(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
18 January 2018 (18.01.2018)

WIPO | PCT

(10) **International Publication Number**
WO 2018/013961 A1

(51) **International Patent Classification:**
H04L 9/32 (2006.01)

(21) **International Application Number:**
PCT/US2017/042197

(22) **International Filing Date:**
14 July 2017 (14.07.2017)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
62/362,876 15 July 2016 (15.07.2016) US

(71) **Applicant: CARDINALCOMMERCE CORPORATION** [US/US]; 8100 Tyler Boulevard, Mentor, OH 44060 (US).

(72) **Inventors: ENRIGHT, Erik, Nils**; 4420 St. John's Bluff Lane, Willoughby, OH 44094 (US). **RATICA, Adam**; 7804 Chillicothe Road, Mentor, OH 44060 (US). **KERESMAN, Michael, A., III**; 8890 Cardinal Drive, Kirtland Hills, OH 44060 (US). **SHERWIN, Francis, M.**; 2940 Falmouth Road, Shaker Heights, OH 44122 (US). **BALASUBRAMANIAN, Chandra, S.**; 3833 Bushnell Road, University Heights, OH 44113 (US).

(74) **Agent: SAMORE, William, J.**; Fay Sharpe LLP, The Halle Building, 5th Floor, 1228 Euclid Avenue, Cleveland, OH 44115-1843 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) **Title:** AUTHENTICATION TO AUTHORIZATION BRIDGE USING ENRICHED MESSAGES

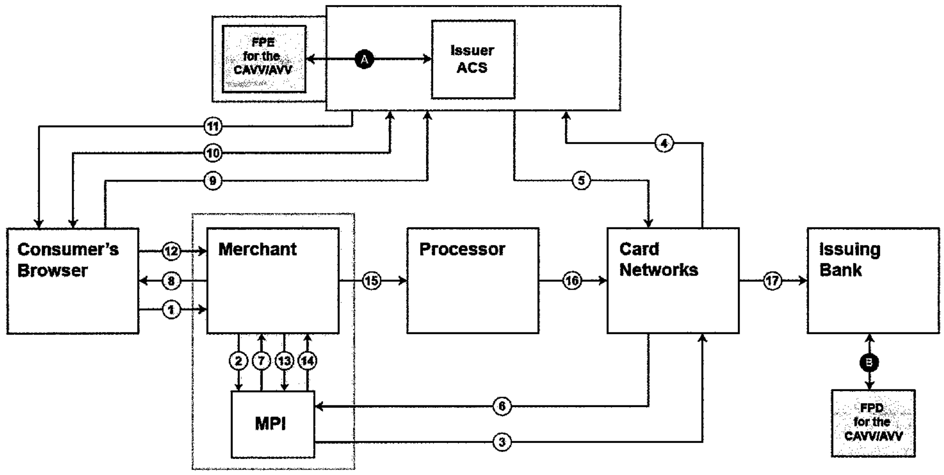

Issuer ACS - Crypto Method

Figure 1

(57) **Abstract:** A system of electronic communication is disclosed. The system may: create a Pre-Authentication Transaction Number (Pre-ATN) by combining a number with a Special Encode Value (SEV), wherein the SEV is a single digit integer value; encrypt the Pre-ATN using a Format Preserving Encryption (FPE) to generate an encrypted Authentication Transaction Number (ATN); and send the encrypted ATN to an access control server (ACS) to use the encrypted ATN to generate a cardholder Authentication Verification Value (CAW) or an Accountholder Authentication Value (AAV).

WO 2018/013961 A1

[Continued on next page]

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

AUTHENTICATION TO AUTHORIZATION BRIDGE USING ENRICHED MESSAGES

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 62/362,876, filed July 15, 2016, which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] The subject matter of the present specification generally relates to the art of secure data communication, and more specifically, to securely sending sensitive information along existing rails to a targeted audience. Exemplary embodiments disclosed herein find particular application in conjunction with the secure communication of selected information or data from an identity authentication system to a transaction authorization system in connection with the processing of a credit card or other payment instrument transaction, and they will be described herein with particular reference thereto. However, it is to be appreciated that various exemplary embodiments such as those disclosed herein are also amenable to other like applications.

[0003] Generally, in connection with credit card and/or other like payment instruments transactions conducted over telecommunication networks (e.g., including without limitation wired and/or wireless networks, the Internet, WiFi, cellular networks, disparate systems, private networks, etc.), the current state of consumer authentication relies on merchants and corresponding systems in a network ecosystem to receive, maintain and forward authentication information. The authentication of cardholders in connection with commercial transactions conducted over a telecommunications network (e.g., such as the Internet) has been popularized by initiatives and/or programs such as Visa's Verified by Visa (VbV) and MasterCard's SecureCode. Such programs allow the issuer of a credit card to authenticate the identity of a cardholder prior to authorizing completion of a transaction. However, the authentication is often isolated from authorization as they are often two separate systems that only communicate via predefined messages, e.g., prescribed by the particular card network, be it Visa, MasterCard or otherwise. Accordingly, this isolation or separation tends to limit the information that can be shared between the authentication and authorization steps. This can become more important when risk based authentication is used by the issuer in the decision to authenticate, and the only information passed to the authorization system is the authentication outcome (e.g., a binary result such as positive or negative).

[0004] Accordingly, it can be desirable to bridge the authentication and authorization systems allowing additional information to be transferred and/or communicated therebetween, e.g., so that false positive and/or false negatives produced by the authorization system may be potentially reduced. However, heretofore, a suitable system, approach and/or method has not been developed and/or implemented.

[0005] Disclosed herein is a new and/or improved system and/or method for securely communicating selected information and data in enriched messages passed between an authentication system and/or step and an authorization system and/or step using existing and/or predefined protocols and/or connections (generally referred to and/or otherwise known as “rails”) established by the card networks, e.g., such as Visa, Mastercard, etc. In essence, by using the enriched message as disclosed herein, a bridge is established between authentication and authorization which is generally referred to nominally herein as an “Authentication/Authorization Bridge.” Using the enriched message and Authentication/Authorization Bridge, a merchant or Access Control Server (ACS) system or other suitable entity is able to pass certain values and/or data through the ecosystem using the existing rails that may be useful throughout the authentication and authorization steps. Suitably, the data in the enriched message is secured and compatible with a network cryptogram check, thus providing the merchant with the appropriate protection offered by consumer authentication. One example that illustrates the usage of the enriched message is the merchant making a minimally invasive change to the message enabling the issuer to better consume and use the authentication results for authorization decision making. More broadly speaking, the approach described herein facilitates the transmitting of information from someone and/or something that is submitting a transaction for settlement or the like to someone and/or something that will provide the requested settlement or the like.

BRIEF DESCRIPTION

[0006] This Brief Description is provided to introduce concepts related to the present specification. It is not intended to identify essential features of the claimed subject matter nor is it intended for use in determining or limiting the scope of the claimed subject matter. The exemplary embodiments described below are not intended to be exhaustive or to limit the claims to the precise forms disclosed in the following Detailed Description. Rather, the embodiments are chosen and described so that others skilled in the art may appreciate and understand the principles and practices of the subject matter presented herein.

