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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2011 (15.09.2011)

PCT

(10) International Publication Number
WO 2011/112394 A3

(51) International Patent Classification:
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/US2011/026747

(22) International Filing Date:
1 March 2011 (01.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/312,196 9 March 2010 (09.03.2010) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, M1-11F, San Francisco, California 94128 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAMMAD, Ayman** [US/US]; 6981 Corte Mercado, Pleasanton, California 94566 (US).

(74) Agents: **GHAZANFARI, Faryar** et al.; Kilpatrick Townsend And Stockton LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA, California 94111-3834 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD INCLUDING DYNAMIC VERIFICATION VALUE

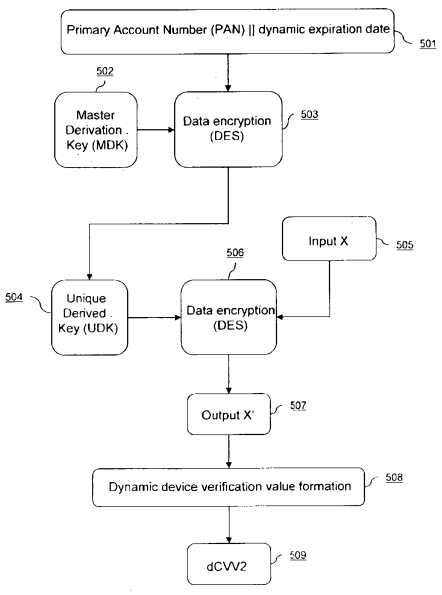


FIG. 5

(57) Abstract: System and methods for generating a dynamic verification value for electronic payment transactions are disclosed. An account identifier and an account attribute associated with an account of a user are received at a server computer. A dynamic account attribute is created and concatenated with the account identifier. The concatenated account identifier and the dynamic account attribute are then used to generate a dynamic verification value. The dynamic verification value and the dynamic account attribute are then sent to a user communication device and used for authentication in a payment transaction.

WO 2011/112394 A3

WO 2011/112394 A3

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
5 January 2012

SYSTEM AND METHOD INCLUDING DYNAMIC VERIFICATION VALUE

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a non-provisional application of and claims priority to U.S. Provisional Application No. 61/312,196, filed on March 9, 2010, the entire disclosure of which is incorporated herein by reference for all purposes.

BACKGROUND

[0002] There is a need for more secure data transfer when paying for goods and services using payment cards such as debit and credit cards.

[0003] In a typical payment transaction, a user may use a credit card to purchase an item at a merchant or enter his account information into a payment page of a merchant's website. The merchant then generates an authorization request message using a POS (point of sale) terminal when the user is present at the merchant location. Alternatively, for an online transaction, the merchant website may generate an authorization request message for card-not-present (CNP) transactions. In either instance, the authorization request message is passed to the issuer of the credit card, and the issuer may approve or deny the request to authorize the transaction.

[0004] There are a variety of methods by which fraudsters attempt to obtain account information of users for conducting fraudulent transactions. Such transactions are susceptible to "man in the middle" attacks whereby an unauthorized person intercepts information between the merchant and the issuer.

[0005] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0006] Embodiments of the invention disclosed herein include systems and methods for generating dynamic verification values for use in the electronic payment transactions.

[0007] One embodiment of the invention is directed to a method comprising receiving an account identifier (e.g., an account number) and an account attribute (e.g., an expiration date) associated with an account such as a credit card account.

The method also includes generating a dynamic account attribute (e.g., a dynamic expiration date) from the account attribute associated with the account, and generating a dynamic verification value (e.g., a dCVV or dynamic card verification value) using the account identifier and the dynamic account attribute. In some embodiments, the generation of the dynamic verification value may include concatenating the account identifier and the dynamic account attribute. The dynamic verification value and, optionally, the dynamic account attribute, can then be used to authenticate the account or a portable consumer device associated with the account.

[0008] Another embodiment of the invention is directed to a method comprising using the concatenated account identifier and the dynamic account attribute as an input into an algorithm that encrypts the concatenated account identifier and the dynamic account attribute using a Master Derivation Key (MDK). The algorithm then generates a Unique Derived Key (UDK).

[0009] Another embodiment of the invention is directed to a method comprising sending an account identifier and an account attribute associated with an account to a server computer, receiving a dynamic verification value and a dynamic account attribute, and sending the dynamic verification value and the dynamic account attribute to a second server computer. The second server computer uses the dynamic verification value and the dynamic account attribute for authentication.

[0010] Another embodiment if the invention is directed to a method including using the dynamic verification value and the dynamic account attribute in an authorization request message.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows a system according to an embodiment of the invention.

[0013] FIG. 2 shows a user communication device according to an embodiment of the invention.

[0014] FIG. 3 illustrates a flowchart that shows the steps involved in generating a dynamic verification value, according to an embodiment of the invention.

[0015] FIG. 4 illustrates a flowchart that shows the steps involved in concatenating an account identifier with a dynamic expiration date, according to an embodiment of the invention.

[0016] FIG. 5 shows the process of generating a dynamic verification value, according to an embodiment of the invention.

[0017] FIG. 6 illustrates a diagram that shows an example of a portable consumer device and a payment page of a merchant website, according to an embodiment of the invention.

[0018] FIG. 7 shows a block diagram of a computer apparatus according to an embodiment of the invention.

DETAILED DESCRIPTION

[0019] In order to provide more security for electronic transactions, additional security data may be used during the processing of electronic payment transactions. Such data can be generated by an external source and introduced into the transaction process at any point, and then verified by a processing entity or the issuer of the debit or credit card to make sure that the transaction has originated from an authorized source.

[0020] One embodiment of the invention is directed to a method comprising receiving, by a server computer associated with a payment processing network and from a user computer, an account number and an account attribute such as an expiration date associated with an account such as a credit card account. The expiration date and the account number may further be associated with a credit card or other portable consumer device. The method also includes generating, by the server computer, a dynamic account attribute such as a dynamic expiration date from the account attribute associated with the account. In the method, the server computer may also generate a dynamic verification value such as a dCVV or dynamic card verification value using the account identifier and the dynamic account attribute.

[0021] The dynamic verification value and, optionally, the dynamic account attribute, can then be used to authenticate the account or a portable consumer device associated with the account. For example, in some embodiments, the dCVV value and the dynamic expiration date can be entered onto a web page on a

merchant's Web site. This data can then be transmitted in an authorization request message from the merchant's website to a payment processing network that is located between many issuers and acquirers. The server computer associated with the payment processing network may then receive the dCVV value and the dynamic expiration date. It may then independently generate the dCVV and the dynamic expiration date and compare it to the dCVV and the dynamic expiration date received from the merchant's website. If they match, then the transaction may then be considered to be authentic.

[0022] An indication of the authenticity of the transaction (e.g., in the form of an authentication score) may then be passed in the authorization request message to the issuer of the account. The issuer of the account may then decide whether or not to authorize the transaction, and may then send an authorization response message back to the merchant website. It may indicate whether or not the issuer approved of the transaction. Then, at the end of the day, a clearing and settlement process can take place.

[0023] Prior to discussing specific embodiments of the invention, a number of terms may be discussed in further detail.

[0024] As used herein, "account identifier" can refer to an identifier for an account. It may comprise any suitable number of characters (e.g., numbers and/or letters) suitable for identifying an account. For example, an account identifier may be a Primary Account Number (PAN) of a credit or debit card. The Primary Account Number (PAN) may include numbers and/or letters and may be in any length. Other examples of account identifiers may include a name of the account holder, an address associated with the account, a phone number associated with an account, a password associated with the account, etc.

