
 - (iii) receiving a transaction script from the remote generator server that has a new security code in the transaction script; and

(iv) retrieving the new security code from the transaction script.

[008d] There is provided a method for generating a security code for a card, comprising the steps of:

transmitting a request for transaction authorization approval from a card to a delivery device;

validating the request for transaction authorization approval by the delivery device;

transmitting an outcome response to the request for transaction authorization approval from the delivery device to the card; and

generating the new security code on the card.

[008e] There is provided a method for generating a plurality of security codes for a card, comprising the steps of:

transmitting a request for transaction authorization approval from a card to a delivery device;

validating the request for transaction authorization approval by the delivery device;

transmitting an outcome response to the request for transaction authorization approval from the delivery device to the card; and

generating a plurality of new security codes on the card.

[008e] There is provided a method of display a security code for a card, comprising the steps of:

transmitting a request for transaction authorization approval from a card to a delivery device;

validating the request for transaction authorization approval by the delivery device;

transmitting an outcome response to the request for transaction authorization approval from the delivery device to the card;

selecting one of the security codes from security codes stored in the memory area;
and

displaying the one security code selected from the security codes on a display embedded in the card.

[009] There is disclosed a comprehensive “Dynamic Security Code” (“DSC”) System (“DSC System”) that can change the security code of a prepaid, debit, or credit card (“Payment Card”). In an effort to thwart Card-Not-Present (“CNP”) fraud, the DSC System provides dynamic security code values (“DSC Values”) that can have a limited use. When needed, another DSC Value will be generated by a DSC Generator Server on a network or generated by the microprocessor embedded in the DSC card. The DSC card can also be used with existing standard payment card infrastructures. In addition, the DSC System can be used with other form factors and in other environments not related to payments such as balance inquiries.

[010] When a DSC Value needs to be validated by the Issuer, it can be sent to the Issuer’s DSC Validator Server (“DSC Validator Server”) using the same channels as the ones used for traditional static security codes. For example, when a Cardholder uses a web browser to manually enter the DSC Value in lieu of the static security code into the electronic form provided by a merchant or into the registration form provided by an online or mobile wallet provider.

[011] In one embodiment of the invention, DSC Values are generated by a DSC Generator Server. When needed, the DSC Generator Server will calculate one or more new DSC Values for a specific DSC Card. Examples include, but are not limited to the Issuer’s EMV authorization processing performed during a payment transaction, a purchase transaction, a purchase transaction with cash advance, an account status inquiry,

a PIN change transaction, a cash withdrawal. However, it could also be done during a card management transaction or any other interaction between the DSC Card and the Issuer.

[012] When DSC Values are generated by a DSC Generator Server, they can be delivered to the DSC Card by embedding them in an EMV script contained in the Issuer's authorization response message, but the DSC Values could also be sent in other types of messages during any other interaction between the DSC Card and the Issuer.

[013] In another embodiment of this invention, DSC Values are generated by the DSC Card itself. When needed, the DSC Card will calculate one or more new DSC Values. Typically, this can be done when the DSC Card is processing an EMV transaction in a POS or ATM terminal.

[014] Other systems, methods, features, and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims.

DETAILED DESCRIPTION OF THE DRAWINGS

[015] The components in the figures are not necessarily to scale, emphasis being placed instead upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[016] Figure 1 is a side view of a card illustrating visible aspects of one side of a typical prepaid, debit or credit card.

[017] Figure 2 is a side view of a card illustrating visible aspects of card data on one side of a prepaid, debit or credit card.

[018] Figure 3 is a block diagram of the internal hardware components in a prepaid, debit or credit card that can receive periodic updated security code information.

[019] Figure 4 is a flow chart of data movement in a prepaid, debit or credit card transaction where the security code is periodically updated.

[020] Figure 5 is a flow chart of data movement in a prepaid, debit and credit card transaction in a Card-Not-Present operating environment.

[021] Figure 6 is a flow chart of data movement in prepaid, debit and credit card transactions with the 3D secure functionality.

