BROWSER INTEGRATION WITH CRYPTOGRAM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application is a non-provisional application of and claims priority to U.S. Provisional Application No. 62/146,100, filed on April 10, 2015 (Attorney Docket No.: 79900-941691), the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND

[0002] Transactions often require that a user provide sensitive data to execute the transaction. Sensitive data may be an access code to a building or payment details, for example. In some cases, personal user information may be handled by multiple entities, including third parties. When the sensitive data is in electronic form, multiple computing devices, networks, and/or entities are sometimes given access to the sensitive information. Thus, it is desirable that the number of networks, computing devices, and/or entities that have access to such sensitive data be reduced in order to limit the access to the sensitive data.

[0003] Embodiments of the invention address this and other problems, individually and collectively.

BRIEF SUMMARY

[0004] Embodiments of the present invention relate to systems and methods for conducting a transaction a browser configured to be integrated with a token cryptogram. According to one embodiment of the invention, a server computer receives authentication credentials from a user. The authentication credentials may be from a web-browser or an operating system (OS) that a user is utilizing in a computing environment. The server computer may identify that the website accessed by the user is "token-aware." The server computer may provide a transaction data identifier

associated with the authentication credentials to the website. The transaction data identifier may identify underlying transaction data. The user may select or confirm the transaction data identifier presented by a website in order to select the underlying transaction data to be used in a transaction. The server computer may receive this confirmation that the transaction data is approved by the user to complete the transaction. The server computer may send a token and a cryptogram request to a processing network. The token may be linked to the transaction data associated with the authentication credentials. The server computer receives from the processing network a token cryptogram based on the token. The server computer provides the token cryptogram and tokenized payment credentials to data fields of a webpage of the website. The fields may be hidden fields in that they are not visible to the users viewing the website. In one embodiment, the server computer identifying that a website is token-aware may include analyzing a HyperText Markup Language (html) tag of the website.

[0005] According to one embodiment of the invention, a transaction data identifier is received from a server computer. The transaction data identifier may be associated with authentication credentials verified by the server computer. The authentication credentials may be obtained from login information that a user provides to a browser or an operating system of a computing environment. A transaction completion interface of a website may be provided to a computing device such as a personal computer, smartphone, tablet, or otherwise. The transaction completion interface makes the transaction data identifier viewable to a user of the computing device. The transaction data identifier identifies underlying transaction data. A confirmation from the user that the transaction data is approved to complete the transaction is received and transmitted to the server computer. An indication that a website is token-aware is also provided to the server computer. A token cryptogram and tokenized payment credentials are received in data fields of a webpage of the website. The fields may be hidden fields that are not rendered for viewing by the user. An authorization request is sent to an acquirer computer. The authorization request includes the token cryptogram, the tokenized

payment credentials, and a unique identifier of the website. An authorization response from the acquirer computer may be received that either approves or declines the transaction.

[0006] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 shows a block diagram of a system and a flowchart according to embodiments of the disclosure.

[0008] FIG. 2 shows a flowchart according to embodiments of the disclosure.

[0009] FIG. 3 shows an example transaction interface for use with a token cryptogram, in accordance with embodiments of the disclosure.

[0010] FIGs. 4 and 5 show example methods of facilitating a transaction that includes populating a hidden field of a webpage with a token cryptogram.

DETAILED DESCRIPTION

[0011] In the following description, various embodiments will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the embodiments. However, it will also be apparent to one skilled in the art that the embodiments may be practiced without the specific details. Furthermore, well-known features may be omitted or simplified in order not to obscure the embodiment being described.

[0012] Embodiments of the present invention are directed to systems, methods, apparatuses, and computer readable media for utilizing a token cryptogram with a browser to facilitate a transaction. During a transaction, sensitive data may be used and limiting the number of entities or computing devices that have access to the sensitive data reduces the exposure of the sensitive data for improper use. Some

examples of the disclosure are directed to transactions initiated by a user with a browser. Conventionally, to complete a transaction, a user enters their payment details (e.g. credit card number, expiration, billing address, shipping address, etc.) into a browser form. In addition to consuming a significant amount of the user's time to enter the details, entering this sensitive data into the browser potentially gives a merchant, a Payment Service Provider, and the networks connecting those entities access to the sensitive data. Reducing the number of entities, networks, and computing systems that have access to the sensitive data is desirable.