[0007] In accordance with one aspect, a system for electronic communication includes: one or more processors of a third party configured to: create a Pre-Authentication Transaction Number (Pre-ATN) by combining a number with a Special Encode Value (SEV), wherein the SEV is a single digit integer value; encrypt the Pre-ATN using a Format Preserving Encryption (FPE) to generate an encrypted Authentication Transaction Number (ATN); and send the encrypted ATN to an access control server (ACS) to use the encrypted ATN to generate a cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV).

[0008] In the system of the preceding paragraph, the ACS may be provisioned with FPE keys, key indexes and SEV definition tables; and the ACS may be configured to use a key index of the key indexes for both FPE and a card verification value (CVV) calculation. The ACS may be configured to use a FPE base key corresponding to a selected key index along with a Primary Account Number (PAN) to create a unique key per PAN. The SEV definition tables may relate particular SEV values to information that is being bridged between: (i) an authentication procedure that authenticates the identity of a user; and (ii) an authorization procedure that authorizes a transaction of the user. The system may further include a decoding entity configured to: perform Format Preserving Decryption (FPD) using the ATN and a Primary Account Number (PAN) unique key to generate the Pre-ATN including the SEV; and use the SEV to look up a corresponding definition in a table. The ACS may be configured to authenticate a consumer by exchanging, with the consumer, authentication credentials including a password; and the system may further comprise one or more processors of a decoding entity configured to obtain the SEV by: receiving an authorization request including the CAVV or the AAV; deconstructing the ATN and a key indicator from the CAVV or AAV; and decrypting the ATN using a Format Preserving Decryption (FPD) routine; and the one or more processors of the decoding entity may be further configured to use the SEV to look up a corresponding definition in a table. The one or more processors of the decoding entity may be further configured to use SEV definition tables to relate particular SEV values to bridge information between the authentication procedure and the authorization procedure. The number may be a random three digit number.

[0009] In accordance with another aspect, a method for electronic communication includes: with one or more processors of a third party: creating a Pre-Authentication Transaction Number (Pre-ATN) by combining a number with a Special Encode Value (SEV), wherein the SEV is a single digit integer value; encrypting the Pre-ATN using a Format Preserving Encryption (FPE) to generate an encrypted Authentication Transaction Number (ATN); and sending the encrypted ATN to an access control server (ACS); and with the ACS: using the encrypted ATN to generate a cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV).

[0010] In a method as described in the preceding paragraph, the ACS may be provisioned with FPE keys, key indexes and SEV definition tables; and a key index of the key indexes is used for both FPE and a card verification value (CVV) calculation. A FPE base key corresponding to a selected key index may be used along with a Primary Account Number (PAN) to create a unique key per PAN. The SEV definition tables may relate particular SEV values to information that is being bridged between: (i) an authentication procedure that authenticates the identity of a user; and (ii) an authorization procedure that authorizes a transaction of the user. The method may further include: performing Format Preserving Decryption (FPD) using the ATN and a Primary Account Number (PAN) unique key to generate the Pre-ATN including the SEV; and using the SEV to look up a corresponding definition in a table. The method may further include: authenticating a consumer by exchanging, between the ACS and the consumer, authentication credentials including a password; and with one or more processors of a decoding entity, obtaining the SEV by: receiving an authorization request including the CAVV or the AAV; deconstructing the ATN and a key indicator from the CAVV or AAV; and decrypting the ATN using a Format Preserving Decryption (FPD) routine; and further with the one or more processors of the decoding entity, using the SEV to look up a corresponding definition in a table. The method may further include: as part of an authentication procedure, authenticating a consumer by exchanging, between the ACS and the consumer, authentication credentials including a password; and as part of an authorization procedure, with one or more processors of a decoding entity, obtaining the SEV by: receiving an authorization request including the CAVV or the AAV; deconstructing the ATN and a key indicator from the CAVV or AAV; and decrypting the ATN using a Format Preserving Decryption (FPD) routine; and further with the one or more processors of the decoding entity, using the SEV to look up a corresponding definition in a table to bridge information between the authentication procedure and the authorization procedure.

[0011] In accordance with another aspect, a decoding entity may include one or more processors configured to: obtain a Special Encode Value (SEV), the SEV being a single digit integer value, by: receiving an authorization request including cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV); deconstructing a Authentication Transaction Number (ATN) and a key indicator from the CAVV or AAV; and decrypting the ATN using a Format Preserving Decryption (FPD) routine; and use the SEV to look up a corresponding definition in a table to bridge information between an authentication procedure and an authorization procedure.

[0012] Numerous advantages and benefits of the subject matter disclosed herein will become apparent to those of ordinary skill in the art upon reading and understanding the present specification. It is to be understood, however, that the detailed description of the various embodiments and specific examples, while indicating preferred and/or other embodiments, are given by way of illustration and not limitation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The following Detailed Description makes reference to the figures in the accompanying drawings. However, the inventive subject matter disclosed herein may take form in various components and arrangements of components, and in various steps and arrangements of steps. The drawings are only for purposes of illustrating exemplary and/or preferred embodiments and are not to be construed as limiting. Further, it is to be appreciated that the drawings may not be to scale.

[0014] FIGURE 1 is a diagrammatic illustration showing one exemplary embodiment employing an Authentication/Authorization Bridge and enhanced messaging system and/or method in accordance with aspects of the present inventive subject matter.

[0015] FIGURE 2 is a diagrammatic illustration showing another exemplary embodiment employing an Authentication/Authorization Bridge and enhanced messaging system and/or method in accordance with aspects of the present inventive subject matter.

[0016] FIGURE 3 is a diagrammatic illustration showing an exemplary encoding and encryption method according to an exemplary embodiment of the present inventive subject matter.

[0017] FIGURE 4 is a diagrammatic illustration showing an exemplary decoding and decryption method according to an exemplary embodiment of the present inventive subject matter.

DETAILED DESCRIPTION

[0018] For clarity and simplicity, the present specification shall refer to structural and/or functional elements, relevant standards, algorithms and/or protocols, and other components, methods and/or processes that are commonly known in the art without further detailed explanation as to their configuration or operation except to the extent they have been modified or altered in accordance with and/or to accommodate the preferred and/or other embodiment(s) presented herein. Moreover, the apparatuses and methods disclosed in the present specification are described in detail by way of examples and with reference to the figures. Unless otherwise specified, like numbers in the figures indicate references to the same, similar or corresponding elements throughout the figures. It will be appreciated that modifications to disclosed and described examples, arrangements, configurations, components, elements, apparatuses, methods, materials, etc. can be made and may be desired for a specific application. In this disclosure, any identification of specific materials, techniques, arrangements, etc. are either related to a specific example presented or are merely a general description of such a material, technique, arrangement, etc. Identifications of specific details or examples are not intended to be, and should not be, construed as mandatory or limiting unless specifically designated as such. Selected examples of apparatuses and methods are hereinafter disclosed and described in detail with reference made to the figures.

[0019] With reference to FIGURE 1, where the particular steps described below are illustrated as circled reference numerals, there is shown a diagrammatic illustration of one exemplary method for processing an authenticated transaction between a consumer and merchant conducted over a telecommunications network, e.g., such as the Internet. As shown, a consumer (e.g., employing a suitable browser or application running on an end user computing and/or communication device or using some form of an Internet connected device) accesses a website of a merchant which is provided via a hardware server (e.g., a web server) operatively connected to a telecommunications network, e.g., such as the Internet. Suitably, the computing device of the consumer may be a computer, smartphone or other like device capable of supporting a browser running thereon and of operatively connecting to the telecommunications network in order to communicate with and/or exchange messages, signals, information and/or data with other elements, systems, servers and/or like components also operatively connected with the telecommunications network.