DETAILED DESCRIPTION

[022] This invention is a comprehensive “Dynamic Security Code” (“DSC”) System (“DSC System”) that can change the security code of a prepaid, debit, or credit card (“Payment Card”). In an effort to thwart Card-Not-Present (“CNP”) fraud, the DSC System provides dynamic security code values (“DSC Values”) that have a limited use. The DSC Values provided by this DSC System can be calculated by various methodologies and can be used within existing standard Payment Card infrastructures. The DSC System can also be used with other form factors and in other aspects not related to payments such as balance inquiries.

[023] In existing systems that use security codes with static values, the bank or other institution issuing a Payment Card (“Issuer” or “Card Issuer”) provides the static value of a card’s security code only once to its holder (“Cardholder”) typically, by printing it on the back of the plastic card. With the DSC System, new DSC Values can be calculated by a DSC Generator Server (“DSC Generator Server”) and delivered to a card (“DSC Card”) when it is communicating with the Issuer, or they can be calculated by the DSC Card itself.

[024] When a DSC Value needs to be validated by the Issuer, it can be sent to the Issuer’s DSC Validator Server (“DSC Validator Server”) using the same channels as those used for traditional static security codes. For example, when a Cardholder uses a web browser to manually enter the DSC Value in lieu of the static security code into the electronic form provided by a merchant or into the registration form provided by an online or mobile wallet provider.

[025] In one embodiment of the invention, DSC Values are generated by a DSC Generator Server. When needed, the DSC Generator Server will calculate one or more

new DSC Values for a specific DSC Card. Examples include, but are not limited to the Issuer's EMV authorization processing performed during a payment transaction, a purchase transaction, a purchase transaction with cash advance, an account status inquiry, a PIN change transaction, a cash withdrawal. However, it could also be done during a card management transaction or any other interaction between the DSC Card and the Issuer.

[026] When DSC Values are generated by a DSC Generator Server, they can be delivered to the DSC Card by embedding them in an EMV script contained in the Issuer's authorization response message, but the DSC Values could also be sent in other types of messages during any other interaction between the DSC Card and the Issuer.

[027] In another embodiment of this invention, DSC Values are generated by the DSC Card itself. When needed, the DSC Card will calculate one or more new DSC Values. Typically, this can be done when the DSC Card is processing an EMV transaction in a POS or ATM terminal.

[028] There are multiple algorithms that can be used to generate DSC Values and they can encompass various forms of data, such as system configuration data, card data, and transaction data. In all embodiments of this invention, including when the DSC Validator Server supports several algorithms, the generation and the validation of DSC Values should be done with the same algorithm.

[029] In all embodiments where the generation of DSC Values is done while performing other card-related processing, this generation should not be tied to the outcome of that specific processing. For example, if the generation of DSC Values is done during the processing of an EMV transaction, these values can be delivered to the DSC Card, whether the transaction is accepted or declined.

[030] A Delivery Device may mean any electronic device capable of transmitting power and data to a DSC Card. This can be done through standard interfaces compliant with IS 7816 ("Contact Interface"), IS 14443, IS 15693, IS 18092, IS 21481 ("Contactless Interface"), or any other interface supported by the DSC Card. Examples of a Delivery Device include, but are not limited to an EMV Point-of-Sales ("POS") terminal, an EMV Automated Teller Machine ("ATM") terminal, an EMV Cardholder

Activated Terminal (“CAT”), an EMV Automated Fuel Dispenser (“AFD”) terminal, a smartphone or mobile device with NFC capabilities (whether built-in or through the use of an add-on), a dedicated bank branch terminal, a personal computer (e.g., desktop, laptop, or tablet) equipped with a contact or contactless chip card reader (whether built-in or through, the use of an add-on).

[031] When used on a Delivery Device, a DSC Card can update its display using a DSC Value received from the DSC Generator Server, stored in the DSC Card’s memory, or generated on the DSC Card itself. Based on their preferences, Issuers can decide on different update strategies. For example, Issuers may decide to have the DSC Card update its display each time it is used on a Delivery Device or for a certain type of transaction, or based on more complex decision criteria using contextual information including, but not limited to card state, transaction data, risk management considerations.

[032] In one embodiment of this invention, a DSC Value can be used for a CNP transaction next to other card credentials, such as the PAN and Expiry Date, in lieu of a static security code. The DSC Validator Server will then validate the DSC Value and share the outcome of the validation with the Issuer’s system as part of the CNP transaction processing.