[0013] In one embodiment of the disclosure, a user is logged into a browser or an operating system and initiates a transaction. The publisher of the browser or operating system may have access to transaction data (e.g. a credit/debit card on file) that is associated with the authentication credentials of the logged in user. A server computer of the publisher of the browser or operating system may provide a transaction data identifier (e.g. last four digits of the card on file) to the browser so that the user can select the card on file to be used in the transaction. Once the user selects the card on file via the transaction data identifier, the server computer may send a token and a cryptogram request to a payment processing network. The token is linked to the card on file that is associated with the user account and authentication credentials. A token cryptogram based on the token is received from the payment processing network at the server computer. The server computer can then provide the token cryptogram (and other secure payment details) to hidden form fields of the browser to facilitate the transaction. The hidden form fields of the browser are not visible to a user viewing the website rendered by the browser. In the disclosure, webpages are configured to accept a token cryptogram payload in hidden form fields and browsers are configured to identify websites or webpages that can accept token cryptogram payloads and provide the token cryptogram to the website. The websites may provide an indication to browsers that the website is "token-aware" in that in can accept a token cryptogram to facilitate a transaction. In this way, the merchants and associated websites are provided the required information to complete a transaction using secure data (e.g.

token and cryptograms) while not having access to the actual underlying sensitive transaction data (e.g. card on file data).

[0014] Before discussing specific embodiments and examples, some descriptions of terms used herein are provided below.

[0015] An "authorization request message" may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with (International Organization of Standardization) ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc.. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0016] An "authorization response message" may be an electronic message reply to an authorization request message generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g. POS equipment)

that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0017] A "token" may include a substitute identifier for some information. For example, a payment token may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For instance, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction. The token may also be used to represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. In other embodiments, a token may be a substitute for non-financial information such as social security numbers, home addresses, birthdays, etc.

[0018] A "cryptogram" may refer to an encrypted representation of some information. A cryptogram can be used by a recipient to determine if the generator of the cryptogram is in possession of a proper key, for example, by encrypting the underlying information with a valid key, and comparing the result to the received cryptogram. A cryptogram may be sent from a payment processing network for use by a merchant in response to the merchant requesting a cryptogram for a specific transaction. The cryptogram may only be valid for the specific transaction.

[0019] "Payment credentials" may include any suitable information associated with an account (e.g. a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived

from information related to the account. Examples of account information may include a PAN (primary account number or "account number"), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors). Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0020] A "mobile device" may comprise any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (*e.g.*, 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (*e.g.*, cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (*e.g.*, when a device has remote access to a network by tethering to another device - *i.e.*, using the other device as a relay - both devices taken together may be considered a single mobile device).

[0021] The term "server computer" may include 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. The server

computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise 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.

[0022] An "acquirer" is typically a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant.

[0023] An "issuer" is typically a business entity (e.g., a bank or credit union) which issues a payment device (such as a credit card, debit card, smart card, prepaid device or contactless device) to an account owner and which provides administrative and management functions for the payment account. Some entities may perform both issuer and acquirer functions. A payment account may be any account usable in a transaction, such as a credit, debit or prepaid account.

[0024] FIG. 1 illustrates an exemplary system 100 with at least some of the components for implementing embodiments of the invention. FIG. 1 includes a user 101, a user device 102, a merchant 103, a gateway service provider 104, a server computer 105, an acquirer computer 106, a payment processing network 107, a token vault 108, and an issuer computer 109. Any of the entities may be in communication by a suitable communications network.

[0025] User 101 (which may alternatively be referred to as a consumer) may be associated with user device 102 and may conduct a transaction utilizing user device 102. In some embodiments, user 101 may utilize user device 102 to access a webpage or mobile application operated by merchant 103 or gateway service provider 104 to conduct a transaction. User 101 may have a user account associated with user device 102 issued by server computer 105, which may authenticate user 101 based on the user account.

[0026] User device 102 may be any suitable device that has wireless communication capabilities. User device 102 may be associated with a user account

that can be authenticated by server computer 105. User 101 may be logged into an operating system of device 102 or user 101 may be logged into a browser running on an operating system of device 102, for example. User 101 may also have a user account associated with an application or mobile application of device 102. Server computer 105 may be operated by a publisher/manufacturer of an operating system or web browser running on the operating system of device 102. In some implementations, user device 102 may be configured to communicate with one or more cellular networks. User device 102 may be utilized by user 101 to access a webpage operated by merchant 103 or gateway service provider 104. User device 102 may also comprise a memory element comprising information or code for implementing any methods described herein. User device 102 may run any suitable operating system and browser. In some embodiments, one or more of the operating system and the browser may be capable of identifying websites that are enabled to receive a payload that includes a cryptogram. The website may be enabled to receive the cryptogram in a hidden field of a webpage of the website that is not viewable to a user of the website.

[0027] Some non-limiting examples of user device 102 may include mobile devices (e.g., cellular phones, keychain devices, personal digital assistants (PDAs), pagers, notebooks, laptops, notepads, smart watches, fitness bands, jewelry, etc.), automobiles with remote communication capabilities, personal computers, and the like.

[0028] Merchant 103 may operate a merchant computer configured to receive transaction data from user 101. Merchant 103 may engage in transactions, sell goods or services, or provide access to goods or services to the consumer. Merchant 103 may sell goods and/or services via a website, and may accept payments over the Internet. Merchant 103 may accept multiple forms of payment and may use multiple tools to conduct different types of transactions. Merchant 103 may also operate a physical store for in-person transactions.