[0020] In practice, the consumer may select a number of goods, services and/or the like, e.g., by selecting and/or placing the same in a virtual shopping cart or the like. After navigating to a checkout or other like page on the merchant's website, the consumer may select to initiate a purchase of the chosen items, e.g., employing their browser to click on a designated link or option provided on the checkout page. Accordingly, the consumer is prompted to select a payment option and/or enter payment information which is in turn forwarded to the merchant. For example, the consumer may select to pay via credit card, in which case the payment information forwarded to the merchant may include the credit card number (e.g., a Primary Account Number (PAN) or dynamic PAN), expiration date, name on the credit card, etc. The forwarding of payment information from the consumer to the merchant's server is illustrated as step 1 in FIGURE 1.

[0021] In response, the merchant's server sends a request to a merchant plug-in (MPI) to create a Verify Enrollment Request (VEReq) or other like message. See step 2 in FIGURE 1. For the sake of simplicity herein, only a single MPI is shown in FIGURE 1. However, in practice, multiple MPIs are typically employed – a separate MPI being employed for each different card network. The VEReq or other like message is used to verify enrollment of the credit card in a particular authentication initiative or program (e.g., VbV, SecureCode, etc.) prescribed by the particular associated payment scheme or card network (e.g., Visa, Mastercard, etc.). In general, the VEReq will include the PAN received with the payment information. Essentially, the VEReq message is a request, ultimately sent to the issuer's Access Control Server (ACS), to check if the PAN (contained in the VEReq) is enrolled in the particular authentication initiative or program.

[0022] In turn (see step 3 of FIGURE 1), the VEReq or other like message is sent to a directory server (DS) for the associated payment scheme or card network. Suitably, the DS is part of the card network. In practice, the DS will perform a Bank Identification Number (BIN) lookup and if the BIN is for an ACS operated by the issuer, then the VEReq is forwarded to the issuer's ACS (see step 4 of FIGURE 1). In general, the ACS is an entity that controls authentication of cardholders. The ACS accepts a VEReq and in response returns a Verify Enrollment Response (VERes); and accepts a Payment Authentication Request (PAReq) and in response returns a Payment Authentication Response (PARes). The ACS is also responsible for generating a Cardholder Authentication Verification Value (CAVV) and/or an Accountholder Authentication Value (AAV). The CAVV and AAV are payment scheme specific values that are generated on successful authentications or attempts transactions. In general, each includes: (i) an Authentication Transaction Number (ATN); and (ii) a Card Verification Value (CVV). Generally, the three digit CVV is computed using the four digit ATN, PAN, status codes, and two Data Encryption Standard DES keys - the specifics of which may be unique between different implementations (e.g., currently the specifics differ as between Visa and MasterCard implementations). The value of the CVV may be validated by having the two DES keys shared between two parties along with the PAN, ATN and status codes.

[0023] In response to the VEReq or other like message, the issuer's ACS replies with a Verify Enrollment Response (VERes) or other like message (see step 5 of

FIGURE 1). In turn, the VERes is forwarded to the MPI (see step 6 of FIGURE 1). Essentially, the VERes indicates whether or not the PAN in question is enrolled in the particular authentication initiative or program. In general, the VERes is ultimately returned to the merchant, and if the PAN is indeed enrolled, the VERes will include the Uniform Resource Locator (URL) or address of the ACS (referred to as the ACSURL). That is to say, the ACSURL indicates the address to which the cardholder's browser should ultimately sent (e.g., via a Hypertext Transfer Protocol (HTTP) POST) a PAReq, Merchant Data (MD) and TermURL (as described below).

[0024] Upon receiving the VERes, the MPI uses the VERes to generate a PAReq or other like message which is forwarded to the merchant's server, e.g., as shown in step 7 of FIGURE 1.

[0025] Accordingly, upon receiving the PAReq, the merchant's server creates a form fields including the PAReq, MD and TermURL and forwards the same to the consumer's browser directing the consumer's browser to submit the data to the ACSURL (e.g., via an HTTP POST). See step 8 of FIGURE 1. In general, the MD is data sent along with the PAReq that will be returned with the corresponding PARes to help the merchant reestablish the session. The TermURL identifies the address to POST or otherwise submit the PARes and MD field from the issuer's ACS to the merchant via the consumer's browser. As shown in step 9, the PAReq, MD and TermURL are in turn POSTed or otherwise submitted the issuer's ACS.

[0026] As shown in step 10, one or more requests, responses, messages, data and/or information may be exchanged between the consumer and the ACS in order to authenticate the consumer. For example, this may include the submission of various authentication credentials, including but not limited to: a password, a Personal Identification Number (PIN), biometric data (such as finger print, retinal scan, voice recognition or facial recognition data), risk criteria and calculation, etc.

[0027] Based on the outcome of the authentication, the CAVV or AAV is generated accordingly. Suitably, the ACS will generate the CAVV or AAV. More specifically, as shown in step A, a Special Encode Value (SEV) (e.g., a single digit integer value between 0 and 9) is first encoded into the ATN. The so encoded ATN is then encrypted using a Format Preserving Encryption (FPE). As shown, the encoding and encryption is carried out by a third party processor and/or hardware server. The so encrypted ATN is then passed back to the ACS and used to generate the CAVV or AAV (as the case may be) with the otherwise standard CAVV/AAV generating algorithm. Then, the PARes message is signed by the ACS. Notably, because the solution proposed herein leverages FPE, it is compatible with the industry standard cryptographic checks used by the card networks.

[0028] As shown in step 11, the issuer's ACS returns a page to the consumer's browser that will POST or otherwise submit the PARes (which includes the CAVV/AAV generated using the encoded/encrypted ATN) and MD field to the TermURL. The POSTed PARes and MD are in turn received by the merchant (see step 12 of FIGURE 1); and in step 13, the merchant passes the PARes to the MPI.

[0029] Suitably, the MPI verifies the signature of the PARes and returns (see step 14) the CAVV/AAV and the Electronic Commerce Indicator (ECI) to the merchant. The ECI a value which indicates the result or outcome of the authentication performed in step 10.

[0030] Having received the CAVV/AAV and ECI, to obtain authorization for the transaction, the merchant forwards the same to a transaction processor (possibly through a payment gateway – not shown). See step 15 of FIGURE 1.

[0031] The transaction processor formats a message for the specific card network (e.g., be it Visa, Mastercard, etc.) and passes the ECI and CAVV/AAV to the card network (see step 16). Suitably, the card network can validate the validity of the CAVV/AAV using the cryptographic method specified for the CAVV/AVV and/or the card network can also perform replay CAVV/AAV analysis without a problem because it is backward compatible. The foregoing feature is significantly noteworthy. Replay analysis asserts that a sample history of successful CAVV/AVV are not being reused.

[0032] Illustrated as step 17, an authorization request, including the PAN and CAVV/AAV, is sent to the issuer.

