

SECURE REMOTE TRANSACTION FRAMEWORK USING DYNAMIC SECURE CHECKOUT ELEMENT

BACKGROUND

[0001] This application claims priority to U.S. Patent Application No. 62/688,863, filed on June 22, 2018, the disclosure of which is herein incorporated by reference in its entirety.

[0002] Because conducting transactions over electronic networks such as the Internet has a number of advantages that include convenience and lower costs, electronic commerce has recently experienced a large amount of growth. However, the anonymity of the Internet increases the issues of fraud and misuse to an electronic retailer. An electronic resource provider has a desire to authenticate a transaction in order to reduce the risk of loss stemming from fraud. Similarly, a consumer has a desire to increase convenience by enabling the use of more channels. Additionally, a consumer often has a desire to remain anonymous, as exposure of personal information may often put the consumer at increased risk.

[0003] In order to complete a transaction, a user is often asked to provide a number of personal details to a merchant. This is problematic if the user wishes to remain anonymous, or if the merchant is not a trusted entity. Some conventional remote transaction systems have been developed that require a user be redirected to another entity to complete the transaction. For example, upon selecting a checkout element, a user may be presented with a popup window which includes his or her personal details. This at least prevents the merchant from gaining access to the user's information, but can also reduce the efficiency of the transaction.

[0004] Furthermore, transactions conducted using access credentials may put those access credentials at risk. For example, a merchant that obtains access credentials from a user during a transaction may sell or use those access credentials to conduct an unauthorized transaction. The use of a token, and more particularly a limited-use token, instead of access credentials may be more secure than the use of access credentials to complete the transaction.

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

SUMMARY

[0006] Described herein are a system and techniques for providing secure remote transaction (SRT) transactions. In some embodiments, a resource provider may embed a checkout element into a website hosted by that resource provider. The checkout element may include an indication as to a type and format of information to be presented within the checkout element. Upon the website being loaded via a browser application, the checkout element may be caused to communicate with an initiator application server in order to be populated in accordance with the indicated information type and format without that information being made available to a resource provider.

[0007] One embodiment of the disclosure is directed to a method comprising presenting a resource document associated with at least one resource managed by a resource provider, upon receiving a request to complete a transaction for the at least one resource, instantiating a checkout element in association with the resource document, identifying, via the checkout element, information indicating an identity of a user of the client device, transmitting the information indicating the identity of the user to a remote server, receiving, from the remote server, a token to be used to complete the transaction, and providing, via the checkout element to the resource provider, the token.

[0008] Another embodiment of the disclosure is directed to A client device comprising: a processor; and a memory including instructions that, when executed with the processor, cause the client device to, at least: present a resource document associated with at least one resource managed by a resource provider, upon receiving a request to complete a transaction for the at least one resource, instantiate a checkout element in association with the resource document, identify, via the checkout element, information indicating an identity of a user of the client device, transmit the information indicating the identity of the user to a remote server, receive, from the remote server, a token to be used to complete the transaction, and provide, via the checkout element to the resource provider, the token.

[0009] Further details regarding embodiments of the disclosure can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 depicts a number of components that may be involved in a system used to implement at least some embodiments of the disclosure;

[0011] FIG. 2 depicts a diagram of an exemplary secure remote transaction (SRT) server that may be configured to conduct secure transaction processing in accordance with at least some embodiments;

[0012] FIG. 3 depicts a swim lane diagram which illustrates an example process for conducting a transaction using a SRT platform in accordance with at least some embodiments;

[0013] FIG. 4 depicts a block diagram illustrating an example process for conducting a transaction while preserving consumer privacy in accordance with at least some embodiments;

[0014] FIG. 5 depicts a first example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure;

[0015] FIG. 6 depicts a second example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure;

[0016] FIG. 7 depicts a third example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure; and

[0017] FIG. 8 depicts a flow diagram illustrating an example process for providing a token to a resource provider in a manner that preserves anonymity for a user in accordance with at least some embodiments.

DETAILED DESCRIPTION

[0018] Embodiments of the disclosure are directed to techniques for securely conducting electronic commerce (e-commerce) transactions. In particular, the disclosure seeks to enable users to conduct transactions with entities with whom they

do not have a relationship while preventing those entities from obtaining sensitive information related to the user.

[0019] In embodiments of the disclosure, upon loading a website that includes a separate application (e.g., a checkout element) on a client device, the client computing device may be caused to initiate communication with a remote initiator server. The initiator server may receive a number of transaction details from the client computing device, as well as user-identifying information. In some embodiments, the initiator server may derive various information from cookies placed upon the client computing device.

[0020] In some embodiments, the initiator server, upon receiving this information, may identify a user identity associated with the transaction. Once the user identity has been identified, the initiator server may determine a number of accounts associated with that user identity. A list of these accounts may be provided to the client computing device to be presented to the user within the separate application. Upon selection of one of the accounts, the initiator server may communicate the selection to a secure remote transaction (SRT) platform associated with that account.

[0021] The SRT platform may then (upon authentication) generate a token specific to the transaction, which may then be provided to the initiator application and subsequently to the resource provider in order to complete the transaction. This may be done without exposing any sensitive information to the host of the website in which the checkout element is embedded.

[0022] Prior to discussing specific embodiments of the invention, some terms may be described in detail.

[0023] An “access device” may be any suitable device that provides access to a remote system. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device.

[0024] “Account credentials” may include any suitable information associated with an account (e.g. an account and/or portable 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 credentials 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.

[0025] An “acquirer” may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular resource provider or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a “transport computer.”

[0026] An “authentication indicator” may be any suitable piece of data that provides additional proof that a particular circumstance is authentic. Exemplary authentication indicators may include cryptograms, flags, or other data which can indicate that a user was authenticated by a computing device.

[0027] An “authorization request message” may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a portable device to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a portable device or account. The authorization request message may include an issuer account identifier that may be associated with a portable device or account. An authorization request message may also comprise additional data elements including one or more of: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or “account number”), a token, a user name, 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, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0028] An “authorization response message” may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing computer. 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 transaction processing computer) to the resource provider's access device (e.g. POS equipment) that indicates approval of the transaction.

[0029] An “authorization entity” may be an entity that authorizes a request. Examples of an authorization entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An “issuer” may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue account credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the user.

[0030] A “checkout element” may be any mechanism for initiating a transaction. For example, a checkout element may comprise a button on a graphical user interface that, when selected, causes a transaction to be initiated.

[0031] A “computing device” may include any suitable device that can electronically process data. Examples of computing devices include desktop computers, mobile devices or mobile computing devices, television sets, etc.