[0029] Gateway service provider 104 (which may also be referred to as a gateway") may operate a merchant webpage (e.g., checkout page) on behalf of merchant 103. Gateway service provider 104 may also be considered a Payment

Service Provider (PSP) that provides online services for accepting electronic payments. In some embodiments, gateway service provider 104 may be a payment gateway that initiates a transaction conducted by user 101. Gateway service provider 104 may communicate with server computer 105 to send and receive information associated with user 101, such as a payload including a token cryptogram.

[0030] In some contexts, large merchants 103 may be highly integrated with gateway service provider 104 such that they are the same entity and operated by a single computer. In a different context, a smaller merchant has a website that includes a checkout widget of the gateway service provider 104. In this context, the website may be operated on a web server that is remote from a computer running the checkout widget of the gateway service provider 104.

[0031] Server computer 105 may be any suitable computer having wired and/or wireless communication capabilities and may be capable of conducting any of the methods described herein. In some embodiments, server computer 105 may be a token requestor with card-on-file (COF) and a browser/operating system provider.

[0032] Server computer 105 may be capable of authenticating user 101 utilizing user device 102. Server computer 105 may maintain a user account associated with user 101. In some embodiments, server computer 105 may authenticate user 101 when user 101 signs in to their user account by providing authentication credentials (e.g., password, PIN, biometric identifier, etc.). In some cases, server computer 105 may be a wallet server, that may store other information (e.g., card-on-file data) associated with the authentication credentials of the user account that may also be utilized to authenticate user 101. In some embodiments, the stored information may be tokenized. For example, server computer 105 may store a tokenized version of a Primary Account Number (PAN) of a Card-On-File (COF) without storing all the payment credentials of the COF.

[0033] Server computer 105 may communicate with payment processing network 107 by sending a token to payment processing network 107 and receiving a token

cryptogram based on the token. The token cryptogram may be sent in a payload to merchant 103 or gateway service provider 104.

[0034] Acquirer computer 106 is typically a system for an entity (e.g., a bank) that has a business relationship with a particular merchant or other entity. Acquirer computer 106 may route an authorization request for a transaction to issuer computer 109 via payment processing network 107.

[0035] Payment processing network 107 may include data processing subsystems, networks, and operations used to support and deliver authorization services, and clearing and settlement services. In some embodiments, payment processing network 107 may be in communciation with token vault 108 that may store the binding between a token and an associated account number of user 101. Payment processing network 107 may comprise information or code that enables generation of a token cryptogram based on a received token.

[0036] Token vault 108 may comprise any information related to tokens. For example, token vault 108 may store tokens associated with user 101 and a mapping of the tokens to their associated payment accounts. Token vault 108 may comprise any sensitive information (e.g., account number) associated with the tokens. In some embodiments, payment processing network 107 may communicate with token vault 108 to de-tokenize a token. Token vault 108 may de-tokenize the token by determining information associated with the token based on the stored mapping. In some embodiments, token vault 108 may reside at payment processing network 110.

[0037] Issuer computer 109 is typically a computer run by a business entity (e.g., a bank) that may have issued the payment (credit/debit) card, account numbers or payment tokens used for the transactions. Some systems can perform both issuer computer 109 and acquirer computer 106 functions. When a transaction involves a payment account associated with issuer computer 109, issuer computer 109 may verify the account and respond with an authorization response message to acquirer computer

106 that may be forwarded to merchant 103 or gateway service provider 104, if applicable.

[0038] In some cases, a clearing and settlement process can occur between acquirer computer 106, payment processing network 107, and issuer computer 109. The communications network of system 100 may comprise a plurality of networks for secure communication of data and information between entities. In some embodiments, the communications network may follow a suitable communication protocol to generate one or more secure communication channels. Any suitable communications protocol may be used for generating a communications channel. A communication channel may in some instance comprise a "secure communication channel," which may be established in any known manner, including the use of mutual authentication and a session key and establishment of an SSL session. However, any method of creating a secure channel may be used. By establishing a secure channel, sensitive information related to user 101 may be more securely transmitted.

[0039] A method according to the embodiments of the invention can be described with respect to FIG. 1 and FIG 2. FIG. 1 shows a flowchart of a method (steps 1~20) for enabling an e-commerce transaction utilizing a token cryptogram based on a token according to embodiments of the present invention. FIG. 2 shows a flowchart 200 of a method that can also be described with respect to FIG. 1 (indicated by S301~S307). User 101 may also be referred to as a consumer.

[0040] Additional methods and processes may be included within these methods and may be recognized by one of ordinary skill in the art, in light of the description below. Further, in some embodiments of the disclosure, the described methods may be combined, mixed, and matched, as one of ordinary skill would recognize.

[0041] At step 1, user 101 may operate user device 102. User 101 may access a website associated with merchant 103 and operated by gateway service provider 104 using the user device 102. In some cases, the website may be operated by merchant 103. In some embodiments, user 101 may sign in to a user account issued by server

computer 105 while utilizing user device 102. The sign in process may comprise user 101 entering enrolled authentication credentials into a browser.