[0025] As used herein, "account attribute" can refer to any data that does not change frequently and is relatively static. It may be associated with a portable consumer device such as a payment card. If they change at all, account attributes typically do not change more than once per year. Examples of account attributes may include, without limitation, an expiration date for payment card, an account holder's name, a service code, and a CVV2 or CVV value. In some embodiments, the account attribute includes data that is stored or present on a payment card (e.g., an expiration date or CVV value).

[0026] As used herein, an "authorization request message" may be a message that includes an issuer account identifier. The issuer account identifier may be a payment card account identifier associated with a payment card. The authorization request message may request that an issuer of the payment card authorize a transaction. An authorization request message according to an embodiment of the invention may comply with ISO 8583, which is a standard for systems that exchange electronic transactions made by cardholders using payment cards. In embodiments of the invention, an authorization request message may include, among other data, an account identifier, one or more account attributes, an amount of the transaction (which may be any type and form of a medium of exchange such a money or points), and identification of a merchant (e.g., a merchant verification value or a merchant ID). Typically, an authorization request message is generated by a server computer (if the transaction is an e-commerce transaction) or a Point of Sale (POS) device (if the transaction is a brick and mortar type transaction) and is sent to an issuer via a payment processing network and an acquirer.

[0027] As used herein, "user communication device" can refer to an electronic device capable of communication with other electronic devices. For example, user communication device may be a desktop computer, laptop computer, netbook computer, tablet computer (e.g. iPad), mobile phone, verification token (described in detail later) and any other electronic device that can be coupled to another electronic device either wirelessly or via a direct connection.

[0028] As used herein "dynamic verification value" (e.g., a dynamic device verification value, a dynamic card verification value, and a dCVV2 value) can refer to a value that can be used to verify that a transaction (and in some cases a portable consumer device used to conduct a transaction) is authentic. It may be a numeric or alpha-numeric value that is generated by an algorithm (e.g. encryption algorithm) that uses account data such as account identifier and account attribute as inputs.

[0029] As used herein, a "server computer" is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a web server.

[0030] Embodiments of the invention disclosed herein include systems and methods for dynamically generating a verification value and for utilizing it to verify that a transaction originates from an authorized source and that a portable consumer device (e.g., debit or credit card) or other means used to conduct the transaction is authentic.

[0031] Embodiments of the present invention are able to maintain or improve existing user experiences, minimize the adverse impacts on merchant processes/systems, leverage existing network data transport mechanisms, utilize existing issuer validation infrastructure, support multiple forms of implementation, and maintain consistency with broader authentication strategies.

[0032] Further details regarding dynamic verification values can be found in U.S. Patent Application No. 12/712,148, filed on February 24, 2010, U.S. non-provisional Application No. 12/939,963 filed on November 4, 2010, and U.S. non-provisional Application No. 12/878,947 , filed on September 9, 2010 which are herein incorporated by reference in their entirety for all purposes.

I. SYSTEMS

[0033] Fig. 1 shows a block diagram illustrating the components of a system according to an embodiment of the invention. Fig. 1 shows a user **110** and a portable consumer device **112** that the user **110** may use to conduct a payment or other type of transaction. The user **110** may also operate a mobile device **118**, a user computer **120**, and a verification token **122**. When purchasing a good or service from the Internet, the user **120** may contact a merchant website **130** run on a server computer **131**.

[0034] Further elements of the system may include an acquirer **140**, a payment processing network **150**, an IP Gateway **152**, and an issuer **160**. The IP Gateway may include an IP Gateway server computer **153** while the payment processing network **150** may include a payment processing network server computer **155**. The IP gateway server computer **153** may include a computer readable medium **154**, a processor **155**, and a generation module **151**. The payment processing network server computer **155** may include a data processor **156**, and a comparison module **158**. A database **159** may be operatively coupled to the server computer **155**.

[0035] As noted above, the user **110** can use the portable consumer device **112**, the mobile device **118**, and the user computer **120**. The user **110** interacts with the merchant website **130** using the user computer **120** and/or mobile device **118**. The mobile device **118**, the verification token **122** and the user computer **120** are capable of communicating with the IP Gateway **152** for requesting and receiving a dynamic verification value (this process will be described in detail later). The merchant website **130** is in communication with the acquirer **140**. The acquirer **140** is in communication with the issuer **160** through the payment processing network **150**. The payment processing network **150** is in communication with the IP Gateway **152**. The IP Gateway **152** has access to the payment processing network server computer **155**.

[0036] The user **110** can be an individual or organization such as a business that is capable of purchasing goods or services or making any suitable payment transaction with the merchant website **130**.

[0037] The portable consumer device **112** can be any suitable device that can be used to conduct a payment transaction, and may be in any suitable form. For example, suitable portable consumer devices **112** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices **112** include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. In some cases, the portable consumer device **112** may be associated with an account of user **110** such as a bank account.

[0038] Portable consumer device **112** may include a contactless element **114** that includes a processor (not shown), an antenna (not shown), computer readable media (not shown), and one or more applications stored on the computer readable media that operate in concert to allow the portable consumer device **112** to wirelessly send its stored card data to a wireless reader. The contactless element **114** provides Near Field Communication (NFC) capability for the portable consumer device **112** such that when the portable consumer device **112** is in close proximity of a wireless reader, the wireless reader powers the contactless element **114** and collects the card data.

[0039] The mobile device **118** may be in any suitable form. For example, suitable mobile device **118** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). Some examples of the mobile device **118** include desktop or laptop computers, cellular phones, personal digital assistants (PDAs), pagers, and the like. In some embodiments, the mobile device **118** and the portable consumer device **112** can be embodied in the same device.

[0040] The user computer **120** may be a personal computer, phone, or a laptop computer. The user computer **120** may run an operating system such as Microsoft Windows™ and may have a suitable browser such as Internet Explorer™.

[0041] The verification token **122** can be an electronic device configured to be coupled to, or can be present within, the user computer **120** and can be capable of wirelessly receiving card data from the portable consumer device **112**. Elements of the verification token **122** and their operation will be described later with reference to Fig. 2.

[0042] The merchant website **130** may be in the form of a website hosted by one or more server computers (e.g. server computer **131**). The user **110** is capable of communicating with the merchant website **130** using the user computer **120** and/or mobile device **118**.

[0043] The acquirer **140** can be any suitable entity that has an account with a merchant associated with the merchant website **130**. In some embodiments, the issuer **160** may also be the acquirer **140**.

[0044] The payment processing network **150** can be a network of suitable entities that have information related to an account associated with the portable consumer device **112**. This information includes data associated with the account on the portable consumer device **112** such as profile information, data, and other suitable information. Such data may be stored in one or more databases such as the database **159** and may be accessible by one or more server computers such as the server computer **155**.

[0045] The payment processing network **150** may have or operate a server computer and may include a database (e.g. the server computer **155** and the database **159**). The database may include any hardware, software, firmware, or combination of the preceding for storing and facilitating retrieval of information. Also,

the database may use any of a variety of data structures, arrangements, and compilations to store and facilitate retrieval of information. The server computer may be coupled to the database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. Server computer may comprises one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0046] The payment processing network **150** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network **150** may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network **150** may use any suitable wired or wireless network, including the Internet.

[0047] The IP Gateway **152** can refer to an entity that includes one or more servers such as IP Gateway server computer **153**. The IP Gateway **152** may also include one or more databases (not shown), and have access to issuer data, transaction data and user data. This data may be used to authenticate portable consumer devices. The IP Gateway **152** also generates and delivers notifications and alert messages to various delivery channels. The IP Gateway **152** may be part of the payment processing network **150** or may be a separate entity in communication with payment processing network **150**.