[0032] A “cookie” (aka, a “web cookie,” “Internet cookie,” or “browser cookie”) may be any suitable piece of data sent from a webserver and stored on a user's computer. A cookie may be placed on a user's computer by the computer's web browser while the user is browsing a website maintained by the webserver.

[0033] A “facilitator” may be any entity capable of authenticating a user of a client device. A facilitator may include a client-side application (e.g., a facilitator application) as well as a backend server (e.g., a facilitator server) capable of supporting the client-side application. In some cases, a facilitator application may be executed upon receiving instructions from a facilitator server to authenticate a user of the client device. The facilitator application may cause the client device upon which it is installed to obtain user-specific data. This user-specific data may then be compared to expected user-specific data, either by the facilitator application on the client device or by the facilitator server, to determine whether the obtained user-specific data matches the expected user-specific data. In some embodiments, a facilitator may be an electronic wallet provider (e.g., Apple Pay). It should be noted that the facilitator may be unaffiliated with the SRT Platform and/or the initiator.

[0034] An “initiator” may be any entity capable of facilitating communication between a resource provider and one or more SRT platforms. An initiator may operate a number of servers which provide at least a portion of the functionality described herein. In some cases, an initiator may obtain approval and/or accreditation from one or more SRT platforms in order to operate in conjunction with those SRT platforms. A resource provider may enroll with the initiator in order to obtain access to at least a portion of the processes described herein. An initiator may provide each resource provider that enrolls with it a link to embed within a checkout element. The link, when activated by a user wishing to transact with the resource provider, may initiate the processes described herein in order to facilitate a transaction between the user and the resource provider. It should be noted that the initiator may be unaffiliated with the SRT Platform and/or the facilitator.

[0035] The term “resource” generally refers to any asset that may be used or consumed. For example, the resource may be computer resource (e.g., stored data or a networked computer account), a physical resource (e.g., a tangible object or a physical

location), or other electronic resource or communication between computers (e.g., a communication signal corresponding to an account for performing a transaction). Some non-limiting examples of a resource may be a good or service, a physical building, a computer account or file, or a payment account. In some embodiments, a resource may refer to a financial product, such as a loan or line of credit.

[0036] A “resource document” may be any document pertaining to a resource. In some embodiments, a resource document may be a webpage document related to a particular product. The webpage may be hosted by a resource provider and in some embodiments may include a checkout element.

[0037] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access to such a resource. Examples of a resource provider include merchants, online or other electronic retailers, access devices, secure data access points, etc. A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services. A “resource provider computer” may be any computing device operated by a resource provider.

[0038] A “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.

[0039] A “secure remote transaction (SRT) platform” may be any entity capable of facilitating a transaction in the manners described. A SRT platform may be capable of communicating with an initiator, a facilitator, and a transaction processing network. In some embodiments, a SRT platform may include a SRT server, a token provider, and a transaction processing network. An SRT platform may be configured to perform one or more processes that include: receive a request for a transaction from an initiator, identify an account associated with the transaction, determine an appropriate facilitator

for the account, cause the determined facilitator to authenticate a user associated with the account, generate a token to be used in the transaction, and provide the token to the initiator to complete the transaction.

[0040] A “token” may be a substitute value for a credential. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include tokens, access tokens, personal identification tokens, etc. A token may include an identifier for an account that is a substitute for an account identifier, such as a primary account number (PAN). For example, 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 transaction 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 transaction or 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. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0041] “Tokenization” is a process by which data is replaced with substitute data. For example, an account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value. Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

[0042] A “token provider” or “token service system” can include one or more computers that service tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as

maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may include or be in communication with a token vault where the generated tokens are stored. The token service system may support token processing of transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN and conducting a transaction using that PAN. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer. Various entities of a tokenization ecosystem may assume the roles of the token provider. For example, processing networks and issuers or their agents may become the token provider by implementing the token services according to embodiments of the present invention.

[0043] A “token vault” may refer to a repository that maintains established token-to-PAN mappings. According to various embodiments, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration and that may be used by the token SRT server to apply domain restrictions or other controls during transaction processing. The token vault may be a part of the token service system. In some embodiments, the token vault may be provided as a part of the token SRT server. Alternatively, the token vault may be a remote repository accessible by the token SRT server. Token vaults, due to the sensitive nature of the data mappings that are stored and managed in them, may be protected by strong underlying physical and logical security.

[0044] A “transaction” may be any interaction or exchange between two or more parties. For example, a transaction may include a first entity requesting resources from a second entity. In this example, the transaction is completed when the resources are either provided to the first entity or the transaction is declined.

[0045] A “transaction processing network,” or “processing network,” may refer to an electronic payment system used to accept, transmit, or process transactions made by payment devices for money, goods, or services. The processing network may

transfer information and funds among authorization entities (e.g., issuers), acquirers, merchants, and payment device users.

[0046] A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer.

[0047] FIG. 1 depicts a number of components that may be involved in a system used to implement at least some embodiments of the disclosure. In FIG. 1, a client device 102 may be in communication with a number of remote entities via a network connection (either wireless or physical). For example, the client device 102 may be used to access a website maintained by a resource provider server 104 via a browser application 106. In this example, the website may have an embedded a checkout element 107 configured to cause the client device 102 to initiate communication with a initiator server 108. The checkout element is an example of a separate application that may be embedded within a webpage. The initiator server 108 may, in turn, be in communication with a secure remote transaction (SRT) platform 110. In some embodiments, the client device 102 may have installed on it a facilitator application, which may be configured to cause the client device 102 to communicate with a facilitator application server 112.

[0048] In some embodiments of the invention, the client device 102 may be a mobile device (e.g. a mobile phone). The mobile device may be capable of communicating with cell towers (e.g., via cellular communications such as GSM, LTE, 4G) and wireless routers (e.g., via WiFi). The mobile device may store the user’s account credentials, such as a PAN (primary account number), a token, a name, an address, a CVV, an expiration date, and any other suitable information. Such data may be securely stored via hardware (e.g., a secure element) or software. In some embodiments, the client device 102 may store, in its memory, a number of cookies, each of which may be store information for the client device and/or a user of the client device. In some embodiments, one or more cookies may include an indication of a payment device to be used in a transaction.

[0049] In some embodiments, the resource provider server 104 may be affiliated with an online retailer or another suitable resource provider having an electronic catalog. The resource provider server 104 may serve one or more pages of a resource provider website to a browser 106 installed on the client device 102. In some embodiments, the website served to the browser application may contain a portal or link that, when accessed using the browser application, initiates communication with the initiator server 108. In some embodiments, the website may include an application that automatically initiates contact with the initiator application server 108 and/or the SRT platform 110 upon the website being loaded into the browser application 106.