[0042] At step 2, user device 102 may send a request to conduct a transaction with merchant 103. User 101 may interact with the browser displaying a webpage to conduct a transaction (e.g., e-commerce transaction). In some cases, user 101 may activate a software button that opens the webpage (or service) and triggers the request to be sent. For example, user 101 may access a merchant website and add items to a card and initiate a checkout process (S301). The webpage may include one or more information fields that may request information surrounding user 101. Any other relevant information surrounding user 101 may be communicated to merchant 103.

[0043] At step 3, merchant 103 may communicate with gateway service provider 104 to take user 101 to an appropriate webpage. For example, user 101 may be taken to a checkout page powered by gateway service provider 104 (or merchant 103) (S302). The checkout page is an example of a transaction completion interface of the website that may be rendered in the browser. Gateway service provider 104 may be capable of accepting a payload with a token cryptogram. In some embodiments, merchant 103 may provide any other suitable information to gateway service provider 104, which may operate the website on behalf of merchant 103. In some embodiments, user device 102 may directly communicate with gateway service provider 104.

[0044] At step 4, gateway service provider 104 may communicate with server computer 105 to authenticate user 101. User 101 may be signed in to their user account issued by server computer 105. Server computer 105 may authenticate user 101 by information (e.g., enrollment data, sign-in credentials) associated with the user account (indicated by "Note" in FIG. 2). In some embodiments, server computer 105 may have stored information (e.g., card-on-file data) associated with the user account of user 101. In some cases, the information may be real payment account information, which can be tokenized. In other cases, some or all of the information may already be tokenized.

[0045] At step 5, server computer 105 may identify that the website operated by gateway service provider 104 (or merchant 103) is "token-aware" and therefore enabled to accept a token cryptogram (S303). In the context of this disclosure, a "token-aware" website is configured to accept a token cryptogram in field of a webpage of the website. In some embodiments, the data field is a hidden field in that it is not viewable to the user. In one embodiment, the website includes a unique identifier and the website is identified as a token-aware website by transmitting the unique identifier to payment processing network to verify the unique identifier. In one embodiment, a "token-aware" website identifies itself by including a HyperText Markup Language (HTML) tag within the website. In one embodiment, the HTML tag functions as the unique identifier. The HTML tag may also verifies the identity of the website and establish the website as a trusted website. In yet another embodiment, identifying the website as token-aware includes receiving an Extended Validation Certificate (EVC) from the website.

[0046] Still referring to step 5, server computer 105 may provide one or more transaction data identifiers associated with the authentication credentials of the user account to gateway service provider 104 after identifying that the website is token-aware. In one embodiment, the transaction data identifier can be the last four digits of a PAN and identifies that particular account for use in the pending transaction.

[0047] Referring to FIG. 3, website webpage 301 includes a transaction completion interface 303 that includes transaction data identifiers 307 and 309, which are the last four digits of different PANs that are associated with the user account 305 and the authentication credentials of the user account 305. Server computer 105 may store the last four digits of a PAN, but not store the complete PAN. User 101 can choose to select one of the transaction data identifiers to complete the pending transaction. The user may also choose to enter a new PAN 311 that has not been linked to the user account. If user 101 selects one of the transaction data identifiers 307/309, the website sends server computer 105 a confirmation of which transaction data identifier was approved by user 101 to complete the pending transaction.

[0048] At step 6 of FIG. 1, gateway service provider 104 may communicate to server computer 105 whether user 101 selects/confirms one of the transaction data identifiers presented on webpage 301. In some embodiments, user 101 may be offered a choice to utilize auto-filled information such as billing address 325, shipping address 335, email address 345, and/or phone number 355. The auto-filled information is generally rendered on the website for viewing by user 101. The auto-filled information may be provided by server computer 105. User 101 may agree with and confirm the form-filled information (e.g., by activating a software button) and trigger a confirmation to be sent to server computer 105 (S304). In some cases, user 101 may reject, delete, and reenter any information in the viewable information fields 325, 335, 345, and/or 355.

[0049] At step 7, in response to the selection of a transaction data identifier, server computer 105 may send a corresponding payment token to and request a token cryptogram based on the payment token from payment processing network 107 (S305). The token may be associated with an account number of a payment account of user 101 that was identified by the transaction data identifier 307 or 309. In other words, if user 101 selects transaction data identifier 307, the token sent by server computer 105 to payment processing network 107 would be associated with the transaction data (PAN) having the last four digits as transaction data identifier 307. Similarly, if user 101 selects transaction data identifier 309, the token sent by server computer 105 to payment processing network 107 would be associated with the transaction data (PAN) having the last four digits as transaction data identifier 309. Server computer 105 may request that the payment processing network 107 to de-tokenize the token to resolve a real account number (e.g., PAN) to be utilized for the transaction. Server computer 105 may also request payment processing network 107 to generate a token cryptogram based on the sent token.