[0033] Having received the authorization request, the issuer may submit the PAN and CAVV/AAV to a Format Preserving Decryption (FPD) routine. Suitably, the routine may be executed by the issuer or a suitable third party. In any event, the ATN and a key indicator are stripped and/or deconstructed from the CAVV/AAV. The ATN is then decrypted using FPD. Accordingly, the SEV is obtained and returned to the issuer.

[0034] FIGURE 2 shows another embodiment in which a Universal Merchant Platform (UMP) is employed. For example, the UMP may be implemented as disclosed in U.S. Patent Nos. 7,051,002; 7,693,783; 8,140,429; 8,645,266; and 8,650,118 and in U.S. Patent Application Publication Nos. US 2014/0081863 A1; US 2014/0108250 A1; US 2014/0089194 A1; and US 2014/0156532 A1; all of which patents and patent application publications are incorporated herein by reference in their entirety.

[0035] With reference to FIGURE 2, where the particular steps described below are again illustrated as circled reference numerals, there is shown a diagrammatic illustration of another exemplary method for processing an authenticated transaction between a consumer and merchant conducted over a telecommunications network, e.g., such as the Internet. As shown, a consumer (e.g., employing a suitable browser or application running on an end user computing and/or communication device) accesses a website of a merchant which is provided via a hardware server (e.g., a web server) operatively connected to a telecommunications network, e.g., such as the Internet. Suitably, the computing device of the consumer may be a computer, smartphone or other like device capable of supporting a browser running thereon and of operatively connecting to the telecommunications network in order to communicate with and/or exchange messages, signals, information and/or data with other elements, systems, servers and/or like components also operatively connected with the telecommunications network.

[0036] In practice, the consumer may select a number of goods, services and/or the like, e.g., by selecting and/or placing the same in a virtual shopping cart or the like. After navigating to a checkout or other like page on the merchant's website, the consumer may select to initiate a purchase of the chosen items, e.g., employing their browser to click on a designated link or option provided on the checkout page. Accordingly, the consumer is prompted to select a payment option and/or enter payment information which is in turn forwarded to the merchant. For example, the consumer may select to pay via credit card, in which case the payment information forwarded to the merchant may include the credit card number (e.g., a Primary Account Number (PAN)), expiration date, name on the credit card, etc. The forwarding of payment information from the consumer to the merchant's server is illustrated as step 1 in FIGURE 2.

[0037] In response, the merchant's server sends a request to a UMP (e.g., supporting a suitable MPI) to create a Verify Enrollment Request (VEReq) or other like message. See step 2 in FIGURE 2.

[0038] In turn (see step 3 of FIGURE 2), the VEReq or other like message is sent to a directory server (DS) for the associated payment scheme or card network. Suitably, the DS is part of the card network. In practice, the DS will perform a Bank Identification Number (BIN) lookup and if the BIN is for an ACS operated by the issuer, then the VEReq is forwarded to the issuer's ACS (see step 4 of FIGURE 2).

[0039] In response to the VEReq or other like message, the issuer's ACS replies with a Verify Enrollment Response (VERes) or other like message (see step 5 of FIGURE 2). In turn, the VERes is forwarded to the UMP (see step 6 of FIGURE 2).

[0040] Upon receiving the VERes, the UMP uses the VERes to generate a PAReq or other like message which is forwarded to the merchant's server, e.g., as shown in step 7 of FIGURE 2.

[0041] Accordingly, upon receiving the PAReq, the merchant's server creates a form fields including the PAReq, MD and TermURL and forwards the same to the consumer's browser directing the consumer's browser to submit the data to the ACSURL (e.g., via an HTTP POST). See step 8 of FIGURE 2. As shown in step 9, the PAReq, MD and TermURL are in turn POSTed or otherwise submitted the issuer's ACS.

[0042] As shown in step 10, one or more requests, responses, messages, data and/or information may be exchanged between the consumer and the ACS in order to authenticate the consumer. For example, this may include the submission of various authentication credentials, including but not limited to: a password, a Personal Identification Number (PIN), biometric data (such as finger print, retinal scan, voice recognition or facial recognition data), risk criteria and calculation, etc.

[0043] Based on the outcome of the authentication, the CAVV or AAV is generated accordingly. Suitably, the ACS will generate the CAVV or AAV in the usual manner. As shown in step 11, the issuer's ACS returns a page to the consumer's browser that will POST or otherwise submit the PARes and MD field to the TermURL. The POSTed

PARes and MD are in turn received by the merchant (see step 12 of FIGURE 2); and in step 13, the merchant passes the PARes to the UMP. In practice, the UMP may employ the appropriate supported MPI for further processing. More specifically, as shown in step A, a Special Encode Value (SEV) (e.g., a single digit integer value between 0 and 9) is first encoded into the ATN. The so encoded ATN is then encrypted using a Format Preserving Encryption (FPE). The so encrypted ATN is then passed back into the otherwise standard CAVV or AAV generating algorithm (as the case may be) to be regenerated based on the pre-shared keys.

[0044] Suitably, the appropriate MPI supported on the UMP verifies the signature of the PARes and returns (see step 14) the CAVV/AAV (which includes the new CAVV/AAV regenerated using the encoded/encrypted ATN) and the Electronic Commerce Indicator (ECI) to the merchant.

[0045] Having received the CAVV/AAV and ECI, to obtain authorization for the transaction, the merchant forwards the same to a transaction processor (possibly through a payment gateway – not shown). See step 15 of FIGURE 2.

[0046] The transaction processor formats a message for the specific card network (e.g., be it Visa, Mastercard, etc.) and passes the ECI and CAVV/AAV to the card network (see step 16). Suitably, the card network can validate the validity of the CAVV/AAV using the cryptographic method specified for the CAVV/AVV and/or the card network can also perform replay CAVV/AAV analysis without a problem.

[0047] Illustrated as step 17, an authorization request, including the PAN and CAVV/AAV, is sent to the issuer.

[0048] Having received the authorization request, the issuer may submit the PAN and CAVV/AAV to a Format Preserving Decryption (FPD) routine. Suitably, the routine may be executed by the issuer or a suitable third party. In any event, the ATN and a key indicator are stripped from the CAVV/AAV. The ATN is then decrypted using FPD. Accordingly, the SEV is obtained and returned to the issuer.

[0049] With reference now to FIGURE 3, there is illustrated an exemplary embodiment by which step A is carried out. As shown, the issuer and encoding entity (e.g., the UPM) are provisioned with appropriate FPE keys, key indexes and SEV definition tables that are suitably maintained in synchronization using a sure methodology. The SEV definition tables relate particular SEV values to specific definitions, e.g., information that is being bridged between the authentication and authorization steps. Initially, a key index is selected, e.g., key index #1. This key index is used for both FPE and CVV calculation. This allows for seamless key rotation.

[0050] The FPE base key corresponding to the selected key index is used along with the PAN (or other suitable data) to create a unique key per PAN. For example, as shown, a 256-bit Secure Hash Algorithm (SHA256) is used to generate the unique key. In practice, a secure key is derived using other suitable means, e.g., including but not limited to Hash Message Authentication Code 256 (HMAC256), etc.