[0048] The databases **159** may be server computers that are capable of storing data and responding to queries from client computers. The database **159** may also be in the form of stand-alone hard drives connected to one or more server computers that retrieve the data from the database **159** as result of queries from client computers.

[0049] As used herein a "computer readable medium" or "computer readable storage medium" is typically a storage medium such a hard disk or any suitable type of data storage medium capable of storing data such as program codes.

[0050] The comparison module **158** can be a software program stored on the computer readable medium, and run by the processor **156**, that monitors the stream of data in an electronic payment transaction and compare various types of data in the electronic payment transaction such as the dynamic verification value with the same type of data supplied by the IP Gateway **152** or any other entity to make sure the data that are part of the electronic payment transactions are accurate and are originated from an authorized source.

[0051] The generation module **151** can be software program stored on the computer readable medium **154** and run by the processor **155** that generates a dynamic verification value. The generation module **151** may also be embodied as a Hardware Security Module (HSM) that generates a dynamic verification value.

[0052] The issuer **160** can be any suitable entity that may open and maintain an account associated with the portable consumer device **112** for the user **110**. Some examples of issuers may be a bank, a business entity such as a retail store, or a governmental entity. In many cases, the issuer **160** may also issue the portable consumer device **112** associated with the account to the user **110**.

[0053] Fig. 2 is a block diagram illustrating various components of the verification token **122** according to one embodiment.

[0054] The embodiment illustrated in Fig. 2 is a USB device that includes a USB connectivity module **230**, a secure element **220** (e.g., a smart card chip), a wireless/contactless reader **210** capable of reading card data (payment data) from a portable consumer device, a built in memory **240**, a self-installing driver **250**, a form fill application **260**, a terminal application **270**, and a heartbeat application **280**. The verification token **122** may also have other features such as a keyboard buffer capability and a unique serial number associated with the verification token. The verification token **122** has no footprint on the user computer **120** with internet connectivity when it is plugged in. The various components and modules on the verification token **122** can be used to implement methods according to embodiments of the invention.

[0055] Although Fig. 2 illustrates a verification token **122** as something similar to a USB stick, the verification token **122** may come in other forms. For example, it may be piece of hardware or other module installed in a computer, consumer device, or other device. For example, in other embodiments, the verification token may be

housed in a computer and need not be a device that is physically separated from the computer.

II. METHODS

[0056] In a typical transaction process, the user **110** may take his portable consumer device **112** and may interact with the verification token **122**. For example, the portable consumer device **112** may be a contactless payment card, and the contactless payment card can be placed near the verification token. Information such as the Primary Account Number (PAN) as well as the expiration date may then pass from the portable consumer device **112**, to the verification token **122**, to the user computer **120**, and to the IP Gateway **152**. The IP Gateway **152** may then receive this information, and this may cause the IP Gateway **152** to generate a dynamic verification value.

[0057] In the embodiments of the invention, a dynamic verification value may be generated by the generation module **151** in the server computer **153** of the IP Gateway **152** and delivered to a user communication device such as the user computer **120**/verification token **122** combination, and the mobile device **118**. In some embodiments, the user communication device that receives the dynamic verification value may be utilized in the process of performing an electronic payment transaction (this process will be described in detail below). In some embodiments, a dynamic verification value may be received by a user communication device (e.g., the mobile device **118**) and the user **110** may manually enter the dynamic verification value in a payment page of a website.

[0058] Before or after sending the dynamic verification value to a user communication device, the IP Gateway server computer **153** may also send the dynamic verification value to the payment processing network server computer **155** in the payment processing network **150**. In one embodiment, the payment processing network **150** may also contact the IP Gateway **152** to receive the dynamic verification value at any time. A program in the payment processing network server computer **155** associates the dynamic verification value with a corresponding account number associated with the user **110**. The account number of the user **110** may be issued by the issuer **160**. In some embodiments, which will be described in detail later, the payment processing network **150** may independently generate the dynamic verification value based on the data received in an

authorization request message and may then compare the generated dynamic verification value the one that was accompanied by the authorization request message.

[0059] When the user **110** purchases goods or services from the merchant website **130** using the user computer **120**, the dynamic verification value is entered in the payment page of the merchant website **130** either automatically via the verification token **122** or manually by the user **110**. After the merchant website **130** receives transaction details including name and address of the user **110**, the account identifier and account attributes, and the payment amount, it then generates an authorization request message which is sent to the acquirer **140**. The acquirer **140** forwards the authorization request message to the payment processing network **150**.

[0060] Upon receipt of the authorization request message, the payment processing network **150** compares the dynamic verification value included in the authorization request message, with the dynamic verification value that was received from the IP Gateway **152** (more specifically, the IP Gateway server computer **153**) or the dynamic verification value that the payment processing network **150** independently generates. This is done via the comparison module **158** which runs on the payment processing network server computer **155**.

[0061] The server computer **155** in the payment processing network **150** then determines whether the dynamic verification value that was included in the authorization request message matches with the copy that was provided by the IP Gateway **152** or that was generated independently from data that are provided in the authorization request message. In one embodiment, the payment processing network **150** then forwards the authorization request message to the issuer **160** along with an indicator that specifies whether there was a match between the dynamic verification values. In one embodiment, if the dynamic verification values do not match, payment processing network **150** may decline the transaction on behalf of the issuer **160**. The issuer **160** or the payment processing network **150** can then generate an authorization response message which indicates whether the transaction is approved or declined. The authorization response message is forwarded to the acquirer **140** and then to the merchant **130**.

[0062] Two specific embodiments in which the user **110** may use a user communication device to request and receive a dynamic verification value will now

be described. It will be understood by those skilled in the art that other ways may be used to request, receive and use the dynamic verification value to conduct an electronic payment transaction.

[0063] Referring to FIG. 1, in an embodiment of the invention, the user **110** may receive a verification token **122** such as the one illustrated in FIG. 2 from his or her financial institution (issuer **160**, for example). Alternatively, a user may receive a verification token **122** from another entity on behalf of a financial institution.

[0064] The user **110** can then connect the verification token **122** to the USB port of his user computer (user computer **120**, for example). The verification token **122** is then powered by the user computer, and it is recognized as a valid device. The verification token **122** can also self-install via the self-installing driver **250** (shown in FIG. 2), and then ping the user computer **120** to check for internet connectivity.

[0065] If Internet connectivity is available, the verification token **122** can then automatically attempt to establish a background SSL session to the IP Gateway **152** through a predefined IP address, using the user computer **120,** so that it can be used as a part of an authentication process. A terminal application **270** and heartbeat application **280** may be used to establish and maintain this connection. If the session connection is successfully established, the verification token **122** identifies itself to the IP Gateway **152** by providing its unique serial number and/or IP address.

[0066] When the user **110** is ready to submit his/her payment information to the merchant website **130**, he/she holds the portable consumer device **112** in close proximity of the verification token **122**. Card data (i.e. account data) associated with the portable consumer device **112** are received by the verification token **122** from the contactless element **114** of the portable consumer device **112**. The verification token **122** encrypts the card data and sends them to the IP Gateway **152** via the previously established SSL session described above. When the IP Gateway **152** receives the encrypted data, the authenticity of the information is validated by validating the account number associated with the portable consumer device **112**. The IP Gateway **152** generates a dynamic verification value based on a predetermined algorithm, and sends the dynamic verification value to the verification token **122**. The dynamic verification value is automatically form-filled in the payment page of the merchant website **130** by the form-fill application **260** shown in FIG. 2.

