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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2013 (01.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/113004 Al

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G06Q 30/06* (2012.01)

(21) International Application Number:
PCT/US20 13/023460

(22) International Filing Date:
28 January 2013 (28.01 .2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/591,224 26 January 2012 (26.01.2012) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSO¬CIATION** [US/US]; P.O Box 8999, San Francisco, CA 94128 (US).

(72) Inventors: **ANDERSON, Lisa;** 2101 Bay Street #104, San Francisco, CA 94123 (US). **CUSHLEY, Seamus;** 55A Broagh Road, Castledawson Deny, BT45 8ER Deny (IE).

(74) Agents: **FELD, Nathan, L.** et al; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 941 11 (US).

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

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

Published:

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

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

(54) Title: SYSTEM AND METHOD OF PROVIDING TOKENIZATION AS A SERVICE

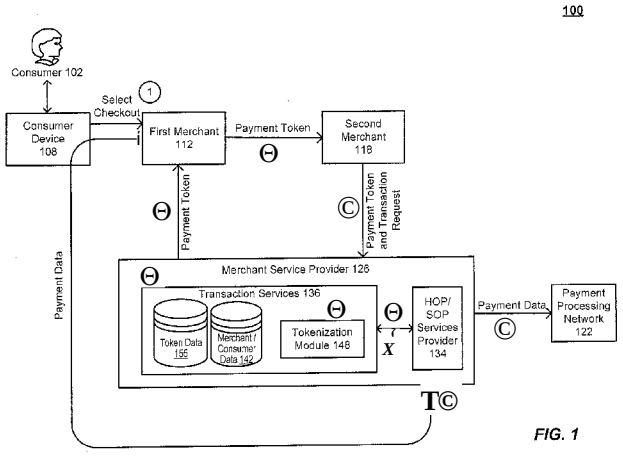

FIG. 1

(57) Abstract: Systems, devices, apparatuses, and methods for providing tokenization as a service are provided. Embodiments of the invention involve decoupling a "tokemzation service" from other services offered by a merchant service provider, and offering the tokenization service as a stand-alone service. In accordance with an embodiment, a merchant service provider can receive payment data associated with a transaction between a consumer and a first entity. The merchant service provider can generate a payment token that represents the payment data and transmit a copy of the payment token to the first entity. The first entity can then transmit the payment token and order information to a second entity specified in the transaction. The merchant service provider can sub - sequently receive a request to complete the transaction from the second entity. The request can include the copy of the payment token from the second entity.

WO 2013/113004 A1

SYSTEM AND METHOD OF PROVIDING TOKENIZATION AS A SERVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from and is a nonprovisional Application of U.S. Provisional Patent Application No. 61/591 ,224, filed on January 26, 2012, titled "TOKENIZATION AS A SERVICE," by Lisa Anderson and Seamus Cushley, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Tokenization is a security (data protection) procedure by which sensitive or otherwise valuable information can be replaced with a token. For example, in paymen transactions, payment account information, such as credit card or bank account numbers, may be replaced with a token by a tokenization service provider. When an online transaction is conducted with a merchant, the payment account information may be sent securely to the merchant's service provider. The service provider can securely store the payment account information and return a token to the merchant. This way, tokenization enables merchants to accept payments via payment card accounts or ban accounts without having to store, transmit or process the sensitive payment data. If th< consumer conducts a subsequent transaction with the merchant, they can select the token associated with the payment account they wish to use and complete the transaction normally. This offers the benefits to the consumer of not having to reenter payment data for each transaction, while protecting the merchant from the risk and cos of storing actual payment data for each of their customers.

[0003] Typically, transaction processing and tokenization are closely coupled service; That is, when a merchant requests a token from their service provider they typically als request that a transaction be processed by their service provider using the payment data corresponding to the token. In current systems, if a merchant were to choose to have a customer's payment data tokenized, and then utilize a different service provider to complete the transaction, the merchant would need to obtain the actual payment dat

to send to the different service provider. As the merchant would now be handling the actual payment data, this would defeat many of the benefits of tokenization.