[033] In another embodiment, a DSC Value can be used as part of a regular Card-Present transaction such as in a consumer electronics store, as an additional security step of the transaction. Similarly to the CNP case, the DSC Value will be validated by a DSC Validator Server.

[034] In all embodiments, DSC Values can be transmitted to the DSC Validator Server using the same channels and interfaces as the ones used to transmit the regular static security codes, such as the Card Validation Code 2 and the Card Verification Value 2.

[035] Figure 1 is a side view illustrating visible aspects of one side of a DSC Card 100 that may have the outward appearances of a traditional Payment Card with a PAN, Expiration Date, name of an individual, company printed on the card. The DSC Card 100 may also have a logo of card issuer, an issuing bank, merchant, etc. (not shown.). Also located on the DSC Card 100 may be a magnetic stripe 102, a signature

area 104, a hologram 106, a display 108, or printed card issuer contact information (not shown.). However, with the exception of the display 108, internal electronic hardware may be hidden within laminated sheets of plastic, metal, or any other types of material.

[036] On prior art Payment Cards, a security code may be printed on the card. For DSC Cards 100 that can change their security codes, a display 108 may be incorporated into the laminated structure of the card. For optimum results, this display 108 may be flexible, such as an electronic paper display, so that it can handle the stresses generated by card use, while also having the capability of displaying different codes or information related to the card and its use. The display 108 may be configured for one or more digits and may support the use of characters as part of the security code or information displayed to the cardholder.

[037] Figure 2 is a side view of a DSC Card illustrating visible aspects of card data on one side of a Payment Card. Some DSC Cards 200 show the card data on one side of the card. In this embodiment, the PAN 202, the validity date range or expiration date 204, and/or the Cardholder's name 206 can be listed on one side of the card. In addition, less critical information such as the starting date 208 the cardholder started with a particular card issuer may also be listed. Likewise, on the same side of the DSC Card 200, a security code field 210 may be shown in a flexible display such as an electronic paper display so that it can handle the stresses generated by card use. Once again, the display 210 may be configured for the display of one or more digits and may support the use of characters as part of the security code or information displayed to the cardholder.

[038] Figure 3 is a block diagram illustrating the internal hardware components of a DSC Card 300. The DSC Card 300 can have a Flexible Printed Circuit ("FPC") 302. The FPC module 302 can have a microprocessor 304, a display 306, a first antenna 308, and potentially other electronic components including, but not limited to resistors and capacitors. The microprocessor 304 may alternatively be a microcontroller. Also, the microprocessor's functionality may be performed by an embedded secure chip 310 that can be either a secure microcontroller or equivalent processing capabilities with internal memory or access to a memory location (not shown). Likewise, the functionality

performed by the microprocessor 304 may be implemented with multiple hardware components.

[039] A memory storage area embedded within the microprocessor 304 may store information for the DSC Card 300 or the memory location may be an off chip memory area that is connected to the microprocessor 304. Also connected to the microprocessor 304 is a display 306. The display 306 may be constructed of a material that allows the display to flex when the DSC Card 300 is bent without causing the display to fail. The DSC Card 300 may be configured so data other than DSC Values may be shown on the display 306, such as a one-time password, the financial balance of the card available to the cardholder, an error message, the number of electronic tickets or vouchers remaining, or other messages providing information to the cardholder.

[040] The microprocessor 304 may also be connected via a plurality of electrical connections and/or communication buses 316 to the embedded secure chip 310 thus allowing for the transfer of power and data. Currently, five electrical connections and/or communication buses 316 link the embedded secure chip 310 to the microprocessor 304 (e.g., two connections are for power, two are for data, and one is for a reset function).

[041] The FPC 302 inside the DSC Card 300 can be assembled into a thin flexible package called a prelamine 322 (i.e., card state prior to lamination). The prelamine 322 is typically a sheet of plastic (or metal, composite material, or any other material) that can be laminated between two sheets of plastic, metal, composite, or any other material to form the final version of the DSC Card 300. The prelamine 322 can include the FPC 302, a second antenna 314, electrical connections 316, an embedded secure chip 310, and other components of the DSC Card 300. The DSC card can be formed from a FPC 302 encapsulated between two laminated blanks formed from plastic materials, composite materials, metal, metal alloys, or ceramic materials.