[0051] Based on the authentication parameters, a SEV to be encoded into the CAVV/AAV is selected, and a Pre-ATN is created. The Pre-ATN is suitably a random three digit number combined with the SEV to form a four digit number. Alternately, the Pre-ATN is not entirely random but rather conforms to a predetermined sequence or is otherwise determined. Then, FPE is performed using the Pre-ATN and the PAN unique key to generate the encoded and encrypted ATN.

[0052] Finally, the ATN and selected key index are passed into the CAVV/AAV calculation. The same index key used for FPE is also used for the key selection used in calculating the CVV in the CAVV/AAV.

[0053] With reference now to FIGURE 4, there is illustrated an exemplary embodiment by which step B is carried out. As shown, the issuer and decoding entity (e.g., the UPM) are provisioned with appropriate FPE keys, key indexes and SEV definition tables that are suitably maintained in synchronization using a sure methodology. The SEV definition tables relate particular SEV values to specific definitions, e.g., information that is being bridged between the authentication and authorization steps. Initially, a key index is selected, e.g., key index #1. This key index is used for both FPE and CVV calculation. This allows for seamless key rotation.

[0054] The FPE base key corresponding to the selected key index is used along with the PAN (or other suitable data) to create a unique key per PAN. For example, as shown, a 256-bit Secure Hash Algorithm (SHA256) is used to generate the unique key. Then, FPD (Format Preserving Decryption) is performed using the ATN and the PAN unique key to generate the Pre-ATN, including the SEV. In this way, the SEV has been communicated to the issuer. Accordingly, the issuer can use the SEV to lookup the corresponding definition in the table. Notably, the SEV and/or its meaning remains opaque, e.g., to other entities handling data and/or messages along the rails.

[0055] Various aspects of the present inventive subject matter have been described herein with reference to exemplary and/or preferred embodiments. Obviously, modifications and alterations will occur to others upon reading and understanding the preceding detailed description. It is intended that the inventive subject matter be construed as including all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

[0056] The above methods, system, platforms, modules, processes, algorithms and/or apparatus have been described with respect to particular embodiments. It is to be appreciated, however, that certain modifications and/or alteration are also contemplated. Moreover, certain nomenclature has been used herein with reference to various massages, information and/or data (e.g., without limitation, PARes, PAReq, VERes, VEReq, etc.). Such nomenclature is merely used herein for purposes of illustration and/or example, and in practice, other like messages, information and/or data are contemplated regardless of the name or label applied thereto so long as it otherwise functions and/or represents its object similarly.

[0057] It is to be appreciated that in connection with the particular exemplary embodiment(s) presented herein certain structural and/or function features are described as being incorporated in defined elements and/or components. However, it is contemplated that these features may, to the same or similar benefit, also likewise be incorporated in other elements and/or components where appropriate. It is also to be appreciated that different aspects of the exemplary embodiments may be selectively employed as appropriate to achieve other alternate embodiments suited for desired applications, the other alternate embodiments thereby realizing the respective advantages of the aspects incorporated therein.

[0058] It is also to be appreciated that any one or more of the particular tasks, steps, processes, methods, functions, elements and/or components described herein may suitably be implemented via hardware, software, firmware or a combination thereof. In particular, various modules, components and/or elements may be embodied by processors, electrical circuits, computers and/or other electronic data processing devices that are configured and/or otherwise provisioned to perform one or more of the tasks, steps, processes, methods and/or functions described herein. For example, a processor, computer or other electronic data processing device embodying a particular element may be provided, supplied and/or programmed with a suitable listing of code (e.g., such as source code, interpretive code, object code, directly executable code, and so forth) or other like instructions or software or firmware, such that when run and/or executed by the computer or other electronic data processing device one or more of the tasks, steps, processes, methods and/or functions described herein are completed or otherwise performed. Suitably, the listing of code or other like instructions or software or firmware is implemented as and/or recorded, stored, contained or included in and/or on a non-transitory computer and/or machine readable storage medium or media so as to be providable to and/or executable by the computer or other electronic data processing device. For example, suitable storage mediums and/or media can include but are not limited to: floppy disks, flexible disks, hard disks, magnetic tape, or any other magnetic storage medium or media, CD-ROM, DVD, optical disks, or any other optical medium or media, a RAM, a ROM, a PROM, an EPROM, a FLASH-EPROM, or other memory or chip or cartridge, or any other tangible medium or media from which a computer or machine or electronic data processing device can read and use. In essence, as used herein, non-transitory computer-readable and/or machine-readable mediums and/or media comprise all computer-readable and/or machine-readable mediums and/or media except for a transitory, propagating signal.

[0059] Optionally, any one or more of the particular tasks, steps, processes, methods, functions, elements and/or components described herein may be implemented on and/or embodiment in one or more general purpose computers, special purpose computer(s), a programmed microprocessor or microcontroller and peripheral integrated circuit elements, an ASIC or other integrated circuit, a digital signal processor, a hardwired electronic or logic circuit such as a discrete element circuit, a programmable logic device such as a PLD, PLA, FPGA, Graphical card CPU (GPU), or PAL, or the like. In general, any device, capable of implementing a finite state machine that is in turn capable of implementing the respective tasks, steps, processes, methods and/or functions described herein can be used.

[0060] Additionally, it is to be appreciated that certain elements described herein as incorporated together may under suitable circumstances be stand-alone elements or otherwise divided. Similarly, a plurality of particular functions described as being carried out by one particular element may be carried out by a plurality of distinct elements acting independently to carry out individual functions, or certain individual functions may be split-up and carried out by a plurality of distinct elements acting in concert. Alternately, some elements or components otherwise described and/or shown herein as distinct from one another may be physically or functionally combined where appropriate.

[0061] In short, the present specification has been set forth with reference to preferred embodiments. Obviously, modifications and alterations will occur to others upon reading and understanding the present specification. It is intended that the inventive subject matter be construed as including all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

[0062] What is claimed is:

CLAIMS

1. A system for electronic communication, comprising:

one or more processors of a third party configured to:

create a Pre-Authentication Transaction Number (Pre-ATN) by combining a number with a Special Encode Value (SEV), wherein the SEV is a single digit integer value;

encrypt the Pre-ATN using a Format Preserving Encryption (FPE) to generate an encrypted Authentication Transaction Number (ATN); and

send the encrypted ATN to an access control server (ACS) to use the encrypted ATN to generate a cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV).

2. The system of claim 1, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

the ACS is configured to use a key index of the key indexes for both FPE and a card verification value (CVV) calculation.

3. The system of claim 1, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

the ACS is configured to use a FPE base key corresponding to a selected key index along with a Primary Account Number (PAN) to create a unique key per PAN.

4. The system of claim 1, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

the SEV definition tables relate particular SEV values to information that is being bridged between:

(i) an authentication procedure that authenticates the identity of a user; and

(ii) an authorization procedure that authorizes a transaction of the user.

5. The system of claim 1, further comprising a decoding entity configured to:

perform Format Preserving Decryption (FPD) using the ATN and a Primary Account Number (PAN) unique key to generate the Pre-ATN including the SEV; and

use the SEV to look up a corresponding definition in a table.

6. The system of claim 1, wherein:

the ACS is configured to authenticate a consumer by exchanging, with the consumer, authentication credentials including a password; and

the system further comprises one or more processors of a decoding entity configured to obtain the SEV by:

receiving an authorization request including the CAVV or the AAV;

deconstructing the ATN and a key indicator from the CAVV or AAV; and

decrypting the ATN using a Format Preserving Decryption (FPD) routine; and

the one or more processors of the decoding entity are further configured to use the SEV to look up a corresponding definition in a table.