[0050] The initiator server 108 may be any suitable computing device configured to generate information to be populated into a checkout element embedded in a checkout website operated by, or on behalf of, the resource provider server 104. In some embodiments, the initiator server 108 may receive information from the resource provider server 104 and/or client device 102 that indicates what information should be presented in a checkout element 107 as well as a format or structure in which data should be presented. The initiator server 108 may be configured to identify a user, identify accounts for that user, and populate a checkout element within a website with the identified user information. The initiator server 108 may also be configured to receive a selection of one of those accounts from the client device 102, communicate the selected account to an SRT platform 110 associated with that account, and complete a transaction using the selected account. It should be noted that the initiator server 108 may be configured to perform each of the above functions without providing confidential information to the resource provider server 104, despite the fact that the checkout element is embedded within a webpage hosted by that resource provider server 104.

[0051] In some embodiments, there may be a number of SRT platforms 110 and the SRT platforms 110 may each be associated with a transaction processing network. Each SRT platform may include some combination of an SRT server (or servers) 110(A), token data 110(B), and a processing network 110(C). Multiple accounts may be associated with a single SRT platform. For example, a user may be associated with two different accounts which are each associated with different authentication entities, while

both accounts are able to be processed using a single SRT platform. The SRT server may be configured to communicate with the initiator application server 108 to provide information to be populated into the checkout element 107. For example, the resource provider server 104 may embed a checkout element 107 into a webpage that it maintains or operates. In this example, the checkout element may indicate a style or format (e.g., “a look and feel”) in which certain user details should be presented to the client device 102. The initiator application server 108 may identify the user details to be presented in the checkout element and may communicate with a number of different SRT platforms 110 to obtain the identified user details. In some embodiments, the checkout element may be a separate computing application, such as a widget.

[0052] The SRT server 110(A) (which may be an example of a secure remote server), may be configured to identify a facilitator application server 112 associated with an account and cause the user to be authenticated using that facilitator application server 112. Additionally, once the user has been authenticated, the SRT server 110(A) may be configured to generate a token to be associated with a transaction which is stored in the respective token data 110(B). The SRT server 110(A) may pass the token to the initiator server 308, which may generate transaction information that includes the token to be used for a transaction. A mapping between the token and the transaction may be maintained by the SRT server 110(A) in its respective token data. In some embodiments, the SRT server 110(A) may receive a number of files from various authorization entities, each of which may include mappings between email addresses and various PANs. In this way, the SRT server 110(A) may maintain a mapping between user identifier information and accounts.

[0053] The facilitator application server 112 may be any suitable computing device that provides support for a respective facilitator application. In some embodiments, the facilitator application server 112 may perform authentication processing on behalf of the facilitator application. For example, the facilitator application may cause the client device 102 to obtain authentication data from a user of the client device 102. Once obtained, the authentication data may be transmitted to the facilitator application server 112 that corresponds to the facilitator application used to collect the

authentication data. The authentication data may then be compared to authentication data on record for that user by the facilitator application server 112.

[0054] A facilitator application may be any suitable set of computer-executable instructions installed on the client device 102 that, when executed, causes the client device 102 to perform an authentication process. In some embodiments, the authentication process may involve the collection of biometric information associated with a user of the client device 102. For example, the facilitator application may obtain voiceprint or fingerprint data to be used to authenticate the user. The facilitator application may be tied to hardware installed on the client device 102. Examples of facilitator applications may include fingerprint, retinal, or voice scanning applications. The hardware associated with those applications may include fingerprint, retinal, or voice scanning hardware such as fingerprint, retinal, or voice sensors. Other types of facilitator applications may also include PIN and password facilitator applications. In some embodiments, a facilitator application may be a wallet SRT server.

[0055] For an illustrative example of at least some embodiments of the disclosure, consider a scenario in which a user accesses a merchant (resource provider 104) website to complete a transaction (e.g., make a purchase). It should be noted in this example that the user may not have any relationship with the merchant (e.g., does not have an account and has not previously conducted a transaction with the merchant). In this scenario, the user may, upon selecting a number of items for the transaction, be served a checkout page for the merchant website. The checkout page may include a list of the items, prices, quantities, or any other suitable transaction-related information. In addition, the checkout page may include a checkout element that contains a list of accounts associated with a the user and shipping information as well as a button that may be selected to initiate a transaction. This list of accounts is able to be provided despite the fact that the user does not have a relationship with the merchant.

[0056] In the scenario above, upon loading of the website that includes the checkout element by the user of the client device 102, the client device 102 may be caused to initiate communication with the initiator server 308. This may involve the transmission of a number of transaction-related details from the client device 102 to the initiator server 106. In some embodiments, the client device 102 may also transmit user-

identifying information to the initiator server 108. For example, a helper feature in the browser application may provide user identifier information (e.g., via cookies). The initiator server 108 may then identify the user associated with the transaction. If the initiator server 108 is not able to identify the user based on the user-identifying information, then the user may be asked to self-identify (e.g., login).

[0057] Once a user has been identified by the initiator server 108, the initiator server 108 may send requests to a number of different SRT platforms 110 to identify accounts associated with the identified user. In some embodiments, a user may have several accounts with a single SRT platform 110 (e.g., across multiple issuers within the same transaction processing network). The initiator server 108 may receive responses from each of the number of different SRT platforms 110 with a list of accounts associated with the user. Once received, the lists may be aggregated into a single list including each of the identified accounts.

[0058] Once an aggregated list of accounts has been created, it may be presented to the user via the client device 102 within the checkout element 107. In this scenario, the user may be presented with a number of different accounts belonging to him or her, with which the transaction can be completed. The user may then select one of the accounts from the list. Once this selection has been made, it is transmitted to the initiator server 108 and onto the SRT platform 110 associated with the selected account. It should be noted that the browser application 106 may be configured so that even though the current website being viewed (and the checkout element 107 embedded therein) is hosted by a merchant, that merchant has no visibility into the user information (e.g., the list of accounts) presented within the checkout element 107.

[0059] Upon receiving a selection of an account to be used, the initiator application server 108 may initiate a transaction using the selected account. For example, the initiator application server 108 may cause the SRT platform 110 to generate a token to be associated with the requested transaction. The token may be mapped to the selected account via the token data 110(B). Once a token has been assigned to the transaction, the SRT platform 110 may provide the token to the initiator server 108. The initiator server 108 may generate transaction information to be provided to the resource provider that includes the token. The resource provider (e.g., the

merchant) may subsequently use the received token to complete the requested transaction.