[042] When the Contact Interface of the DSC Card 300 is used with a Delivery Device ("Contact Mode"), the DSC Card 300 receives its power and can transmit and/or receive data via the ISO contact plate 312 that connects the Delivery Device and the DSC Card's embedded secure chip 310. The embedded secure chip 310 and ISO contact plate 312 can be assembled into a package called a module 320. The contact connection

between the DSC Card's embedded secure chip 310 and the Delivery Device can also provide the pathway for the transmittal and reception of data between the Delivery Device and the FPC 302.

[043] When the Contactless Interface of the DSC Card 300 is used with a Delivery Device ("Contactless Mode"), the DSC Card 300 receives its power and can transmit and receive data via one or more antennae. In one embodiment, only one antenna, 308 or 314, may be used to provide power to the FPC 302. The same antenna 308 or 314 may also provide the communication path for exchange of data between the Delivery Device and the FPC 302. In another embodiment, both antennae 308 and 314 can be used to provide power and/or the communication path for the exchange of data between the Delivery Device and the FPC 302.

[044] In all embodiments, and for both the Contact and Contactless Modes, the DSC Card 300 is powered by a power source that is not embedded within the DSC Card 300. Typically, this power source is the Delivery Device.

[045] In all embodiments where new DSC Values are generated by a DSC Generator Server, and for both the Contact and Contactless Modes, the new DSC Values are transmitted to the DSC Card 300 by a Delivery Device (e.g., in an EMV Script Tag 71 or 72, or some other suitable transport mechanism). During a transaction in Contact Mode, the DSC Values are received through the Delivery Device and the ISO Contact Plate 312 connection. During a transaction in Contactless Mode, the DSC Values are received via the first antenna 308 and/or second antenna 314.

[046] In one embodiment, the DSC Card 300 itself can generate new DSC Values. When the DSC Card 300 is powered by a Delivery Device, for both the Contact and the Contactless Modes, the microprocessor 304 can generate one or more new DSC Values by using a predefined algorithm and input data coming from a memory location 318 accessible by the embedded secure chip 310 or microprocessor 304 (e.g., cryptographic keys, card credentials, payment application data, and/or configuration data) and/or data coming from the Delivery Device. Microprocessor 304 can handle the functionality of the embedded secure chip 310, the security code generation and the display driver in either a single chip or dual chip architecture. Based on their

preferences, Issuers can decide on different strategies. For example, Issuers may decide to have the DSC Card generate one or more new DSC Value(s) each time it is used on a Delivery Device or a certain type of transaction is processed, or based on more complex decision criteria using contextual information including, but not limited to card state, transaction data, risk management considerations.

[047] In all embodiments, and when the DSC Card 300 is used with a Delivery Device to perform additional processes (e.g., to process an EMV transaction) the generation of new DSC Values should not depend on the outcome of these additional processes (e.g., new DSC Values can be generated even when an EMV payment transaction is declined or when the EMV payment transaction is approved by an offline terminal.)

[048] In all embodiments of the DSC Card 300, DSC Values – whether generated by a DSC Generator Server or by the DSC Card 300 itself – are stored in a memory location on the embedded secure chip 310 and/or in a memory location 318.

[049] In all embodiments, and when the DSC Card 300 is used with a Delivery Device to perform additional processes (e.g., to process an EMV transaction) the storage of new DSC Values should not depend on the outcome of these additional processes (e.g., new DSC Values can be stored even when an EMV payment transaction is declined or when an EMV transaction is approved by an offline terminal)

[050] Based on their preferences, Issuers can decide to issue the DSC Card 300 with or without the first DSC Value(s) stored into the card's memory. If the DSC Card 300 is issued without any DSC Value, the first DSC Value(s) can be delivered when the DSC Card 300 is used for the first time by the Cardholder with a Delivery Device. If the DSC Card 300 is issued with one or more initial DSC Values, these DSC Values can be loaded into the DSC Card's memory when it is personalized by the Issuer or personalization bureau.