[0067] When the dynamic verification value is submitted to the merchant website **130**, the merchant website **130** then generates an authorization request message which is sent to the acquirer **140**. Acquirer **140** passes the authorization request to the payment processing network **150**. Payment processing network **150** compares the dynamic verification value that is in the authorization request message from the acquirer **140** (which is received from the merchant website **130**) to the dynamic verification value that is received from the IP Gateway **152** or the dynamic verification value that was independently generated by the payment processing network **150**. This is performed by the comparison module **158**. If they match, the payment processing network **150** sends the authorization request message to the issuer **160**. The issuer **160** generates an authorization response message which indicates whether the transaction is approved or declined. The authorization response message is sent to the payment processing network **150** which then sends it to the acquirer **140**. The acquirer **140** informs the merchant associated with the merchant website **130** about the result.

[0068] In another embodiment, the user **110** requests and receives the dynamic verification value using the mobile device **118**. The user **110** then initiates a request by sending an SMS from the mobile device **118** to the IP Gateway **152**. When the IP Gateway **152** receives the request, the phone number and the Primary Account Number (PAN) associated with the mobile device **118** are identified. The IP Gateway **152** then validates the account number associated with the portable consumer device **112** and phone number of the mobile device **118**. The IP Gateway **152** generates a dynamic verification value, based on a predetermined algorithm, which is sent to the mobile device **118**. The mobile device may receive the dynamic verification value via SMS or through application that communicates with the IP Gateway server computer **153**. The generated dynamic verification value is also sent to the payment processing network **150**. Then, user **110** enters the dynamic verification value at the payment page of the merchant website **130** along with the payment information to purchase goods or services. The mobile device **118** may also have a form-fill application that automatically form-fills the dynamic verification value into a payment page of a web site accessed via the mobile device **118**.

[0069] GENERATION OF A DYNAMIC VERIFICATION VALUE

[0070] A method of the generating a dynamic verification value will now be described with reference to the Figures. In the embodiments of the invention, the dynamic verification value may be generated from the account identifier (e.g. a Primary Account Number (PAN)), and one or more account attributes (e.g. an expiration date). FIGs. 3-5 illustrate the process of generating the dynamic verification value according to an embodiment of the invention. As shown in FIG. 3, in step **S301** the IP Gateway **152** receives an account identifier (e.g. the Primary Account Number (PAN)) and an account attribute (e.g. the expiration date) associated with the portable consumer device **112** of the user **110** from the verification token **122** or the mobile device **118**.

[0071] Optionally, the IP Gateway **152** verifies that the account identifier and the account attributes such as the expiration date are valid. This step which is not shown in the flowchart of the FIG. 3, may be performed by the payment processing network **150** at the time of receiving an authorization request message.

[0072] In step **S302**, the IP Gateway **152** generates a dynamic expiration date from the expiration date associated with the portable consumer device **112**. In step **S303**, the account identifier (e.g. the Primary Account Number (PAN)) is concatenated with an account attribute (e.g. the expiration date).

[0073] This process is further illustrated in the flowchart of FIG. 4. In FIG. 4, an example of an account identifier in the form of a 16-digit Primary Account Number (PAN) and an account attribute in the form of the expiration date are shown. In step **S401** the Primary Account Number (PAN) and an expiration date associated with a portable consumer device are obtained. At step **S402** a dynamic expiration date is generated from the expiration date, and at step **S403** the dynamic expiration date is concatenated with the Primary Account Number (PAN). In some embodiments, the dynamic expiration date may be generated via an algorithm that accepts the expiration date as an input and uses a predetermined formula to generate a dynamic expiration date.

[0074] Referring back to FIG. 3, at step **S304** the concatenated account identifier (e.g. Primary Account Number (PAN)) and the dynamic account attribute (e.g. dynamic expiration date) are inputted into a key derivation algorithm. In step **S305**, a Unique Derived Key (UDK) that is obtained from the key derivation algorithm

is inputted into another algorithm that generates a dynamic verification value. The dynamic verification value is then provided to the verification token **122** or the mobile device **118**.

[0075] The process described in steps **S304** and **S305** in FIG. 3 will now be described in detail with reference to FIG. 5. As shown in FIG. 5, the data string **501** which may be formed by concatenation of the account identifier (e.g. the Primary Account Number (PAN)) and the dynamic account attribute (e.g. dynamic expiration date) can be altered (i.e. encrypted) to form a Unique Derived Key (UDK) **504**. In this process, which is referred to as the key derivation process, the data string **501** is inputted into a data encryption algorithm **503** (also referred to as the key derivation algorithm) such as DES or triple-DES, for example. The Master Derivation Key (MDK) **502** is then used to encrypt the data string **501**. The value resulting from the encryption algorithm **503** is the Unique Derived Key (UDK) **504**.

[0076] In some embodiments, the data string **501** may be formed from concatenation of more than two types of account data. For example, data string **501** may be formed by concatenating the Primary Account Number (PAN), a sequence number which changes with each transaction and the dynamic expiration date. Utilization of more account data to form the data string **501** results in a more complex and secure Unique Derived Key (UDK) **504**. Although concatenation of an account identifier and an account attribute are described in detail, embodiments of the invention are not limited to concatenation and such data elements can merely be used as inputs to form a dynamic verification value.

[0077] In some embodiments, the data encryption algorithm **503** may not be able to accepts an input that is larger than a pre-determined number of bits/bytes. In such embodiments, the data string **501** may be truncated as needed. In some other embodiments, the data encryption algorithm may expect an input that is larger than a pre-determined bits/bytes. In such embodiments, the data string **501** may be padded with zeros at either end.

[0078] The Unique Derived Key (UDK) **504** and a data encryption algorithm **506** can be used to alter (i.e. encrypt) a second data string (e.g. data string **505** "input X"). The data encryption algorithm **506** may be the same type of algorithm as the data encryption algorithm **503** or may be any other suitable encryption algorithm. Data string **505** may be the same as data string **501** or may be any other suitable

data string. In one example, data string **505** may be the account identifier (i.e. Primary Account Number (PAN)) of the portable consumer device of the user. The data string **505** is then encrypted via Unique Derived Key (UDK) **504** to form the data string **507** (i.e., output X'). The resulting data string **507** is then altered via the algorithm **508** to form a dynamic verification value **509**.

[0079] The algorithm **508** may be any suitable algorithm and may perform a suitable alteration process on the resulting data string **509**. For example, the algorithm **508** may take the last 32 bits of data (i.e. 4 digits) from the data string **507** as the dynamic verification value.

[0080] **PERFORMING A PAYMENT TRANSACTION**

[0081] The method of performing a payment transaction will now be described with reference to the figures. FIG. 6 shows the portable consumer device **600** and the payment page **601**.

[0082] The payment page **601** is a payment page of a website from which the user **110** whishes to purchase goods or services. The payment page **601** may be accessed by using user computer **120**. After choosing the goods or services, the user **110** is directed to the payment page **601** to provide the information needed to perform a payment transaction. In a typical payment transaction, the information in fields **602-610** are automatically form-filled via verification token **122**. As shown in FIG. 6, these information include: first name **602**, last name **603**, street address **604**, city **605**, state **606**, zip code **607**, account number **608**, expiration date **609** and card verification value (CVV2) **610**. FIG. 6 also shows two additional fields **611** and **612** which will be described in detail later.

[0083] The portable consumer device **600** may be embodied as data stored on a user communication device such as a mobile device. For example, a mobile device may contain an application that stores the account number, expiration date, security code and any other data needed to perform a payment transaction. Furthermore, the mobile device may be capable of Near Field Communication (NFC) with the verification token **122**. Therefore, the example of the portable consumer device **600** shown in FIG. 6 as a credit/debit card is not intended to be limiting.