[0060] For clarity, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1. In addition, the components in FIG. 1 may communicate via any suitable communication medium (including the internet), using any suitable communication protocol.

[0061] FIG. 2 depicts a diagram of an exemplary SRT server 200 that may be configured to conduct secure transaction processing in accordance with at least some embodiments. The SRT server 200 may be an example of the SRT server 110 described with respect to FIG. 1 above.

[0062] The SRT server 200 may be any type of computing device capable of receiving data from a checkout element and providing/processing a token to be used in completing a transaction. In at least some embodiments, the SRT server 200 may include at least one memory 202 and one or more processing units (or processor(s)) 204. The processor(s) 204 may be implemented as appropriate in hardware, computer-executable instructions, firmware or combinations thereof. Computer-executable instruction or firmware embodiments of the processor(s) 204 may include computer-executable or machine executable instructions written in any suitable programming language to perform the various functions described.

[0063] The memory 202 may store program instructions that are loadable and executable on the processor(s) 204, as well as data generated during the execution of these programs. Depending on the configuration and type of SRT server 200, the memory 202 may be volatile (such as random access memory (RAM)) and/or non-volatile (such as read-only memory (ROM), flash memory, etc.). The SRT server 200 may also include additional storage 206, such as either removable storage or non-removable storage including, but not limited to, magnetic storage, optical disks, and/or tape storage. The disk drives and their associated computer-readable media may provide non-volatile storage of computer-readable instructions, data structures, program

modules, and other data for the SRT server 200. In some embodiments, the memory 202 may include multiple different types of memory, such as static random access memory (SRAM), dynamic random access memory (DRAM) or ROM.

[0064] Turning to the contents of the memory 202 in more detail, the memory 202 may include an operating system and one or more application programs or services for implementing the features disclosed herein including at least a module for determining whether to approve or decline a transaction (authorization module 208) and a module for identifying user accounts based on provided data (account identification module 210). The memory 202 may also include a number of data stores, including user data 212, which maintains information associated with individual users, and/or token data 214, which may maintain information on tokens associated with particular users and/or transactions. In some embodiments, the SRT server 200 may maintain one or more accounts associated with a user.

[0065] In some embodiments, the authorization module 208 may, in conjunction with the processor 204, be configured to determine whether to authorize a transaction related to an authorization request message. In some embodiments, the authorization module 208 may receive an authorization request message that includes a token. In some embodiments, the token may be formatted such that the authorization request message is routed to the SRT server 200. For example, the token may include a six-digit banking identification number (BIN) associated with the SRT server 200 that causes a transaction processing network to route any authorization request message that includes the token to the SRT server 200. Upon receiving the authorization request message that includes the token, the authorization module 208 may identify an account associated with the token (e.g., via token data 214) and retrieve data associated with that account from user data 212. In some embodiments, the authorization module 208 may then determine whether to approve or decline the transaction based on information included in the authorization request message as well as data associated with the user. In some embodiments, the authorization module 208 may identify a payment account to be used to complete the transaction and may generate a new authorization request message that includes an identifier for that payment account, which the authorization module 208 may subsequently route to an authorization entity for that payment account.

In at least some of these embodiments, upon receiving an authorization response message from the authorization entity, the authorization module 208 may generate a new authorization response message which includes the token in place of the payment account identifier, and transmit that authorization response message to the resource provider from which the authorization request message was received.

[0066] In some embodiments, the account identification module 210 may, in conjunction with the processor 204, be configured to identify an account to be used to complete a transaction. In some embodiments, the account identification module 210 may be in communication with a checkout element instantiated on a user device 228. The account identification module 210 may receive, from the checkout element, one or more data retrieved from the user device 228. In some embodiments, the data may include data retrieved from a cookie or other document. In some embodiments, the data may include an identifier for the user device 228 itself, such as a phone number, serial number, international mobile equipment identifier (IMEI), or other suitable identifying information). In some embodiments, the checkout element installed on the user device 228 may cause a facilitator application 234 to be instantiated (e.g., using an application programming interface (API) call), and the data may include information generated by the facilitator application 234. The account identification module 210 may then use the received data to identify an account from user data 212. Additionally, the account identification module 210 may identify a payment account to be used to complete a transaction for the identified account. In some cases, this may involve multiple steps, including identifying a number of payment accounts associated with the identified account, presenting a list of identifiers for those payment accounts to a user (e.g., via a checkout element on a user device 228), and receiving a selection of one of the payment accounts from the user. In some embodiments, the account identification module 210 may select a default payment account to be used in a transaction. Once a payment account has been identified, the account identification module 210 may generate (or select) a token to be used in a transaction, the token being associated with the resource provider, user, and/or payment account. The account identification module 210 may then provide the token to the user device 228 via a checkout element.

[0067] The data stored in databases 212 and 214 may be dynamic, static, or some combination of dynamic and static data. In some embodiments, user data 212 may include any information about users. For example, user data 212 may include demographic data, internet search history data, purchase history data, clickstream data, or any other suitable information related to the user. In some embodiments, token data 214 may include information about tokens previously generated for, or assigned to, transactions to be conducted. In some embodiments, token data 214 may be a token vault.

[0068] The SRT server 200 may also contain communications interface(s) 222 that enable the SRT server 200 to communicate with a stored database, another computing device or server, one or more remote devices, and/or any other suitable electronic devices. In some embodiments, the communication interface 222 may enable the SRT server 200 to communicate with other electronic devices on a network 224 (e.g., on a private network). The SRT server 200 may also include input/output (I/O) device(s) and/or ports 226, such as for enabling connection with a keyboard, a mouse, a pen, a voice input device, a touch input device, a display, speakers, a printer, etc.

[0069] In some embodiments, the network 224 may include any one or a combination of many different types of networks, such as cable networks, the Internet, wireless networks, cellular networks, and other private and/or public networks. While the illustrated example depicts various electronic devices accessing the SRT server 200 over the network 224, the described techniques may equally apply in instances where the electronic devices interact with the SRT server 200 over a landline phone, via a kiosk, or in any other manner. It is also noted that the described techniques may apply in other client/server arrangements (e.g., set-top boxes, etc.), as well as in non-client/server arrangements (e.g., locally stored applications, peer to-peer systems, etc.).

[0070] The SRT server 200 may be in communication with a number of other electronic devices. For example, the SRT server 200 may be in communication with user devices 228 and/or resource providers 230. Each of the user devices 228 and resource providers 230 may be capable of interacting with the SRT server 200 to receive and/or process a token.