[0050] At step 8, payment processing network 107 may communicate with token vault 108 to de-tokenize the received token. For example, payment processing network 107 may access the mapping of tokens to account numbers stored by token vault 108 to retrieve the account number of user 101 associated with the token.

[0051] At step 9, token vault 108 may send the retrieved account number (e.g., PAN) to payment processing network 107. The account number may be associated with the payment account to be utilized for the transaction conducted by user 101.

[0052] At step 10, payment processing network 107 may generate a token cryptogram based on the token and send the token cryptogram to server computer 105. The token cryptogram may be generated by any suitable method and may be a one-time token cryptogram that is specific to the pending transaction (token cryptogram is only valid for use in the transaction). In some embodiment, the token cryptogram may be generated using an encryption key (e.g., a symmetric encryption key) that may be used with an encryption algorithm such as DES, TDES, AES, ECC, etc. The cryptogram may be generated using any suitable input data including one or more of a token, a timestamp, a transaction amount, etc.

[0053] At step 11, server computer 105 may send tokenized payment credentials associated with user 101 with the token cryptogram to the webpage operated by gateway service provider 104 (or merchant 103) (S306). In one embodiment, the token cryptogram is a Token Authentication Verification Value (TAVV). As discussed previously, the operating system or the browser displaying the webpage of user device 102 may be capable of identifying that the webpage is enabled to accept a payload that includes a token cryptogram. Consequently, gateway service provider 104 may support an additional information field for the token cryptogram received from payment processing network 107 during the transaction conducted by user 101. The additional information field may be a hidden data field that is not rendered for viewing by the user.

[0054] Referring again to FIG. 3, payload 319 that includes the token cryptogram and tokenized payment credentials of user 101 can be provided to hidden payment fields 315. Payload 319 may be encrypted. Hidden payment fields 315 are illustrated with dashed lines to indicate that they are not viewable by a user 101 of webpage 301. Hidden Payment Fields 315 may be configured to receive a token number, a token expiration date, the token cryptogram, a payment account reference (PAR), and other tokenized payment credentials.

[0055] At step 12, gateway service provider 104 may send any received transaction information to merchant 103 to process the transaction. The transaction may be continued if the token cryptogram is valid. In some embodiments, user 101 may receive a confirmation of payment from gateway service provider 104 (or merchant 103). Subsequently, payment processing of gateway service provider 104 with the received token payment credentials may be initiated for authorization (S307).

[0056] At step 13, merchant 103 may generate and send an authorization request message to acquirer computer 106. The authorization request message includes the token cryptogram and may include a unique identifier of the website and tokenized payment credentials.

[0057] At step 14, acquirer computer 106 may forward the authorization request message to payment processing network 107. The payment processing network 107 may then analyze the authorization request message and may perform any suitable authentication processing, including validation of the cryptogram in the authorization request message. This one or more inputs (e.g., the token, timestamp, transaction amount, etc.) that may be present in the authorization request message, and creating a cryptogram which can be compared against the cryptogram received in the authorization request message. In other embodiments, the cryptogram can be decrypted and the input data can be recovered and compared against data in the authorization request message. In other case, the cryptogram can be verified. If it is verified, than the authorization request message may be modified to include a flag which indicates that the cryptogram has been validated. In addition, the payment processing network 107 may take the tokenized payment credentials (e.g., including a payment token) and may retrieve the real payment credentials (e.g., a PAN) from the token vault. The modified authorization request message may also include the real credentials instead of the tokenized credentials.

[0058] At step 15, payment processing network 107 may forward the authorization request message to issuer computer 109. Issuer computer 109 may determine whether the transaction should be authorized and may generate an

authorization response message including an authorization decision. As noted above, if the cryptogram was validated by the payment processing network 107, then this can give the issuer computer 109 assurance that the transaction is authentic. If the cryptogram was not validated by the payment processing network 107, then, the issuer computer 109 may want to perform additional authentication processing with respect to the user device 102 and/or the user of the user device 102 before authorizing the transaction. In some embodiments, issuer computer 109 may include other relevant information in the authorization response message, such as risk analysis information.

[0059] At step 16, issuer computer 109 may send the authorization response message to payment processing network 107. Payment processing network 107 and issuer computer 109 may communicate by any suitable communications network.

[0060] At step 17, payment processing network 107 may send the authorization response message to acquirer computer 106. Payment processing network 107 and acquirer computer 106 may communicate by any suitable communications network.

[0061] At step 18, acquirer computer 106 may send the authorization response message to merchant 103. Merchant 103 may determine whether to complete the transaction based on the received response which may include an approval or denial of the transaction. Acquirer computer 106 and merchant 103 may communicate by any suitable communications network.

[0062] At step 19, merchant 103 may send a confirmation to user device 102 if the transaction is approved. User device 102 may communicate with other entities, including merchant 103 and gateway service provider 104 by any suitable communications network.