[051] Once the DSC Card 300 is issued, the antennae 308 and/or 314 may be used to download and update the firmware of the microprocessor 304 or embedded security chip 310, download updated algorithms for calculating the DSC Values,

resynchronize the card with the card Issuer's network, or download an updated list of DSC Values into the DSC Card's memory.

[052] DSC Value(s) stored in the DSC Card's memory, whether generated by a DSC Generator Server or by the DSC Card itself, can be encrypted. Cryptographic key(s) stored into the DSC Card's memory, whether used to generate new DSC Values or to encrypt and decrypt stored DSC Values, can be encrypted.

[053] DSC Value(s) can be stored into devices with a form factor that is not compliant with the IS 7810's ID-1 format. Examples include other card form factors, and non-card form factors including, but not limited to, hardware tokens, key fobs, wearable devices (such as a health monitoring device), mobile applications running on smartphones. Similarly, these other form factors can also be used to generate new DSC Values.

[054] The functionality of the DSC Server described in this invention comprises of at least two modules, the generation and delivery of new DSC Values by the DSC Generator Server and the validation of DSC Values by the DSC Validator Server. The two modules may operate on the same system or may be split and operate on separate systems. The DSC Generator Server and/or the DSC Validator Server can be operated by the Issuer or by third parties, on in-house systems and/or hosted systems.

[055] Figure 4 is a flow chart of data movement in a Payment Card transaction where the DSC Value(s) can be updated based upon the occurrence of certain events, including, but not limited to an online authorization request, an online PIN change or card management transaction, a cash withdrawal. As an example implementation, a DSC Card 400 utilizes the EMV standard so that the DSC Card 400 is operable on an Online Delivery Device 402, such as a Point-Of-Sales ("POS") Terminal and/or ATM terminal. Payment transaction data processed by the Online Delivery Device 402 can be sent across the network 406 (including, but not limited to a payment service provider, an acquirer, a processor, a card scheme network) to a card Issuer 408. Typically, payment transactions include, but are not limited to data needed to request a transaction approval, a balance inquiry such as when the card is presented to an ATM terminal. In this invention, the DSC Card 400 can also use a payment transaction to send information about its state

(including, but not limited to what is showed on its electronic display, what is stored in its storage memory) back to the DSC Generator Server 410. The card Issuer 408 can approve or deny the payment transaction or the card information inquiry to the Cardholder. During the transaction processing, one or more new DSC Value(s) may be generated by the DSC Generator Server 410 and transmitted back though the network 406 (e.g., in an EMV script) to the Online Delivery Device 402. The Online Delivery Device 402 then sends the new DSC Values(s) to the DSC Card 400 for storage and/or display. After the DSC Card 400 has updated its display, it may send a message across the network 406 and back to the Issuer 408 to confirm the update of the display. This confirmation message can transmit additional data including, but not limited to the actual value that has been displayed, a reference value of the value that has been displayed, the value stored in its storage memory.

[056] As another example implementation, a DSC Card 400 utilizes the EMV standard so that the DSC Card 400 is operable on an Offline or Offline-Capable Delivery Device 404, such as a POS Terminal. Payment transaction data processed by the Offline or Offline-capable Delivery Device 404 are not sent online through the network 406. Rather, the payment transaction is authorized locally by the Offline or Offline-Capable Delivery Device 404 and the Payment transaction data may be stored in a memory location on the Offline or Offline-Capable Delivery Device 404 and later transmitted through the network 406 to the Issuer 408 for updating its transaction records and the DSC Validator records. In this implementation, no new DSC Values(s) are generated by the DSC Generator Server 410 because the DSC Card 400 will not be in communication with the card Issuer 408. However, if capable, the DSC Card 400 could generate, store, and display new DSC Value(s) or display a stored DSC Value when operated on an Offline or Offline-Capable Delivery Device 404.

[057] Based on their preferences, Issuers can decide on different strategies. For example, Issuers may decide to have the DSC Generator Server 410 generate one or more new DSC Value(s) each time it is communicating with a DSC Card 400 or a certain type of transaction is processed, or based on more complex decision criteria using contextual information including, but not limited to card state, transaction data, risk management considerations.