[0071] In some embodiments, a user device 228 may include a mobile application 232, which may be a set of computer executable instructions (e.g. an application) which, when executed, causes the user device 228 to present a checkout element via a display of the user device 228. In some embodiments, the checkout element may be embedded within another element and may be configured to provide data to the SRT server 200 and to receive a token in response. For example, the user device 228 may instantiate a checkout element via a browser application (i.e., an example of mobile application 236) which causes the user device 228 to communicate with the SRT server 200. In some embodiments, the user device 228 may also include a facilitator application 234 (e.g., an eWallet mobile application) capable of authenticating a user. In some embodiments, a checkout element, once instantiated on the user device 228, may cause the facilitator application 234 to execute and authenticate the user. For example, the checkout element may present one or more payment options as well as one or more authentication options to a user. Upon selection of an authentication option that involves a particular facilitator application 234, the checkout element may cause the facilitator application 234 to execute using an API call. In this example, the facilitator application 234, when executed, may be provided with details of the transaction and may be caused to authenticate the user of the user device 228. Upon authenticating the user of the user device 228, the facilitator application 234 may provide a certificate of authenticity and/or a user identifier to the checkout element, which may then convey that data to the SRT server 200.

[0072] In some embodiments, a resource provider 230 may be any computing device capable of providing authorization request messages to the service provider 200. In some embodiments, the resource provider 230 may be a retailer (e.g., an electronic retailer) or some other resource provider which manages access to one or more resources (goods and/or services). In some embodiments, the resource provider 232 may include, in its memory, one or more modules for conducting a transaction for a resource (transaction module 238). The resource provider 230 may maintain, or host, a website from which a user may purchase one or more resources managed by the resource provider 230.

[0073] In some embodiments, the SRT server 200 may maintain an account with respect to one or more user devices 228. It should be noted that an account maintained by the SRT server 200 for the user device 228 may be different from an account maintained by a resource provider 230 for that same user device 228. Each of an SRT server 200 and a resource provider 230 may separately maintain information related to a user in relation to their respective accounts.

[0074] FIG. 3 depicts a swim lane diagram which illustrates an example process for conducting a transaction using a SRT platform in accordance with at least some embodiments. Depicted in FIG. 3 are interactions between various components as described herein. In particular, the process 300 depicts interactions between a client device 102, a resource provider 104, a browser 106 (installed on the client device 102), an initiator server 108, and a SRT server 110. Each of these components may be examples of the respective components depicted in FIG. 1.

[0075] Process 300 may begin at 302, when a user visits a checkout page (e.g., an electronic shopping cart) associated with a resource provider. In some embodiments, the user may select a number of resources (e.g., goods and/or services) provided by an electronic retailer. Once the user has selected a number of resources, the user may select an option to complete a transaction for the resources and may be provided with a checkout page.

[0076] On the checkout page, the resource provider may display an embedded checkout element. Upon loading the checkout page, the checkout element may be caused to communicate with the initiator server 108 to initialize payment options at 304. The checkout element may communicate a type and/or format of information needed to the initiator server 108 at this step. Additionally, the resource provider 104 may send information to the initiator server 108 related to a potential transaction. For example, the resource provider 104 may send information related to one or more resources to be obtained by the user as well as a total cost or any other suitable information. In some embodiments, when a user visits a checkout page with an embedded checkout element, the initiator may determine whether or not the user is a recognized user. To do this, the initiator may receive identifier information from the resource provider or from an application (e.g., the checkout element) embedded within the checkout page. In some

embodiments, when the user visits a checkout page or selects the checkout element on a resource provider checkout page, that user's email address may be transmitted by the browser 106 (e.g., via a helper feature) to the initiator server. In the scenario in which the initiator server 108 is able to obtain an identifier (e.g., an email address) for the user, the initiator server 108 may transmit that identifier to a number of different SRT servers 110 which support the initiator server 108 at 306.

[0077] The SRT servers 110, upon receiving the identifier information, may each determine whether or not an authorization entity associated with the SRT server maintains at least one account associated with that user. In some embodiments, this may involve the SRT server querying a number of authorization servers. In some embodiments, each of the SRT servers 110 may maintain mappings between various accounts and identifiers. In these embodiments, the SRT servers 110 may each query a database that it maintains in order to identify a list of accounts based on the identifier.

[0078] Upon identifying a number of accounts, each SRT server 110 may return a list of those accounts, as well as other account details, to the initiator server 108. If the SRT server has not been able to identify any accounts associated with the identifier, then the SRT server may return an indication that the user is not recognized. In some embodiments, the initiator server 108 may provide an indication to the resource provider 104 that the user is recognized at 308.

[0079] In the scenario in which the user's email address is unable to be obtained from the browser, the user may be asked to enter his or her email address. The initiator server may then identify that user's accounts from the file including the mapping of the accounts to the user's email address. In some embodiments, if the initiator server is unable to identify an account from the mapping file, then the user may be asked to provide an account identifier. The initiator may perform more or more authentication techniques in order to confirm that the user is actually in possession of a provided email address. For example, in some embodiments, the initiator server may send a one-time password (e.g., a code or pin) to the email address, which the initiator may require that the user provide back. The SRT server may then query the SRT servers in the manner described above to identify a number of accounts available for a user.

[0080] At 310, the user may initiate a transaction with the resource provider via the checkout page by selecting a displayed checkout button. It should be noted that some embodiments of the disclosure may not include steps 308 and/or 310. For example, in some embodiments the following steps may be performed automatically (e.g., without generation of, and selection of, a checkout button).

[0081] At step 312, the initiator server 108 may populate the checkout element with information about the user. In some embodiments, the checkout element may be a widget or other separate application embedded into a webpage hosted by the resource provider computer 104. In some embodiments, the initiator server 108 may communicate with the browser 106 at 314 to identify at least some portion of data with which to populate the checkout element. For example, the browser may maintain (e.g., in cookies or user settings) information such as shipping information for the user, which may be populated into the checkout element.

[0082] Once the initiator server 108 has identified a user and populated the checkout element with a list of accounts associated with that user, the initiator server 108 may provide the populated checkout element to the user at 316. In some embodiments, the client device 102 may be configured to display the populated checkout element. The client device 102 may enable the user to select a specific account from the list of accounts to be used to complete the transaction. The user's selection of a specific account is then provided to the initiator server 108 at 318. The client device 102 may enable the user to select a specific shipping address to be used to complete the transaction at 320. Additionally, the client device 102 may enable the user to select a number of other details to be used to complete the transaction at 322.