[0063] At step 20, user device 102 may inform user 101 that the transaction has been completed. In some embodiments, user device 102 may present a notification (e.g., pop-up, audio, etc.) indicating the completion of the transaction. In other embodiments, the webpage utilized for the transaction may be updated with information indicating to user 101 that the transaction has been completed.

[0064] FIG. 4 illustrates a process 400 of performing a transaction that includes populating a hidden field of a browser with a token cryptogram. The process 400 is illustrated as a logical flow diagram, each operation of which represents a sequence of operations that can be implemented in hardware, computer instructions, or a combination thereof. In the context of computer instructions, the operations represent computer-executable instructions stored on one or more computer-readable storage media that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described operations can be omitted or combined in any order and/or in parallel to implement this process and any other processes described herein.

[0065] Some or all of the process 400 (or any other processes described herein, or variations and/or combinations thereof) may be performed under the control of one or more computer systems configured with executable instructions and may be implemented as code (e.g., executable instructions, one or more computer programs or one or more applications). In accordance with at least one embodiment, the process 400 of FIG. 4 may be performed by server computer 105. The code may be stored on a computer-readable storage medium of server computer 105, for example, in the form of a computer program including a plurality of instructions executable by one or more processors. The computer-readable storage medium may be non-transitory.

[0066] In process block 405, authentication credentials are received by a server computer (e.g. server computer 105). The authentication credentials may be associated with a user account of an operating system or a web browser, for example. The server computer may be operated by a publisher of a browser. The server computer identifies that a website accessed by a user is token-aware, in process block 410. A transaction data identifier associated with the authentication credentials is provided to the website in process block 415. The transaction data identifier identifies

underlying transaction data. In one embodiment, the transaction data identifier is the last four digits of a PAN and the underlying transaction data is the full PAN or tokenized version of the full PAN. The server computer may store or have access to the transaction data identifiers as they are associated with the authentication credentials and the user account. The user may have previously stored payment credentials (that include the transaction data identifiers) into the user account that the server computer maintains or has access to. The underlying transaction data may be payment credentials or tokenized versions of the payment credentials. The website may render one or more transaction data identifiers to a user of the website so that the user can select/confirm the transaction data the user desires to complete the transaction using the transaction data identifiers as a proxy for the actual transaction data.

[0067] In process block 420, the server computer receives a selection or confirmation that the transaction data identified by the transaction data identifier is approved by the user to complete the transaction. In process block 425, the server computer transmits a token and a cryptogram request to a processing network (e.g. payment processing network 107). The token is tokenized version of the transaction data that was identified by the transaction data identifier. In process block 430, a token cryptogram is received from the processing network. The token cryptogram is based on the token sent to the processing network. In process block 435, the token cryptogram and tokenized payment credentials are provided to the hidden fields of the webpage of the website. The hidden fields are not visible to the user viewing the webpage or website.

[0068] In one embodiment, the server computer assigns a unique identifier to the website and includes the unique identifier in the cryptogram request of process block 425. The unique identifier may be a randomly generated unpredictable number. The unique identifier is also included in the payload (e.g. payload 319) that is sent to the hidden fields of the webpage. When the merchant/PSP initiates an authorization request message that is forwarded to the payment processing network (steps 13 and 14 of FIG. 1) the authorization request can include the token cryptogram and the unique

identifier. Therefore, the token cryptogram and the unique identifier will ultimately be forwarded back to the payment processing network, which gives the payment processing network further verification that the merchant/PSP that received the unique identifier and the token cryptogram is also the entity transmitting the authorization request message. Hence, as a technical advantage of the disclosure, the server computer including the unique identifier in the cryptogram request allows the processing network to link the token cryptogram that it generates with the unique identifier and then enforce a domain restriction by verifying the authenticity of the authorization request message by verifying the unique identifier and the token cryptogram are still paired together in the authorization request message.

[0069] FIG. 5 illustrates a process 500 of performing a transaction that includes populating a hidden field of a browser with a token cryptogram. The process 500 is illustrated as a logical flow diagram, each operation of which represents a sequence of operations that can be implemented in hardware, computer instructions, or a combination thereof. In the context of computer instructions, the operations represent computer-executable instructions stored on one or more computer-readable storage media that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described operations can be omitted or combined in any order and/or in parallel to implement this process and any other processes described herein.

[0070] Some or all of the process 500 (or any other processes described herein, or variations and/or combinations thereof) may be performed under the control of one or more computer systems configured with executable instructions and may be implemented as code (e.g., executable instructions, one or more computer programs or one or more applications). In accordance with at least one embodiment, the process 500 of FIG. 5 may be performed by merchant 103 and/or gateway service provider 104.

The code may be stored on a computer-readable storage medium, for example, in the form of a computer program including a plurality of instructions executable by one or more processors. The computer-readable storage medium may be non-transitory.