[0084] As described before, the user **110** can bring his portable consumer device (e.g. portable consumer device **600**) in close proximity of the verification token **122** and the verification token **122** receives the account data including an account identifier (e.g. Primary Account Number (PAN)) and an account attribute (e.g. expiration date) from the portable consumer device of the user **110** and sends the account identifier and the account attribute, among other account data, to the IP Gateway server computer **153** and requests a dynamic verification value.

[0085] As described above, the generation module **151** of the IP Gateway server computer **153** then generates a dynamic verification value and a dynamic expiration date which are sent from the IP Gateway server computer **153** to the verification token **122**.

[0086] At this point, the dynamic verification value and the dynamic expiration date can be form-filled and/or included in the payment information in payment page **601** in several ways which will now be described in detail.

[0087] In some embodiments, In addition to the expiration date field **609** and the CVV2 field **610**, the payment page **601** may include a dynamic expiration date field **611** and the dynamic verification value (dCVV2) field **612** which will be form-filled with the dynamic expiration date and the dynamic verification value respectively. In such embodiments, the user **110** will be able to see that fields **611** and **612** are form-filled.

[0088] In some embodiments, the user **110** may not see the fields **611** and **612** shown inside the dotted square in payment page **601**. In such embodiments, the fields **611** and **612** are hidden fields which will be form-filled in the background. This is advantageous because fraudsters cannot determine that these fields exist and such data are used in the payment transaction.

[0089] In some embodiments, the CVV2 field **610** and/or expiration date field **609** may be form-filled with fake values (i.e. values different from what is displayed on the portable consumer device **600**). In such embodiments, the fields **611** and **612** may or may not be hidden fields. Using fake values is advantageous, because the fraudsters cannot determine whether the fake values shown in the fields **610** or **609** are really used or not.

[0090] In one example, the dynamic expiration date field **611** and the dynamic verification value (dCVV2) field **612** may be visible, and in addition the CVV2 field **610** may be form-filled with a fake number. However, when the data are sent to the merchant website **130**, the correct CVV2 value may be used instead of the fake value. In this example, even if a fraudster can determine the data that are form-filled in the payment page **601**, he is not aware that in the background, other values may be actually sent to the merchant website **130**. Therefore, the fraudster will not be able to perform an unauthorized payment transaction.

[0091] When the user **110** clicks on the submit or "Make Payment" button on the payment page **601**, the data that are form-filled in the payment page **601** including the fields that may not be visible, are sent to the merchant website **130**.

[0092] Merchant website **130** receives the data from the payment page **601** and generates an authorization request message. The authorization request message will include the dynamic expiration date and the dynamic verification value. As discussed before, the authorization request message may also include the actual expiration date and CVV2 or fake expiration date and/or CVV2.

[0093] The authorization request message will be sent to the payment processing network **150** through acquirer **140**. The payment processing network **150** may regenerate the dynamic verification value and the dynamic expiration date via the same method used by the IP Gateway **152** and using the comparison module **158** compare the regenerated values with the ones included in the authorization request message.

[0094] In some embodiments, the payment processing network **150** may receive the dynamic verification value and the dynamic expiration date from the IP Gateway **152**. In such embodiments, the comparison module **158** of the payment processing network **150** may compare the values that received from the IP Gateway **152** with the ones that are accompanied with the authorization request message.

[0095] Upon verification of the dynamic verification value and the dynamic expiration date, the payment processing network **150** sends the authorization request message to the issuer **160**.

[0096] It can be appreciated that the embodiments of the invention have many advantageous. Inclusion of the dynamic verification value and the dynamic

expiration date in the payment data used to generate an authorization request message is advantageous in that it is hard for fraudsters gain access to such data or to be able to generate the same values. Moreover, making the dynamic verification value and the dynamic expiration date invisible in a payment page is advantageous because fraudsters will not know that such data are used in a payment transaction. Furthermore, replacing the CVV2 field and/or the expiration date with fake values makes it harder for the fraudsters to accurately determine how such fake values are obtained and if they are actually used in a payment transaction.

[0097] The various participants and elements of the system shown in FIG. 1 may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in FIG. 1 may use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 7. The subsystems shown in FIG. 7 are interconnected via a system bus **775**. Additional subsystems such as a printer **774**, keyboard **778**, fixed disk **779** (or other memory comprising computer readable media), monitor **776**, which is coupled to display adapter **782**, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller **771**, can be connected to the computer system by any number of means known in the art, such as serial port **777**. For example, serial port **777** or external interface **781** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor **773** to communicate with each subsystem and to control the execution of instructions from system memory **772** or the fixed disk **779**, as well as the exchange of information between subsystems. The system memory **772** and/or the fixed disk **779** may embody a computer readable medium.

[0098] The software components or functions described in this application may be implemented as software code to be executed by one or more processors using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer-readable medium, such as a random access memory (RAM), a read-only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may also reside on or within a

single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0099] The present invention can be implemented in the form of control logic in software or hardware or a combination of both. The control logic may be stored in an information storage medium as a plurality of instructions adapted to direct an information processing device to perform a set of steps disclosed in embodiments of the present invention. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods to implement the present invention.

[0100] In embodiments, any of the entities described herein may be embodied by a computer that performs any or all of the functions and steps disclosed.

[0101] Any recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0102] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

WHAT IS CLAIMED IS:

1. A computer apparatus comprising:

a computer readable medium;

a processor coupled to the computer readable medium; wherein the processor is configured to execute program code stored on the computer readable medium to implement a method comprising:

receiving an account identifier and an account attribute associated with an account;

generating a dynamic account attribute from the account attribute associated with the account;

generating a dynamic verification value using the account identifier and the dynamic account attribute; and

providing the dynamic verification value and the dynamic account attribute to a verification token, wherein the dynamic verification value and the dynamic account attribute are used for authentication.

2. The system of claim 1, wherein the account identifier is a Primary Account Number (PAN) associated with the account, and wherein generating the dynamic verification value comprises concatenating the account identifier and the account attribute.

3. The system of claim 2, wherein the Primary Account Number (PAN) is associated with a portable consumer device.

4. The system of claim 1, where in the account attribute is an expiration date associated with a portable consumer device.

5. The system of claim 1, wherein the account attribute is selected from any one of a birthday and personal identification number of a user associated with the account.

6. The system of claim 1, wherein the account identifier and the dynamic account attribute are used as input for an algorithm that encrypts the concatenated account identifier and the dynamic account attribute using a Master Derivation Key (MDK).

7. The system of claim 1, wherein the account identifier and the dynamic account attribute are used as an input for an algorithm that generates a Unique Derived Key (UDK).

8. The system of claim 7, wherein the Unique Derived Key (UDK) is used for generating a dynamic verification value.

9. A method comprising:

receiving an account identifier and an account attribute associated with an account;

generating a dynamic account attribute from the account attribute associated with the account;

generating a dynamic verification value using the account identifier and the dynamic account attribute; and

providing the dynamic verification value and the dynamic account attribute to a verification token, wherein the dynamic verification value and the dynamic account attribute are used for authentication.

10. The method of claim 9, wherein the account identifier is a Primary Account Number (PAN) associated with the account, and wherein generating the dynamic verification value comprises concatenating the account identifier and the account attribute.

11. The method of claim 10, wherein the Primary Account Number (PAN) is associated with a portable consumer device.

12. The method of claim 9, wherein the account attribute is an expiration date associated with a portable consumer device.

13. The method of claim 9, wherein the account identifier and the dynamic account attribute are used as input for an algorithm that encrypts the concatenated account identifier and the dynamic account attribute using a Master Derivation Key (MDK).

14. The method of claim 9, wherein the account identifier and the dynamic account attribute are used as an input for an algorithm that generates a Unique Derived Key (UDK).