[0083] Upon receiving the user's selection, the initiator server 108 may initiate an authentication process to verify that the user is authorized to complete the transaction at 324. In some embodiments, the authentication process may be a native CVM process implemented via the browser 106. In some embodiments, the authentication process may be initiated via a facilitator application installed upon the client device 102.

[0084] Once authenticated, the initiator server 108 may identify the SRT server associated with the selected account. The initiator server 108 may generate and

transmit a request to the appropriate SRT server 110 at 326. In some embodiments, the request may include details of the transaction to be conducted. It should be noted that each account is associated with only one SRT server 110 whereas a single SRT server 110 may be associated with multiple accounts.

[0085] Once the request has been received by the SRT server and the user for the transaction has been identified, account information stored by the SRT server 110 may be identified with respect to that user. Once the account information has been identified, the user may be asked to authenticate himself or herself using a separate authentication process. It should be noted that the authentication process 306 may be separate from any login required in a user identification process. In some embodiments, if this is the first time that the user has utilized a particular account with a particular browser application, the user may be required to perform one or more extra steps to confirm his or her identity (e.g., a IDD process). Once this is done, the user's identity may be securely bound to the user's identity within the browser.

[0086] In some embodiments, once the SRT server 110 has determined that the user is authenticated, it may generate a token to be used in the requested transaction. This may involve generating a token (e.g., a randomly generated string of characters) which may be mapped to the selected account in a token vault. Once the SRT server 110 has identified any relevant supplemental information to be included in the transaction (e.g., shipping information), the SRT server 110 may provide a token to the initiator server 108 at 328. The initiator server 108 may subsequently complete the transaction and present a confirmation notification. In some embodiments, to do this, the initiator server may provide the token to the resource provider 104 for the resource provider to complete the transaction using the token at 330. In some embodiments, the resource provider 104 may store the token for future use. In some embodiments, the initiator server 108 may generate an authorization request message on behalf of the resource provider, which it may route to the SRT server 110 (e.g., via a transaction processing network).

[0086] In some embodiments, the resource provider may complete the transaction by submitting an authorization request message including the token, the transaction amount, and a resource provider ID to the processing network (e.g.,

processing network 110(C)(1)) via an acquirer computer (not shown). The processing network may determine a real account identifier (e.g., a PAN or primary account number) associated with the token, and may generate a modified authorization request message including the real account identifier to an authorizing entity computer operated by an authorizing entity such as an issuer. The authorizing entity may approve or deny the request, and may generate an authorization response message including the authorization decision. The authorization response message may be transmitted back to the processing network, and the processing network may substitute the token for the real account identifier in the authorization response message. The modified authorization response message may then be transmitted back to the resource provider. At the end of the day or any other suitable period of time, a clearing and settlement process may take place between the acquirer and the authorizing entity, via the processing network.

[0087] FIG. 4 depicts a block diagram illustrating an example process for conducting a transaction while preserving consumer privacy in accordance with at least some embodiments. The process 400 may be performed by a number of components, including at least a client device 102, a resource provider 404, and an SRT server 110. Each of components client device 102, resource provider 404, and SRT server 110 may be examples of their respective components described with respect to FIG. 1 above.

[0088] Process 400 may begin at step 1, when a browser application installed upon a client device 102 is executed and directed to a website operated by a resource provider server 104. In some embodiments, the browser application 106 may request a resource document (e.g., a webpage) 402 related to a particular resource managed by the resource provider. In some embodiments, the browser application 106 may request a resource document 402 related to a checkout page (e.g., an electronic shopping cart) managed by the resource provider.

[0089] At step 2, the process 400 may involve, upon receiving the request for the resource document 402 by the resource provider server 104, serving the resource document 402 to the client device 102. The resource document 402 may then be presented via the browser application 402. In some embodiments, the resource document 402 may include a link (or other suitable reference) to a checkout element 107. The resource document may include a number of data and/or populated data fields

associated with a transaction to be conducted. For example, the resource document 402 may include data related to an amount of a transaction to be conducted, identifiers for one or more resources to be involved in the transaction, shipping information, etc.

[0090] At step 3, the process 400 may involve instantiating a checkout element 107. In some embodiments, the checkout element 107 may be instantiated upon the browser application 106 loading the resource document 402. In some embodiments, the checkout element 107 may be instantiated upon selection of a button or other mechanism located on the resource document 402. For example, the checkout element 107 may be instantiated upon selection of a “checkout” button displayed via the browser application 106 by a user of the client device 102. In some embodiments, data related to a transaction to be conducted may be provided to the checkout element. For example, data related to an amount of a transaction to be conducted, identifiers for one or more resources to be involved in the transaction, shipping information, etc., may be retrieved from the resource document 402 and provided to the checkout element 107.

[0091] At step 4, the process 400 may involve identifying information associated with a user. In some embodiments, this may involve retrieving data from a memory 404 of the client device 102. For example, the checkout element 107 may retrieve information stored in a cookie placed in memory of the client device 102. In some embodiments, the information stored in the cookie may include an identifier for the user. It should be noted that an identifier for the user may not be used by another entity to identify the user. For example, the identifier for the user may be a random or pseudo-random string of characters that is associated with the user via a database mapping maintained by the SRT server 110.

[0092] In some embodiments, step 4 may involve execution of a facilitator application 406 on the client device 102. In at least some of these embodiments, a user may be presented with a list of facilitator applications 406 available (e.g., installed upon) the client device 102. Upon selection of a particular facilitator application 406, the checkout element 107 may cause that facilitator application to be executed on the client device. This may involve the checkout element 107 interacting with the facilitator application 406 via one or more APIs associated with the facilitator application 406. In some embodiments, the checkout element 107 may provide data related to the

transaction to the facilitator application 406. Once executed, the facilitator application 406 may be caused to authenticate the user of the client device 102. Upon authenticating the user of the client device 102, the facilitator application 406 may provide an indication of the user's authenticity and/or an identifier for the user to the checkout element 107.

[0093] At step 5, the process 400 may involve the checkout element providing user data to the SRT server 110. As described elsewhere, in some embodiments data may be provided by the checkout element 107 to an initiator application server, such as initiator application server 108 described with respect to FIG. 1. While described with respect to the SRT server 110, it should be noted that at least a portion of the functionality described for process 400 may be performed by an initiator application server. In some embodiments, the user data may include data retrieved from the memory 404 of the client device. In some embodiments, the user data may include an indication of a user's authenticity and/or an identifier for the user generated by a facilitator application 406. The SRT server 110 may identify an account associated with the user based on the provided user data. The SRT server 110 may also identify a payment account to be used in the transaction. In some embodiments, this may involve multiple steps in which the SRT server 110 identifies a number of payment accounts available to the user, provides a list of the number of payment accounts to the checkout element 107, and receives a selection of a payment account from the list of available payment accounts. In this scenario, the checkout element 107 may present the list of available payment accounts to a user (e.g., via a drop-down list) and may provide the user's selection from that list to the SRT server 110. Upon determining a payment account to be used to complete the transaction, the SRT server 110 may generate a token to be associated with the transaction. The data received from the checkout element 107 (including transaction details) and an indication of the payment account may be stored in relation to the token by the SRT server 110.