[0071] In process block 505, a transaction data identifier (e.g. last four digits of a PAN) is received from a server computer (e.g. server computer 105). The transaction data identifier is associated with authentication credentials verified by the server computer. In process block 510, a transaction completion interface (e.g. 303) of a website is provided to a computing device (e.g. user device 102). The transaction data identifier is made visible to the viewer/user of the website. A confirmation is received from the user (process block 515) that the transaction data identified by the transaction data identifier is approved to complete a pending transaction. For example, the user may have an item in the user's cart ready for checking out. The confirmation is transmitted to the server computer in process block 520.

[0072] In process block 525, an indication is provided to the server computer that the website is token-aware (configured to accept a token cryptogram in hidden fields of a webpage of the website). In one embodiment, the indication is an HTML tag. In process block 530, tokenized payment credentials and a token cryptogram is received from the server computer in hidden fields of the webpage of the website. The hidden fields are not rendered for viewing by the user. In process block 535, an authorization request message is transmitted to an acquirer computer (e.g. acquirer computer 106). The authorization request message includes the tokenized payment credentials, the token cryptogram and a unique identifier of the website. The unique identifier of the website may be assigned to the website by the server computer.

[0073] After transmitting the authorization request message, an authorization response message may be received from the acquirer computer. The authorization response message either approves or declines the transaction. When the authorization response message approves the transaction, a transaction completion message may be sent from the merchant or PSP to the user's computing device.

[0074] Embodiments of the invention may provide a number of technical advantages. For example, integrating the use of a token cryptogram in a payload to a merchant checkout page can make a transaction more secure by not requiring the user to enter their PAN to complete a transaction. Rather, because the server computer 105 can provide the last four digits or other transaction data identifier to the merchant and have the user select the transaction data identifier as a proxy for the actual PAN, the server computer 105 nor the user provides the actual PAN (and other payment credentials) to the merchant 103 and/or gateway service provider 104. Instead, tokenized payment credentials and a token cryptogram are provided to the merchant and/or gateway service provider 104 to complete the transaction. Therefore, the entities (e.g. merchant and PSP) and networks connecting those entities never receive the PAN, which limits the opportunity for the PAN to be misappropriated. Yet another technical advantage is that the transaction friction of entering payment credentials into a browser (especially a mobile browser) is reduced in that the user need only select the account (represented by the last 4 digits of the PAN in some embodiments) that they prefer to use to complete the transaction and the rest of the payment details (e.g. shipping and billing address) may be auto form-filled in the viewable data fields of the checkout page while the token cryptogram and other sensitive data elements are in hidden data fields of the checkout page. The viewable data fields and the sensitive data elements in the hidden fields may then be easily packaged by the merchant and send as part of the authorization request. Embodiments that utilize hidden fields may add an additional layer of security in that the token cryptogram is not viewable on the webpage.

[0075] Although the above-noted examples relate to e-commerce payment transactions, embodiments of the invention are not so limited. For example, the use of a token-aware websites, tokens, and cryptograms as described above in the e-commerce payment examples could be used in other non-financial contexts, such as obtaining access to secure data. For instance, instead of a merchant, a person may wish to access his or her healthcare records at a medical institution. Rather than storing actual sensitive data such as social security numbers at the medical institution

Website, the medical institution may store tokens associated with those social security numbers. A similar process as described above in the e-commerce example can be applied when a user wishes to access his or her health records at the medical institution.

[0076] A computer system that may be used to implement any of the entities or components described above may include subsystems such as a printer, keyboard, fixed disk (or other memory comprising computer readable media), monitor, which is coupled to a display adapter. The subsystems may be interconnected via a bus. Peripherals and input/output (I/O) devices, which couple to I/O controllers (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as a serial port. For example, a serial port or network interface 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 to communicate with each subsystem and to control the execution of instructions from a system memory or a fixed disk, as well as the exchange of information between subsystems. The system memory and/or the fixed disk may embody a computer readable medium. In some embodiments, the monitor may be a touch sensitive display screen. Processing logic of the computer system may have access to a computer readable medium and be configured to execute instructions stored in the computer readable medium. Processing logic may include processors, microprocessors, field-programmable gate arrays (FPGAs), Application-Specific Integrated Circuits (ASICs), or other suitable processing logic. The processing logic may be coupled to a network interface to facilitate sending and receiving network traffic via the network interface.

[0077] A computer system can include a plurality of the same components or subsystems, e.g., connected together by external interface or by an internal interface. In some embodiments, computer systems, subsystem, or apparatuses can communicate over a network. In such instances, one computer can be considered a client and another computer a server, where each can be part of a same computer

system. A client and a server can each include multiple systems, subsystems, or components.

[0078] It should be understood that any of the embodiments of the present invention can be implemented in the form of control logic using hardware (e.g. an application specific integrated circuit or field programmable gate array) and/or using computer software with a generally programmable processor in a modular or integrated manner. As used herein, a processor includes a single-core processor, multi-core processor on a same integrated chip, or multiple processing units on a single circuit board or networked. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement embodiments of the present invention using hardware and a combination of hardware and software.