7. The system of claim 1, wherein:

the ACS is configured to perform an authentication procedure to authenticate a consumer by exchanging, with the consumer, authentication credentials including a password; and

the system further comprises one or more processors of a decoding entity configured to, as part of an authorization procedure, obtain the SEV by:

receiving an authorization request including the CAVV or the AAV;

deconstructing the ATN and a key indicator from the CAVV or AAV; and

decrypting the ATN using a Format Preserving Decryption (FPD) routine; and the one or more processors of the decoding entity are further configured to use SEV definition tables to relate particular SEV values to bridge information between the authentication procedure and the authorization procedure.

8. The system of claim 1, wherein the number is a random three digit number.

9. A method for electronic communication, comprising:

with one or more processors of a third party:

creating a Pre-Authentication Transaction Number (Pre-ATN) by combining a number with a Special Encode Value (SEV), wherein the SEV is a single digit integer value;

encrypting the Pre-ATN using a Format Preserving Encryption (FPE) to generate an encrypted Authentication Transaction Number (ATN); and

sending the encrypted ATN to an access control server (ACS); and

with the ACS:

using the encrypted ATN to generate a cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV).

10. The method of claim 9, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

a key index of the key indexes is used for both FPE and a card verification value (CVV) calculation.

11. The method of claim 9, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

a FPE base key corresponding to a selected key index is used along with a Primary Account Number (PAN) to create a unique key per PAN.

12. The method of claim 9, wherein:

the ACS is provisioned with FPE keys, key indexes and SEV definition tables; and

the SEV definition tables relate particular SEV values to information that is being bridged between:

(i) an authentication procedure that authenticates the identity of a user; and

(ii) an authorization procedure that authorizes a transaction of the user.

13. The method of claim 9, further comprising:

performing Format Preserving Decryption (FPD) using the ATN and a Primary Account Number (PAN) unique key to generate the Pre-ATN including the SEV; and

using the SEV to look up a corresponding definition in a table.

14. The method of claim 9, further comprising:

authenticating a consumer by exchanging, between the ACS and the consumer, authentication credentials including a password; and

with one or more processors of a decoding entity, obtaining the SEV by:

receiving an authorization request including the CAVV or the AAV;

deconstructing the ATN and a key indicator from the CAVV or AAV; and

decrypting the ATN using a Format Preserving Decryption (FPD) routine; and

further with the one or more processors of the decoding entity, using the SEV to look up a corresponding definition in a table.

15. The method of claim 9, further comprising:

as part of an authentication procedure, authenticating a consumer by exchanging, between the ACS and the consumer, authentication credentials including a password; and

as part of an authorization procedure, with one or more processors of a decoding entity, obtaining the SEV by:

receiving an authorization request including the CAVV or the AAV;

deconstructing the ATN and a key indicator from the CAVV or AAV; and

decrypting the ATN using a Format Preserving Decryption (FPD) routine; and

further with the one or more processors of the decoding entity, using the SEV to look up a corresponding definition in a table to bridge information between the authentication procedure and the authorization procedure.

16. A decoding entity comprising one or more processors, the one or more processors configured to:

obtain a Special Encode Value (SEV), the SEV being a single digit integer value, by:

receiving an authorization request including cardholder Authentication Verification Value (CAVV) or an Accountholder Authentication Value (AAV);

deconstructing a Authentication Transaction Number (ATN) and a key indicator from the CAVV or AAV; and

decrypting the ATN using a Format Preserving Decryption (FPD) routine; and

use the SEV to look up a corresponding definition in a table to bridge information between an authentication procedure and an authorization procedure.