[058] In another embodiment, Issuers can have offline Delivery Devices query the DSC Card 400 regarding the number of DSC Value(s) remaining in a stored list in the Card 400. If the number of DSC Value(s) stored in memory on the Card 400 are at or below a predetermined number (e.g., one, two or more based on the Issuers' preference), the Delivery Device 404 can be forced to go online so that an additional DSC Value or DSC Values can be downloaded by the DSC Generator Server 410.

[059] Figure 5 is a flow chart of data movement in a CNP transaction. In such an operating environment, the chip of the DSC Card 500 is not used and instead the Cardholder enters their card information (this includes, but it not limited to the PAN, the expiration date, the Cardholder name, the DSC Value displayed by the DSC Card 500) on a mobile device, laptop, or desktop. In such CNP transactions, the cardholder can input the card data into a browser or app 502 that connects to a merchant 504. The Payment Card transaction information is sent through a network 506 to a card Issuer 508.

[060] In a CNP payment transaction, the DSC Value received by the Issuer 508, in lieu of the regular static security code, is validated by the DSC Validator Server 510. The DSC Validator Server 510 can provide different types of answers to the Issuer 508, depending on the type of DSC Value validation that is performed. For example, the DSC Validator Server 510 could provide a simple binary answer (i.e., the DSC Value is correct or not correct) or a more complex answer to the Issuer 508 (e.g., the DSC Value is contained within an acceptable range). The DSC Validator Server 510 can also respond with the regular static security value associated with the DSC Card 500's PAN and Expiry Date, and that can be used to substitute the DSC Value in the authorization request message. Once the card Issuer 508 authorizes a transaction, the transaction authorization response is transmitted back through the network 506 and on through to the merchant 504. The merchant can then alert the Cardholder via the browser / application 502 that the transaction was authorized or denied. Once the payment transaction is authorized, the Issuer 508 can recognize that the transaction was a CNP transaction and no new DSC Value is generated since the DSC Card 500 is not in communication with the Issuer 508. Similarly, the DSC Card 500 cannot generate new DSC Value(s) since it is not being used on a Delivery Device.

[061] Figure 6 is a flow chart of data movement in a CNP transaction using 3-D Secure ("3DS") functionality. DSC Card 600 information is typed into a browser or online application 602 when the cardholder uses a DSC Card 600 to conduct a CNP transaction. The Merchant 606 can check with the Registry 608 whether the DSC Card 600 supports the 3DS functionality. The Merchant 606 also transmits payment transaction data that involves a request for transaction approval. The Registry 608 is in communication with the Merchant 606, network 610 and/or Issuer 612. If 3DS is not supported, the transaction is processed as described in Figure 5. If 3DS is supported, the Merchant 606 redirect the browser or online application 602 to the Access Control Server 604. The Access Control Server 604 ("ACS") can implement a DSC Validator Server as part of 3DS' Cardholder Authentication step. Programs such as Verified By Visa and MasterCard SecureCode are examples of the implementation of the 3DS technology. The ACS 604 is in communication with the Issuer 612.

[062] When 3DS transactions are approved or denied, the card Issuer 612 does not generate any new DSC Value(s) as the transaction was previously identified as a CNP transaction and there is no connection to upload any new DSC Value(s) onto the DSC Card 600.

[063] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention.

CLAIMS

What is claimed is:

1. A method for generating a security code for a card on a transaction event basis, the card having a display and no internal electrical battery power source, comprising the steps of:
 - (a) during each transaction using the card, performing at least the following:
 - (1) interfacing the card with an external electrical power source associated with a delivery device;
 - (2) after and while providing electrical power to the card from the external electrical power source, performing at least the following:
 - (i) transmitting a request for transaction authorization approval from the card to the delivery device connected to a network;
 - (ii) transmitting the request for transaction authorization approval from the delivery device to the network;
 - (iii) validating the request for transaction authorization approval by the network;
 - (iv) generating a new security code at a generator server and inserting the new security code into a transaction script;
 - (v) transmitting the transaction script from the network to the delivery device;
 - (vi) transmitting the transaction script from the delivery device to the card; and
 - (vii) retrieving the new security code from the script in the card.
2. The method for generating the security code for the card of claim 1, further comprising the step of (viii) storing the new security code in a memory area.
3. The method for generating the security code for the card of claim 1, further comprising the step of (viii) displaying the new security code on a display embedded in the card.
4. The method for generating the security code for the card of claim 3, further comprising the step of (iv) transmitting a confirmation message about the outcome of the display update step to the network.
5. The method for generating the security code for the card of claim 1, where the step of transmitting the script from the delivery device to the card is by a contact connection with the card.