15. The method of claim 14, wherein the Unique Derived Key (UDK) is used for generating a dynamic verification value.

16. A method comprising:

sending an account identifier and an account attribute associated with an account to a first server computer.

receiving a dynamic verification value and a dynamic account attribute; and

sending the dynamic verification value and the dynamic account attribute to a second server computer, wherein the second server computer uses the dynamic verification value an the dynamic account attribute for authentication.

17. The method of claim 16, wherein the dynamic verification value and the dynamic account attribute are automatically form-filled into a payment page of a website automatically.

18. The method of claim 16, wherein the dynamic verification value and the dynamic account attribute are used to generate an authorization request message.

19. The method of claim 16, wherein the account identifier is a Primary Account Number (PAN) associated with the account.

20. The method of claim 16, wherein the account attribute is an expiration date associated with a portable consumer device.

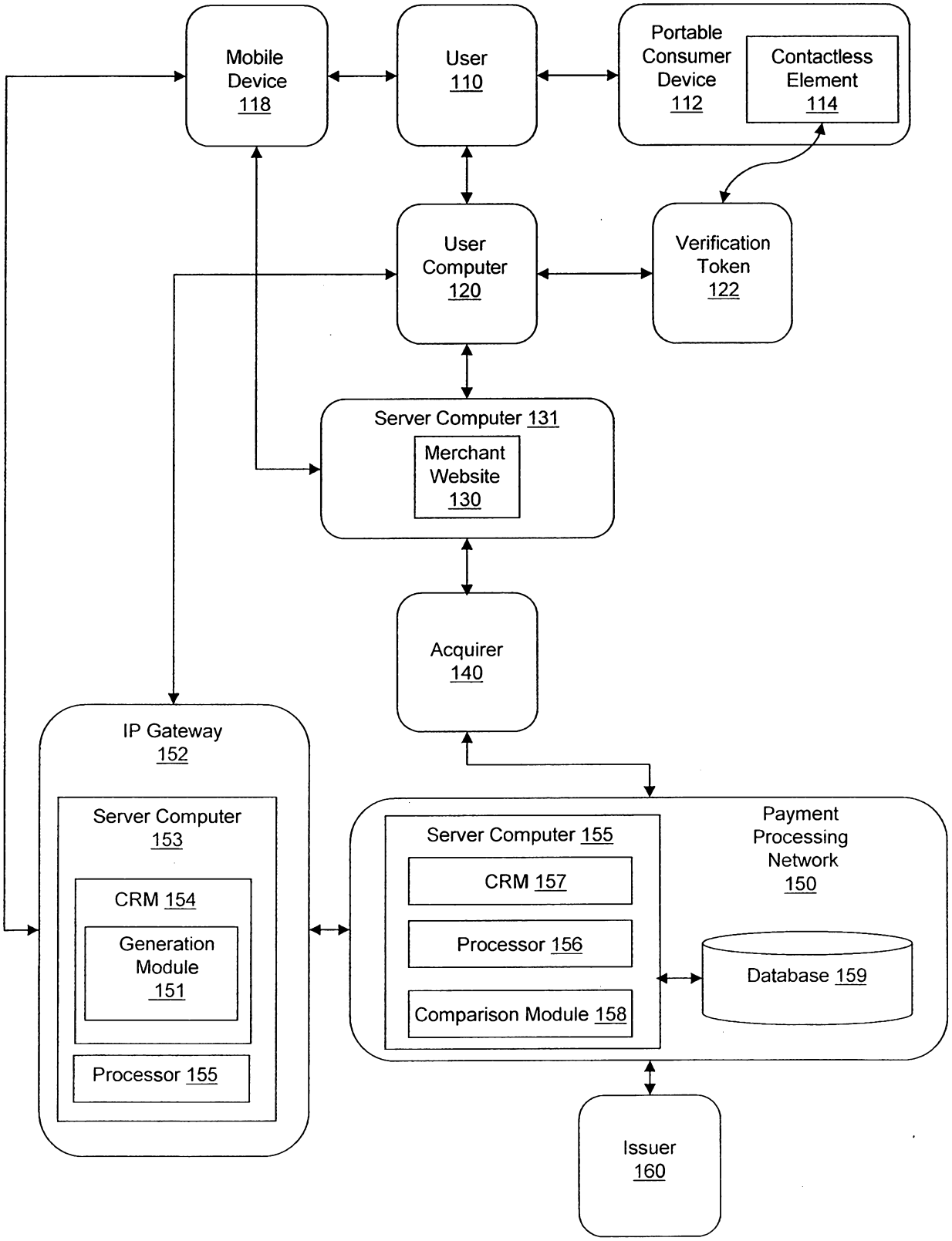

Mobile Device 118
User 110
Portable Consumer Device 112
Contactless Element 114
User Computer 120
Verification Token 122
Server Computer 131
Merchant Website 130
Acquirer 140
IP Gateway 152
Server Computer 153
CRM 154
Generation Module 151
Processor 155
Server Computer 155
CRM 157
Processor 156
Comparison Module 158
Payment Processing Network 150
Database 159
Issuer 160

FIG. 1

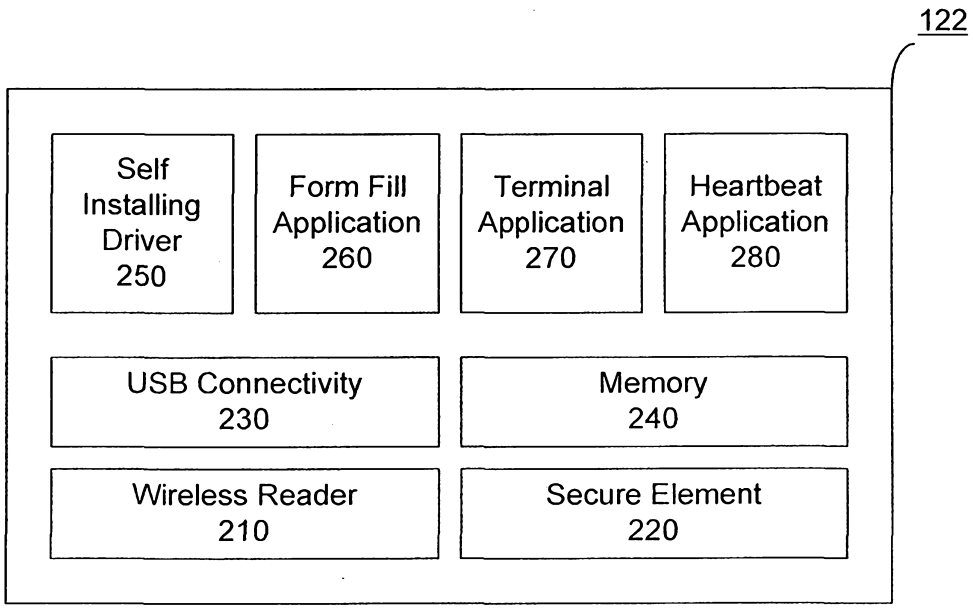

122
Self Installing Driver 250
Form Fill Application 260
Terminal Application 270
Heartbeat Application 280
USB Connectivity 230
Memory 240
Wireless Reader 210
Secure Element 220