[0094] At step 6, the process 400 may involve the SRT server 110 providing the generated token to the checkout element 107. Once received the checkout element 107 may provide the token to the resource provider server 104 via the resource document at

step 7. The resource provider server 104 may then use the provided token to complete a transaction

[0095] FIG. 5-7 each depict example processes for enabling a transaction to be conducted in accordance with at least embodiments of the disclosure. Each of these processes are depicted as a series of graphical user interface (GUI) elements.

[0096] FIG. 5 depicts a first example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure. In FIG. 5, the process 500 is depicted via a series of GUIs that include GUI 502, GUI 504, and GUI 506. In FIG. 5, a checkout element 508 may be embedded within a product website on an electronic retail site. For example, the user may be given the ability to check out with a particular item without the need to add items to a cart and proceed to an actual checkout page.

[0097] The checkout element 508 may be populated within a GUI 502 depicting a resource provider's checkout page. Upon loading a website with the checkout element 508, the user may be identified (e.g., based on information stored in a memory of the device on which the checkout element is implemented) and presented an account selection option 510 containing one or more available accounts for that user. As described herein, the user may be identified by an initiator server by querying a number of SRV servers supporting that initiator server based on cookies stored on a client device from which the functionality is accessed.

[0098] In some embodiments, the user may be given the ability to confirm the transaction via a confirmation GUI 504. In some embodiments, this may involve presenting a summarization of data to the user. In some embodiments, the user may be given the ability to indicate whether an expedited process should be used to conduct future transactions with the resource provider. For example, if the user indicates that future transactions with the resource provider should be expedited, that resource provider may be given a token that may be used in future transactions. In some embodiments, the token may be resource provider-specific. The user may also be notified of the completion of a transaction via a transaction completion GUI 506.

[0099] FIG. 6 depicts a second example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure. FIG. 6 is similar to FIG. 5 described above. However, as depicted via GUIs 602, 604, and 606 of FIG. 6, a checkout element 608 may be embedded within a resource provider's checkout page. Hence, the checkout element 608 may be instantiated upon the checkout page being loaded by a browser application via communication between the browser application and an SRT server. Once instantiated, various fields within the checkout element 608 may be populated with data obtained from a memory of the device on which the browser application is instantiated (e.g., from cookies). The resource provider checkout page and the checkout element 608 may be separated such that data populated into the various fields of the checkout element 608 may not be provided to the resource provider. Instead, as described elsewhere, the checkout element 608 may communicate the data to an SRT server and may receive a token to be used in the transaction. The checkout element 608 may then provide the token to the resource provider (via the checkout page) to be used to complete the transaction.

[0100] FIG. 7 depicts a third example of a process for enabling a transaction to be conducted in accordance with at least some embodiments of the disclosure. FIG. 7 is similar to FIG. 5 and FIG. 6 described above. However, as depicted via GUIs 702, 704, and 706 of FIG. 7, a checkout element 708 may be presented when the user elects to conduct the transaction in a manner which is anonymous to the resource provider. For example, upon selecting an option to check out as a "guest," the checkout element 708 described above may be populated in accordance with techniques described herein. Once populated, the checkout element may convey the populated values to the SRT server, which may provide a token to be used in the transaction depicted in GUIs 702-700. The checkout element may then pass the token to the resource provider (via the resource provider website) in order to enable completion of the transaction without providing sensitive information to the resource provider.

[0101] FIG. 8 depicts a flow diagram illustrating an example process for providing a token to a resource provider in a manner that preserves anonymity for a user in accordance with at least some embodiments. The process 800 may be performed on a client device, such as the client device 228 depicted in FIG. 2.

[0102] Process 800 may begin at 802, when a resource document is presented on a client device. The resource document may be associated with a resource managed by a resource provider. For example, the resource document may be a webpage hosted by the resource provider with respect to a particular product sold by the resource provider. In some embodiments, the resource document may be a “checkout” webpage hosted by a resource provider, with which a user is able to complete a purchase.

[0103] At 804, the process 800 may involve instantiating a checkout element. In some embodiments, the checkout element may be embedded within the resource document. For example, a resource document may include a link or other reference to the checkout element at a particular location within the resource document. When the resource document is loaded by a browser application, the browser application may be caused to retrieve the checkout element via the link and display that checkout element in a specified location within the resource document. It should be noted that though the checkout element may be embedded in the resource document, the resource document may not be granted access to information populated into the checkout element.

[0104] At 806, the process 800 may involve identifying, by the checkout element, user-specific information. In some embodiments, this may involve the checkout element obtaining data stored in an internet cookie in the memory of the client device. In some embodiments, the user-specific information may be a random, or pseudo-random, string of characters which is associated with the user at the remote server, but otherwise unassociated with the user. In at least some embodiments, the resource provider may be prevented from accessing the information indicating the identity of the user obtained by the checkout element.

[0105] In some embodiments, the user-specific information may be obtained via a facilitator application, such as the facilitator application 406 depicted in FIG. 4. In at least some of these embodiments, the user-specific information may include a authentication decision generated by the facilitator application. In some embodiments, a number of facilitator applications may be installed upon the client device. The checkout element may identify the number of facilitator applications (e.g., via an application discovery process) and provide a list of the number of facilitator applications to a user. A facilitator application may then be selected by a user from the list of the number of

facilitator applications installed on the client device. Upon receiving a selection of the facilitator application to be used, the facilitator application may be caused to be launched to authenticate the user, and generate the authentication decision upon authenticating the user. In some embodiments, the checkout element may cause the facilitator application to be launched via an application programming interface. In some embodiments, the remote server, upon being provided an indication of a facilitator application on the client device, may communicate with a facilitator application server to cause it to launch the facilitator application on the client device. In some embodiments, the facilitator application may be provided a number of transaction details upon its launch (e.g., as parameters in a method call). Upon generation of a authentication decision by the facilitator application, that certificate may be provided to the remote server.

[0106] At 808, the process 800 may involve transmitting the user-specific information to a remote server. In some embodiments, the remote server may be an initiator application server, such as the initiator application server 108 described with respect to FIG. 1 above. In some embodiments, the remote server may be a secure remote transaction server, such as the SRT server 110(A) described with respect to FIG. 1 above.