[0079] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python 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 for storage and/or transmission, suitable media include 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 compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0080] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may

reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0081] 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.

[0082] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0083] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0084] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED

1. A method of performing a transaction comprising:

assigning, by a server computer, a unique identifier to a website

receiving, by the server computer, authentication credentials of a user accessing the website;

identifying, by the server computer, that the website accessed by the user is token-aware by identifying the unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

providing, by the server computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the authentication credentials;

receiving, by the server computer, a confirmation that the transaction data identified by the transaction data identifier is approved by the user to complete a transaction;

transmitting, by the server computer, a token and a cryptogram request comprising the unique identifier of the website to a processing network, wherein the token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the server computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the website to conduct a transaction.

2. The method of claim 1 further comprising:

providing the unique identifier of the website to the data fields of the webpage, wherein the data fields are hidden fields not visible to the user viewing the website.

3. The method of claim 1, wherein identifying that the website is token-aware includes analyzing an html (HyperText Markup Language) tag of the website.

4. The method of claim 3, wherein the html tag also verifies a trusted identity of the website.

5. The method of claim 1 wherein the tokenized credentials are provided to the data fields of the webpage only when the website is identified as token-aware.

6. The method of claim 1, wherein the transaction data is the tokenized credentials.

7. The method of claim 1, wherein the transaction data identifier is a last four digits of a Primary Account Number (PAN).

8. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a computer readable medium accessible to the processing logic, the computer readable medium comprising code, executable by a processor, for implementing a method comprising:

assigning, by a server computer, a unique identifier to a website;

receiving, by the server computer, authentication credentials of a user accessing the website;

identifying, by the server computer, that the website accessed by the user is token-aware by identifying the unique identifier of the website and transmitting the unique identifier of the website to a processing network to verify the unique identifier of the website, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

providing, by the server computer, a transaction data identifier to the website, wherein the transaction data identifier identifies underlying transaction data and is associated with the authentication credentials;

receiving, by the server computer, a confirmation that the transaction data identified by the transaction data identifier is approved by the user to complete a transaction;

transmitting, by the server computer, a token and a cryptogram request comprising the unique identifier of the website to a processing network, wherein the token is linked to the transaction data identified by the transaction data identifier;

receiving from the processing network, a token cryptogram based on the token; and

providing, by the server computer, tokenized credentials and the token cryptogram to the data fields of the webpage of the website to conduct a transaction.

9. A method of performing a transaction comprising:

receiving a transaction data identifier from a server computer, wherein the transaction data identifier is associated with authentication credentials verified by the server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

receiving a confirmation from the user that the transaction data identified by the transaction data identifier is approved to complete a transaction;

transmitting the confirmation to the server computer;

providing an indication to the server computer that the website is token-aware, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

receiving, from the server computer, tokenized credentials, a unique identifier of the website, and a token cryptogram in the data fields of the webpage of the website; and

transmitting an authorization request to conduct a transaction to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the website.

10. The method of claim 9 further comprising:

receiving an authorization response from the acquirer computer, the authorization response either approving or declining the transaction.

11. The method of claim 10 further comprising:

sending a transaction completion message to the computing device when the authorization response approves the transaction.

12. The method of claim 9, wherein the token-aware indication includes an html (HyperText Markup Language) tag.

13. The method of claim 12, wherein the token-aware indication also serves to verify the website as a trusted website.

14. The method of claim 9, wherein the token-aware indication includes an Extended Validation Certificate.

15. The method of claim 9, wherein the data fields are hidden fields that are not rendered for viewing by the user.

16. The method of claim 9, wherein the transaction data identifier is a last four digits of a social security number.

17. The method of claim 9, wherein the authentication credentials are associated with a browser publisher of a browser that the website is rendered in.

18. A computer comprising:

processing logic;

a network interface coupled to the processing logic; and

a computer readable medium accessible to the processing logic, the computer readable medium comprising code, executable by a processor, for implementing a method comprising:

receiving a transaction data identifier from a server computer, wherein the transaction data identifier is associated with authentication credentials verified by the server computer;

providing a transaction completion interface of a website to a computing device, the transaction completion interface making the transaction data identifier viewable to a user of the transaction completion interface, wherein the transaction data identifier identifies underlying transaction data;

receiving a confirmation from the user that the transaction data identified by the transaction data identifier is approved to complete a transaction;

transmitting the confirmation to the server computer;

providing an indication to the server computer that the website is token-aware, wherein the token-aware website is configured to accept a token cryptogram in data fields of a webpage of the website;

receiving, from the server computer, tokenized credentials, a unique identifier of the website, and a token cryptogram in the data fields of the webpage of the website; and

transmitting an authorization request to an acquirer computer, wherein the authorization request includes the tokenized credentials, the token cryptogram, and the unique identifier of the website.