FIG. 2

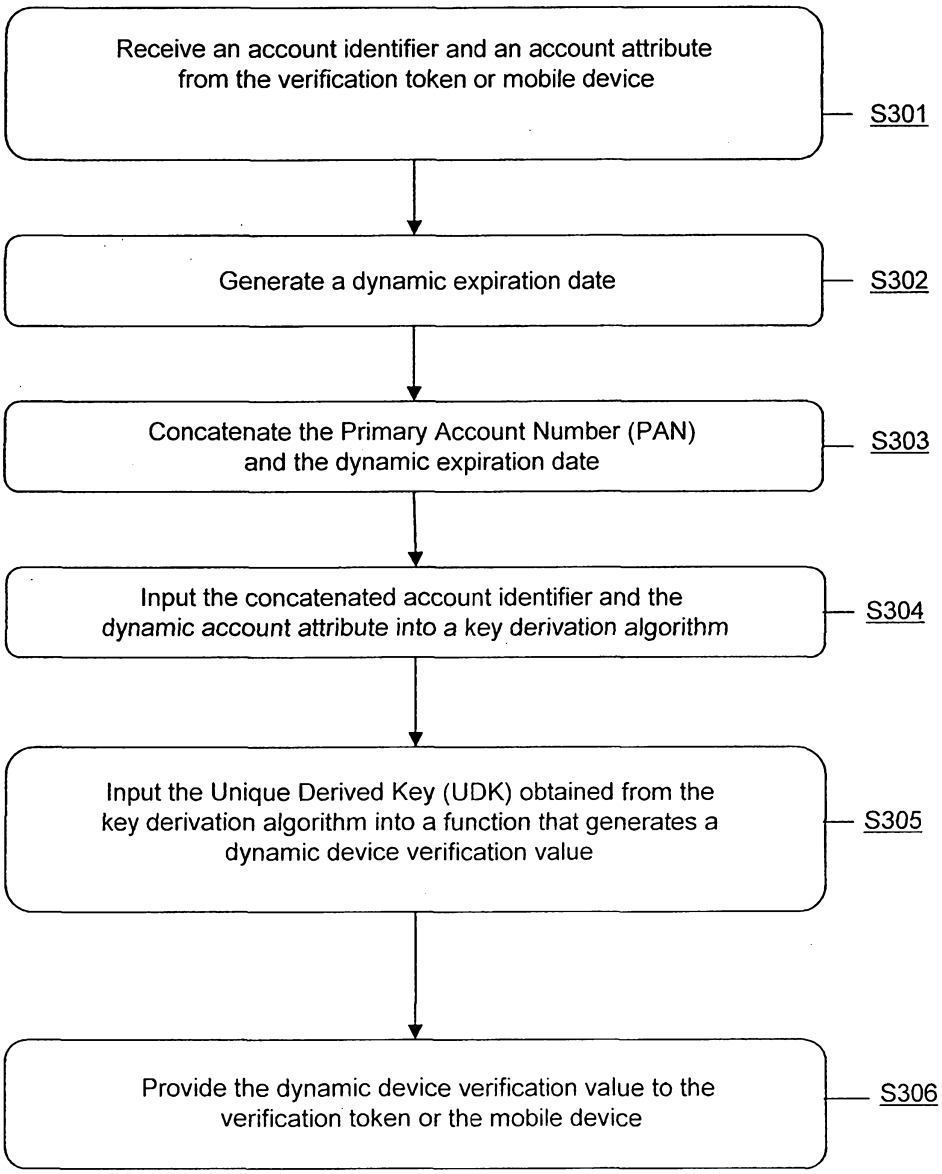

Receive an account identifier and an account attribute from the verification token or mobile device
S301
Generate a dynamic expiration date
S302
Concatenate the Primary Account Number (PAN) and the dynamic expiration date
S303
Input the concatenated account identifier and the dynamic account attribute into a key derivation algorithm
S304
Input the Unique Derived Key (UDK) obtained from the key derivation algorithm into a function that generates a dynamic device verification value
S305
Provide the dynamic device verification value to the verification token or the mobile device
S306

FIG. 3

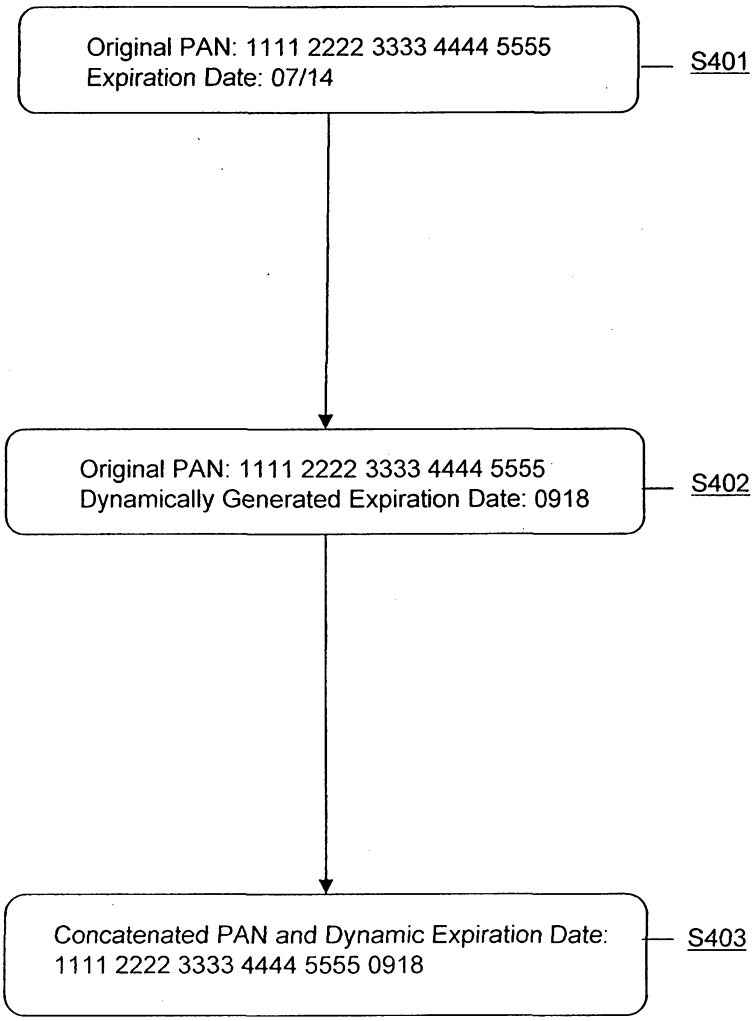

Original PAN: 1111 2222 3333 4444 5555
Expiration Date: 07/14
S401
Original PAN: 1111 2222 3333 4444 5555
Dynamically Generated Expiration Date: 0918
S402
Concatenated PAN and Dynamic Expiration Date:
1111 2222 3333 4444 5555 0918
S403