Issuer ACS - Crypto Method

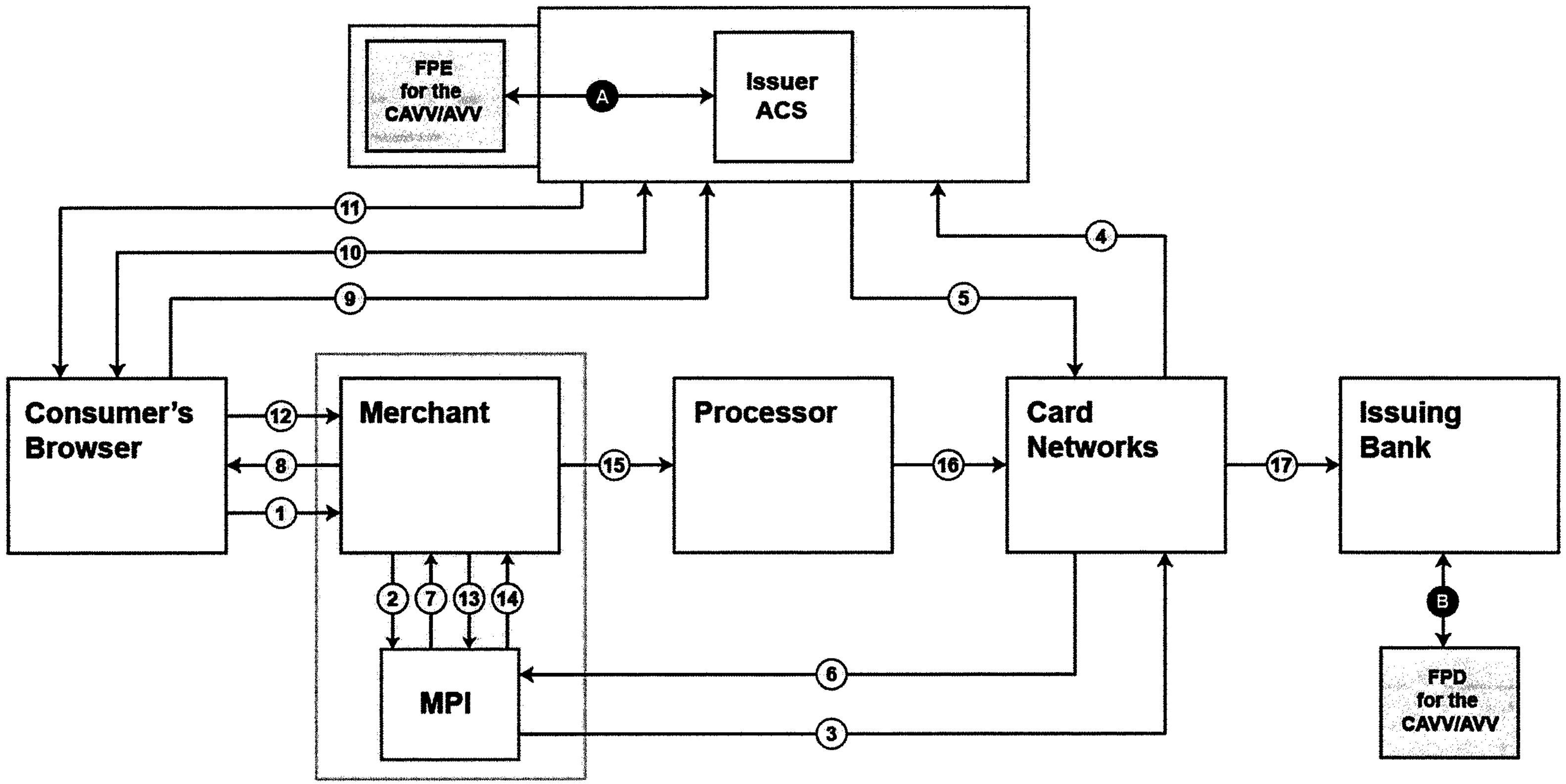


Figure 1

UMP Merchant with Issuer Partnership

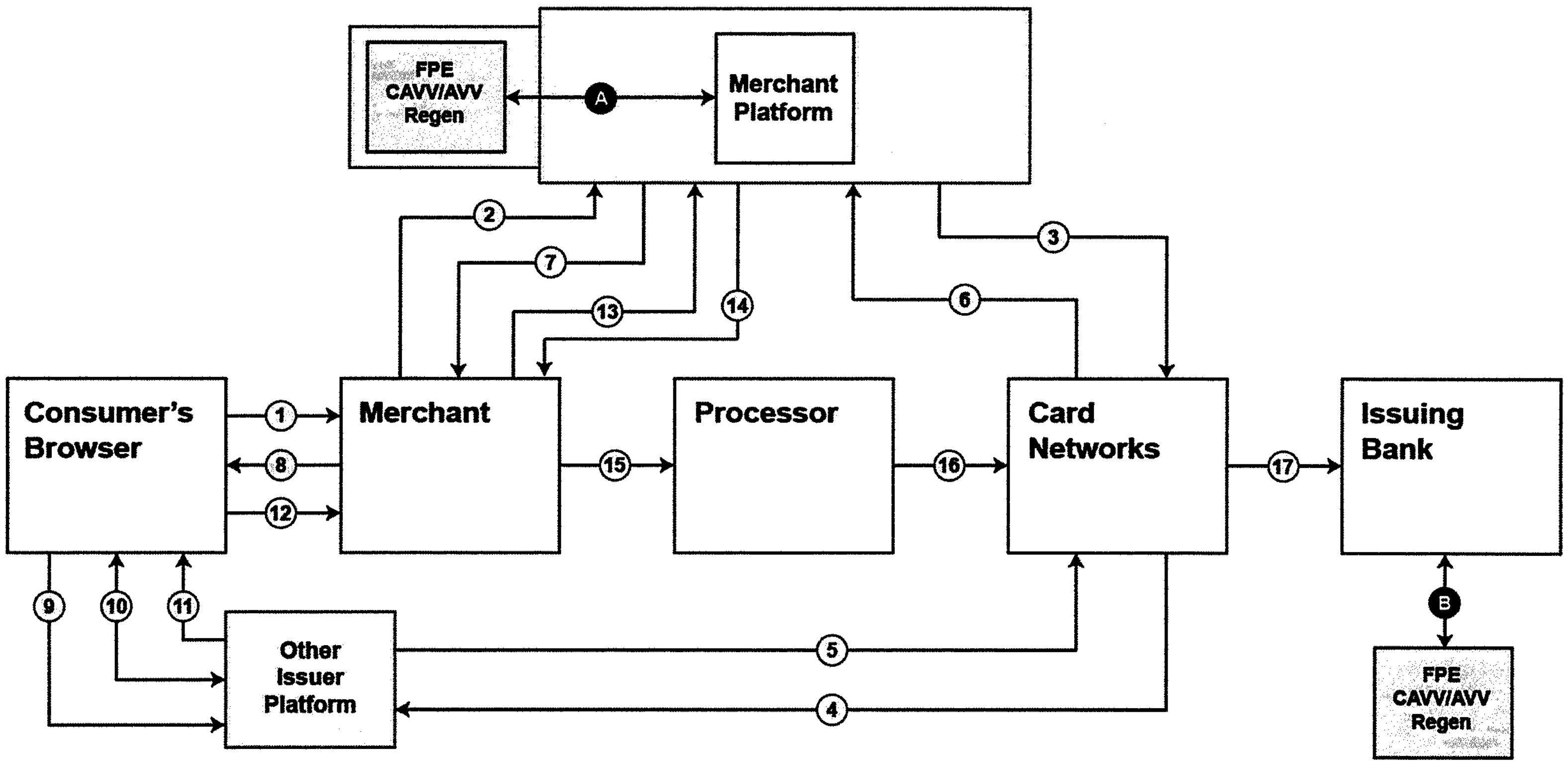
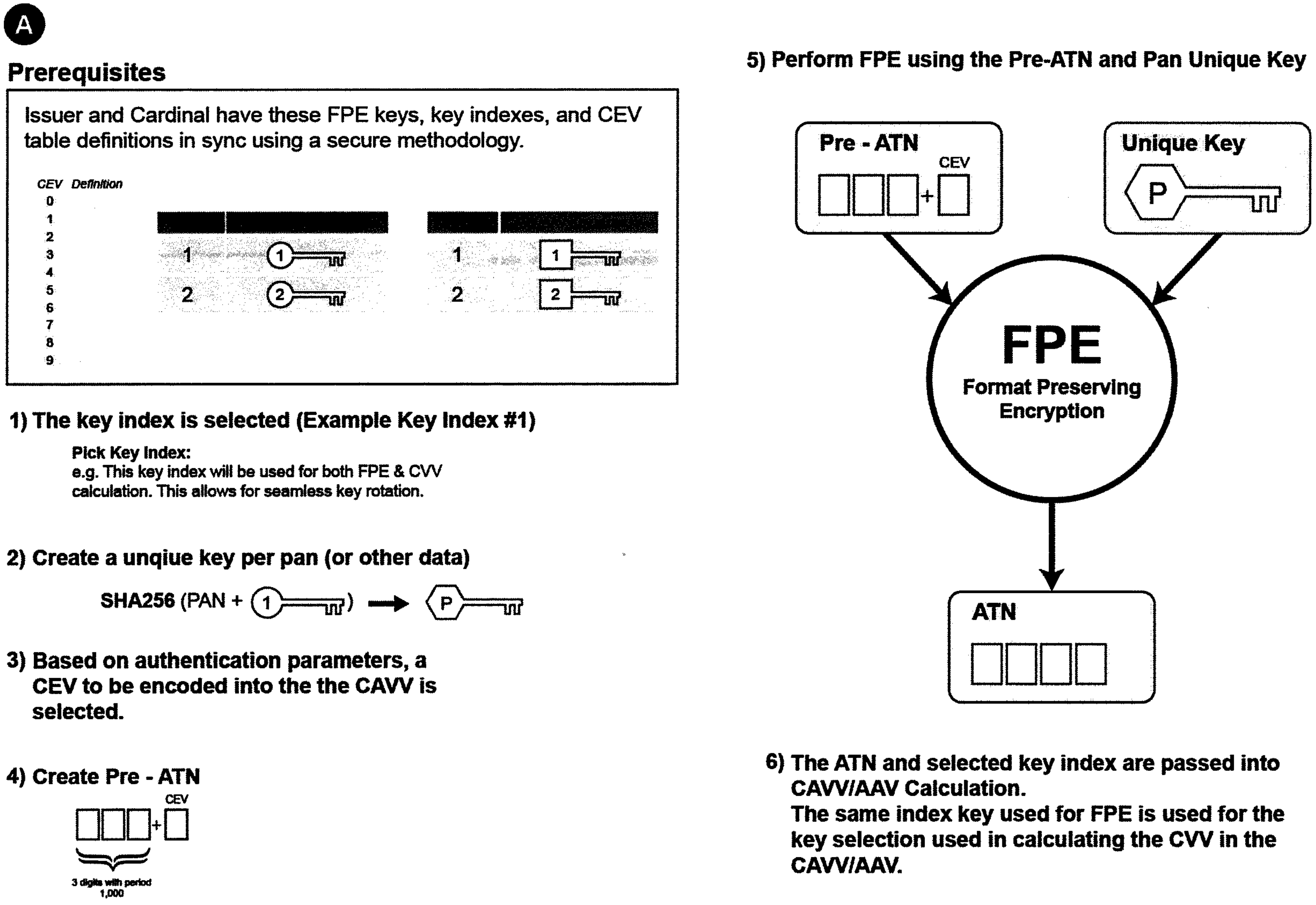