6. The method for generating the security code for the card of claim 1, where the step of transmitting the script from the delivery device to the card is by a contactless connection between the online delivery device and the card.
7. The method for generating the security code for the card of claim 1, where the step of transmitting the request for transaction authorization to a network is by an offline delivery device that is forced to go online by the card.
8. A method for generating a plurality of security codes for a card on a transaction event basis, the card having a display and no internal electrical battery power source, comprising the steps of:
 - (a) during each transaction using the card, performing at least the following:
 - (1) interfacing the card with an external electrical power source associated with a delivery device;
 - (2) after providing electrical power to the card from the external electrical power source, performing at least the following:
 - (i) transmitting a request for transaction authorization approval from the card to the delivery device connected to a network;
 - (ii) transmitting the request for transaction authorization approval from the delivery device to the network;
 - (iii) validating the request for transaction authorization approval by the network;
 - (iv) generating a plurality of security codes from a generator server and inserting the plurality of security codes into a transaction script;
 - (v) transmitting the transaction script from the network to the delivery device;
 - (vi) transmitting the transaction script from the delivery device to the card; and
 - (vii) retrieving the new security codes from the script in the card.
9. The method for generating a plurality of security codes for the card of claim 8, further comprising the step of (viii) storing the plurality of security codes in a memory area.
10. The method for generating a plurality of security codes for the card of claim 9, further comprising the step of (ix) selecting one of the new security codes from the plurality of security codes stored in the memory area.
11. The method for generating a plurality of security codes for the card of claim 10, further comprising the step of (x) displaying one of the plurality of security codes on the display in the card.

12. The method for generating the security code for the card of claim 8, further comprising the step of (viii) transmitting a confirmation message about the outcome of the display update step to the network.

13. The method for generating the security code for the card of claim 8, where the step of transmitting the script from the delivery device to the card is by a contact connection with the card.

14. The method for generating the security code for the card of claim 8, where the step of transmitting the script from the delivery device to the card is by a contactless connection between the online delivery device and the card.

15. The method for generating the security code for the card of claim 8, where the step of transmitting the request for transaction authorization to a network is by an offline delivery device that is forced to go online by the card.

16. A method for generating a security code for a card on a transaction event basis, the card having a display and no internal electrical battery power source, comprising the steps of:

(a) during each transaction using the card, performing at least the following:

(1) interfacing the card with an external electrical power source associated with a delivery device;

(2) while interfaced, performing at least the following:

(i) receiving electrical power from the external electrical power source;

(ii) after receiving the electrical power from the external electrical power source, transmitting a request for transaction authorization approval from the card to the delivery device, thereby causing the request for transaction authorization approval to be transmitted from the delivery device to a remote generator server;

(iii) receiving a transaction script from the remote generator server that has a new security code in the transaction script; and

(iv) retrieving the new security code from the transaction script.

17. The method of claim 16, further comprising the step of (v) storing the security code in a memory area of the card while the card is receiving the electrical power.

18. The method of claim 16, further comprising the steps of:

(v) receiving one or more other new security codes from the transaction script;

(vi) selecting one of the security codes; and

(vii) wherein the new security code that is retrieved is the selected one.

19. The method of claim 16, further comprising the step of (v) transmitting a confirmation message about an outcome of the displaying to the remote generator server.

20. The method of claim 16, wherein the step of (i) receiving the electrical power and the step of (iii) receiving the transaction script are performed with a contact connection with the card.

21. The method of claim 16, wherein the step of (i) receiving the electrical power and the step of (iii) receiving the transaction script are performed with a contactless connection with the card.

22. The method of claim 16, wherein the step of (ii) transmitting the request for transaction authorization is by way of an offline delivery device that is forced to go online by the card.

23. The method of claim 16, further comprising the step of (v) displaying the new security code on the display associated with the card.