FIG. 4

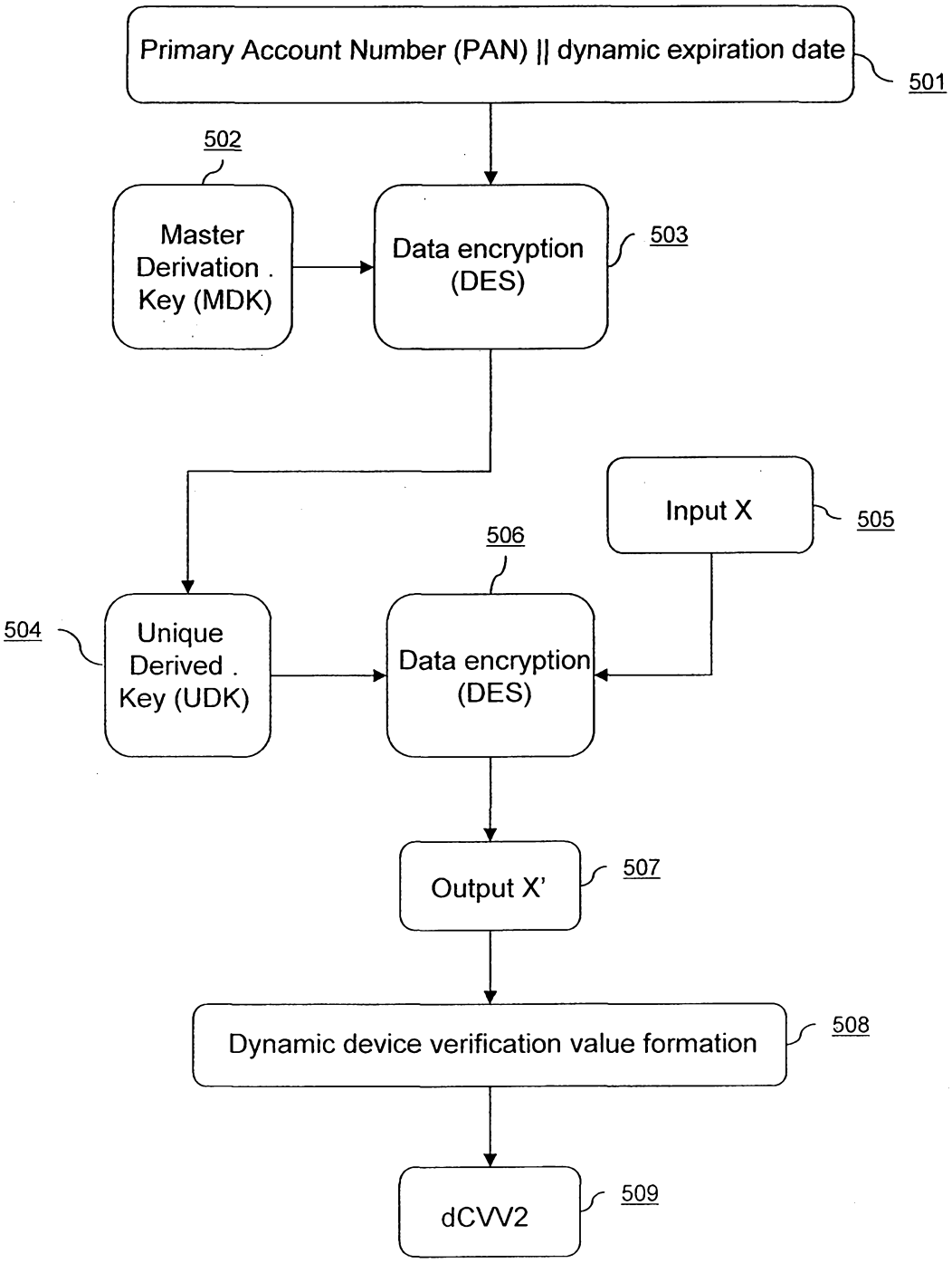
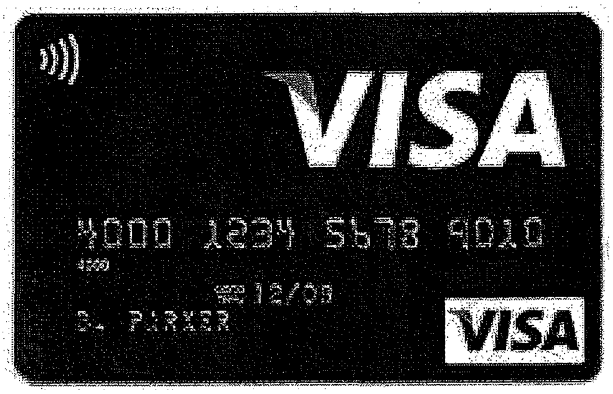

Primary Account Number (PAN) || dynamic expiration date
501
502
Master Derivation . Key (MDK)
Data encryption (DES)
503
Input X
505
506
504
Unique Derived . Key (UDK)
Data encryption (DES)
Output X'
507
Dynamic device verification value formation
508
dCVV2
509

FIG. 5



Portable Consumer Device 600

Payment Page 601

First Name: B — 602

Last Name: Parker — 603

Street Address: 123 First St — 604

City: San Francisco — 605

State: California — 606

Zip Code: 94111 — 607

Account Number: 4000 1234 5678 9010 — 608

Expiration Date: 12/08 — 609

CVV2: 123 — 610

611 — Dynamic Expiration Date:

dCVV2: — 612

Make Payment

FIG. 6

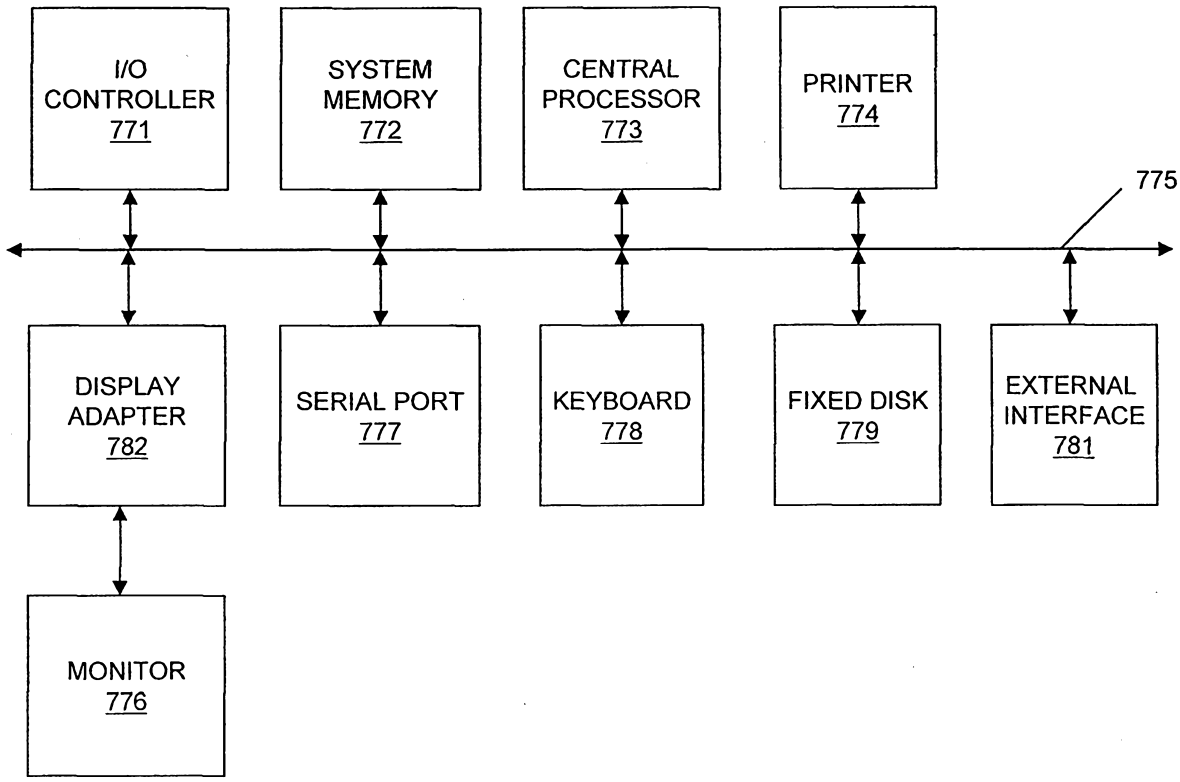

I/O CONTROLLER 771
SYSTEM MEMORY 772
CENTRAL PROCESSOR 773
PRINTER 774
775
DISPLAY ADAPTER 782
SERIAL PORT 777
KEYBOARD 778
FIXED DISK 779
EXTERNAL INTERFACE 781
MONITOR 776

FIG. 7