Figure 2



Prerequisites

Issuer and Cardinal have these FPE keys, key indexes, and CEV table definitions in sync using a secure methodology.

CEV	Definition
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

1) The key index is selected (Example Key Index #1)

Pick Key Index:
e.g. This key index will be used for both FPE & CVV calculation. This allows for seamless key rotation.

2) Create a unqiue key per pan (or other data)

SHA256 (PAN + 1) → P

3) Based on authentication parameters, a CEV to be encoded into the the CAVV is selected.

4) Create Pre - ATN

5) Perform FPE using the Pre-ATN and Pan Unique Key

6) The ATN and selected key index are passed into CAVV/AAV Calculation.
The same index key used for FPE is used for the key selection used in calculating the CVV in the CAVV/AAV.

Figure 3

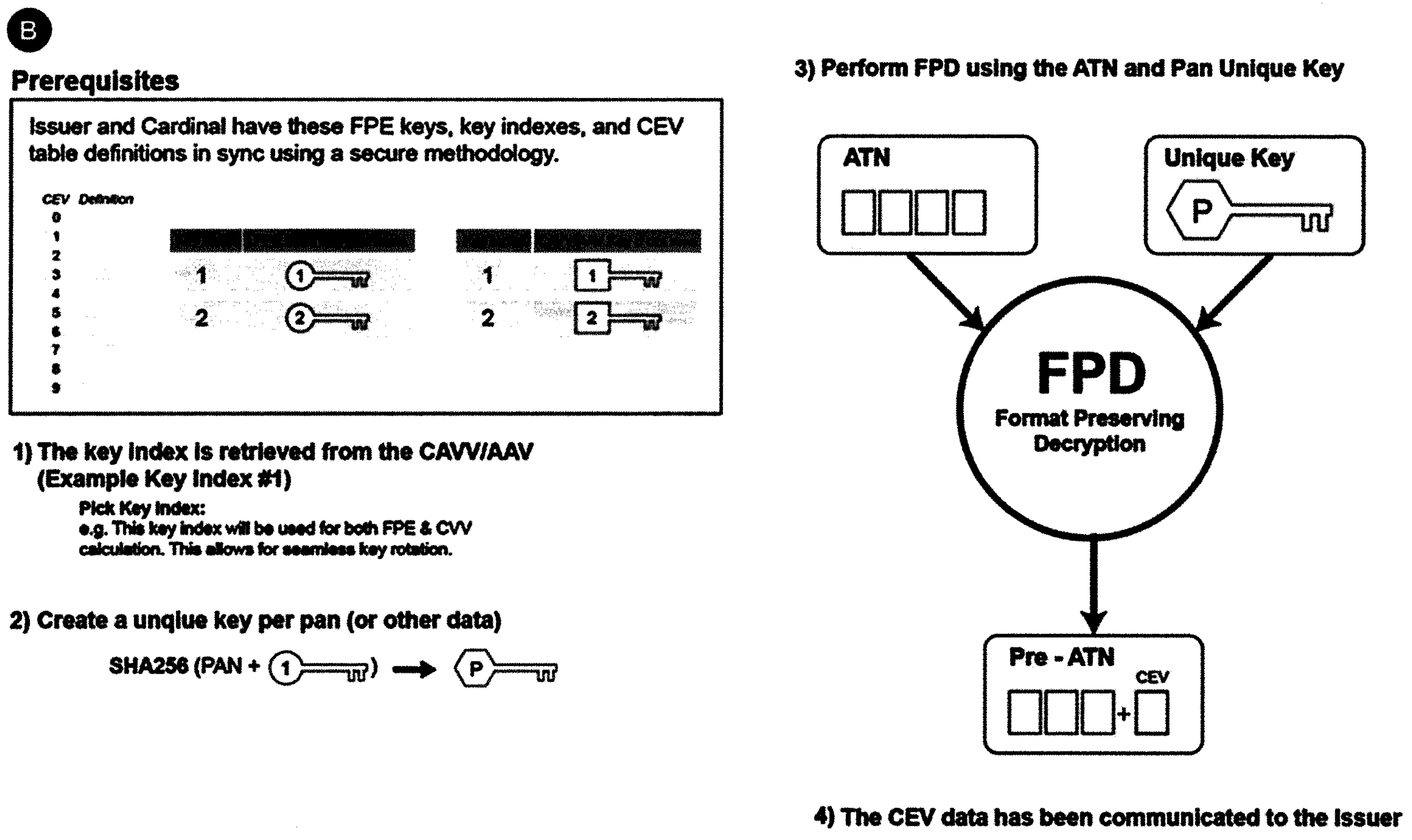

B
Prerequisites
Issuer and Cardinal have these FPE keys, key indexes, and CEV table definitions in sync using a secure methodology.
CEV Definition
0
1
2
3
4
5
6
7
8
9
1
1
2
2
1
1
2
2
1) The key index is retrieved from the CAVV/AAV (Example Key Index #1)
Pick Key Index:
e.g. This key index will be used for both FPE & CVV calculation. This allows for seamless key rotation.
2) Create a unqiue key per pan (or other data)
SHA256 (PAN + 1) → P
3) Perform FPD using the ATN and Pan Unique Key
ATN
Unique Key
P
FPD
Format Preserving Decryption
Pre - ATN
CEV
+
4) The CEV data has been communicated to the Issuer

Figure 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2017/042197

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/32

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/318468 A1 (CARR ROBERT O [US] ET AL) 16 December 2010 (2010-12-16) abstract paragraphs [0044] - [0047] paragraphs [0079] - [0082] paragraphs [0101] - [0103] paragraphs [0122] - [0125] -----	1-16
X	US 2016/092872 A1 (PRAKASH GYAN [US] ET AL) 31 March 2016 (2016-03-31) abstract paragraphs [0021] - [0028] -----	1-16
A	US 2011/103579 A1 (MARTIN LUTHER W [US] ET AL) 5 May 2011 (2011-05-05) abstract paragraphs [0009], [0010] -----	1-16

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 11 September 2017	Date of mailing of the international search report 19/09/2017
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Di Felice, M

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/042197

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010318468 A1	16-12-2010	NONE	
US 2016092872 A1	31-03-2016	NONE	
US 2011103579 A1	05-05-2011	US 2011103579 A1 US 2015134972 A1	05-05-2011 14-05-2015