[0107] Upon receiving the user-specific information, the remote server may identify the user and a payment account associated with the user to be used to complete the transaction. In some embodiments, this may involve the client device receiving, from the remote server via the checkout element, a number of accounts associated with the user, presenting the number of accounts to the user within the checkout element, receiving a selection of a particular account from the number of accounts, and providing the selected account from the number of accounts to the remote server. In some embodiments, the number of accounts associated with the user may be determined by the remote server through communication with a number of processing networks. For example, upon identifying the user based on the provided user identification information, the remote server (which may be an initiator application server) may provide the user's identity to one or more transaction processing networks,

which may then identify accounts issued to the user by various issuers and return a list of available payment accounts to the remote server.

[0108] At 810, the process 800 may involve the checkout element receiving a token from the remote server. The token may be associated with the identified payment account, user, resource provider, and/or transaction. In some embodiments, the token may be a limited-use token that can only be used to complete the transaction at issue. At 812, the process 800 may involve the checkout element providing the received token to a resource provider to complete the transaction.

[0109] Embodiments of the disclosure provide for a number of technical advantages over conventional systems. For example, unlike conventional transaction processing systems, the current disclosure enables a user to conduct transactions with a resource provider while preventing the resource provider from gaining access to sensitive information for the user. Essentially, the user is able to complete a transaction using any account available to that user while being protected from potential risk of unauthorized use of that account. On the other hand, a resource provider is able to ensure that it receives payment for the transaction. This is accomplished via the use of a checkout element that is dynamically populated with user-specific data while that user-specific data is not visible to the resource provider. Hence, embodiments of the disclosure enable a user to conduct transactions securely with a number of entities with which that user does not currently have a relationship.

[0110] A computer system may be used to implement any of the entities or components described above. The subsystems that may be included include system bus. Additional subsystems include a printer, keyboard, storage device, and monitor, which are coupled to display adapter. Peripherals and input/output (I/O) devices, which couple to I/O controller, can be connected to the computer system by any number of means known in the art, such as a serial port. For example, I/O port or external 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 system memory or the storage device, as well as the exchange of

information between subsystems. The system memory and/or the storage device may embody a computer-readable medium.

[0111] As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably-programmed computing device, microprocessor, data processor, or the like. The set of instructions or software code may be stored in a memory or other form of data storage element which is accessed by the computing device, microprocessor, etc.

[0112] 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++ 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 reside on or within one or more computational apparatuses within a system or network.

[0113] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

[0114] As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 presenting a resource document associated with at least one resource
3 managed by a resource provider;
4 upon receiving a request to complete a transaction for the at least one
5 resource, instantiating a checkout element in association with the resource document,
6 the checkout element including one or more fields, the one or more fields of the
7 checkout element determined based on cookies of a client device presenting the
8 resource document and filled with data from the client device;
9 identifying, via the checkout element, information indicating an identity of a
10 user of the client device, wherein the resource provider is prevented from accessing the
11 information obtained by the checkout element, and wherein the information is stored in
12 a memory of the client device;
13 transmitting the information indicating the identity of the user to a remote
14 server;
15 receiving, from the remote server and via the checkout element, a number
16 of accounts associated with the user;
17 presenting the number of accounts to the user within the checkout
18 element via the client device;
19 transmitting a selection of an account from the number of accounts to the
20 remote server;
21 receiving, from the remote server and via the checkout element, a token to
22 be used to complete the transaction, the token generated by the remote server in
23 response to receiving the selection of the account, the token associated with the
24 account, and the token being specific to the resource provider; and
25 providing, via the checkout element to the resource provider, the token.

1 2. The method of claim 1, wherein the resource document associated
2 with the at least one resource comprises a webpage hosted by the resource provider.

1 3. The method of claim 2, wherein the checkout element is embedded
2 into the webpage hosted by the resource provider.

1 4. The method of claim 1, wherein the number of accounts associated
2 with the user is determined by contacting one or more processing networks.

1 5. The method of claim 1, wherein the remote server is an initiator
2 application server.

1 6. The method of claim 1, wherein the remote server is a secure
2 remote transaction (SRT) server.

1 7. The method of claim 1, wherein the information indicating the
2 identity of the user is obtained from an internet cookie stored in the memory of the client
3 device.

1 8. The method of claim 7, wherein the information indicating the
2 identity of the user comprises a random string of characters associated with the user at
3 the remote server.

1 9. A client device comprising:
2 a processor; and
3 a memory including instructions that, when executed with the processor,
4 cause the client device to, at least:
5 present a resource document associated with at least one resource
6 managed by a resource provider;
7 upon receiving a request to complete a transaction for the at least
8 one resource, instantiate a checkout element in association with the resource
9 document, the checkout element including one or more fields, the one or more
10 fields of the checkout element determined based on cookies of the client device
11 presenting the resource document and filled with data from the client device;
12 identify, via the checkout element, information indicating an identity
13 of a user of the client device, wherein the resource provider is prevented from

14 accessing the information obtained by the checkout element, and wherein the
15 information is stored in the memory of the client device;
16 transmit the information indicating the identity of the user to a
17 remote server;
18 receive, from the remote server and via the checkout element, a
19 number of accounts associated with the user;
20 present the number of the accounts to the user within the checkout
21 element;
22 transmit a selection of an account from the number of accounts to
23 the remote server;
24 receive, from the remote server and via the checkout element, a
25 token to be used to complete the transaction, the token generated by the remote
26 server in response to receiving the selection of the account, the token associated
27 with the account, and the token being specific to the resource provider; and
28 provide, via the checkout element to the resource provider, the
29 token.

1 10. The client device of claim 9, wherein the information indicating the
2 identity of the user of the client device comprises an authentication decision.

1 11. The client device of claim 10, wherein the authentication decision is
2 generated by a facilitator application installed on the client device.

1 12. The client device of claim 11, wherein the facilitator application is
2 selected by the user from a number of facilitator applications installed on the client
3 device.

1 13. The client device of claim 11, wherein the instructions further cause
2 the client device to:
3 launch the facilitator application to authenticate the user; and
4 generate the authentication decision upon authenticating the user.

1 14. The client device of claim 13, wherein the facilitator application is
2 provided a number of transaction details upon its launch.

1 15. The client device of claim 11, wherein the facilitator application is
2 launched via an application programming interface associated with the facilitator
3 application.

1 16. The client device of claim 9, wherein the token is a limited-use
2 token that can only be used to complete the transaction.