BRIEF SUMMARY

[0004] A "tokenization service" offered by a merchant service provider (e.g., CYBERSOURCE) is sometimes coupled with the merchant service provider's "paymen authorization service." For example, when a merchant requests that merchant service provider run a payment authorization on a particular credit card, the merchant may alsc request that merchant service provider tokenize the credit card and send a copy of the resulting payment token back to the merchant. In future payment authorization reques involving the same credit card, the merchant can submit the payment token to merchar service provider instead of the actual credit card number. In many instances, the merchant cannot use the payment token for anything other than to request that the merchant service provider run a payment authorization on the underlying credit card. Thus, a merchant may not often request that the merchant service provider tokenize a credit card without also requesting that merchant service provider use the resulting payment token to run payment authorizations.

[0005] Embodiments of the invention involve decoupling the "tokenization service" from the "payment authorization service," and offering the tokenization service as a stand-alone service. By decoupling these services, tokenization as a service (TaaS) enables merchants to share payment tokens.

[0006] For example, a first entity, such as an online travel agent (e.g., ORBITZ), whic provides reservation services for, among other things, rental cars, uses a merchant service provider's (e.g., CYBERSOURCE) hosted payment acceptance services to collect credit card data on its behalf. Further, according to this example, the online travel agent uses the merchant service provider's tokenization service to tokenize the collected credit card data. Thus, according to this example, when a customer enters hi credit card data in the online travel agent's website to pay for a rental car, the merchan service provider would collect the credit card data on travel agent's behalf, generate a

payment token for the credit card, and pass the payment token back to the online trav< agent.

[0007] According to some embodiments, instead of also using the merchant service provider's payment authorization service to run a payment authorization on the credit card, the online travel agent passes a copy of the token to the rental car company frorr which the customer is renting a car. The rental car company, according to some embodiments, can then submit a copy of the token to back to the merchant services provider and request that merchant service's provider: (1) run a payment authorization on the consumer's credit card on behalf of the rental car company to pay for the cost o the rental car (this would enable the rental car company to also avoid handling the cre(card data); or (2) provide the rental car company with the corresponding credit card da so that the rental car company can run the payment authorization itself.

[0008] Embodiments of the invention are directed to methods, a computer-readable medium, servers and systems for enabling entities to transmit payment tokens, insteac of actual payment data. For example, according to embodiments, a payment services server receives from a server of a first entity a consumer's payment data via a network interface. The payment services server processes the payment data to generate a payment token that represents the payment data, and transmits a copy of the resulting payment token, via a network interface, back to the server of the first entity. The serve of the first entity transmits, via a network interface, a copy of the payment token to a server of a second entity. The server of the second entity, via a network interface, transmits a copy of the payment token to the payment services server along with a request to: (1) provide the server of the second entity with the consumer's payment dat that corresponds to the copy of the payment token; or (2) process a payment transaction on behalf of the second entity using the consumer's payment data that corresponds with the payment token. Among other benefits, embodiments of the invention not only enable the first entity to avoid handling the consumer's payment date but embodiments also enable the first entity to avoid being the party that requested the payment transaction. Further advantages of embodiments include enabling the seconc entity to also avoid handing the consumer's payment data.

[0009] Other embodiments of the invention are directed to computer-readable media comprising code for performing the described methods as well as systems, apparatus* and devices that perform the methods and/or that use the computer-readable media.

[0010] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Figure 1 is a block diagram of an example of an operating environment in whic embodiments of the invention can be implemented.

[0012] Figure 2 provides an example process for providing tokenization as a service, according to an embodiment.

[0013] Figure 3 is a block diagram of an example of an operating environment in whic embodiments of the invention can be implemented.

[0014] Figure 4 provides an example process for providing tokenization as a service, according to an embodiment.

[0015] Figure 5 is a block diagram of an exemplary system in which token access is centrally managed, in accordance with an embodiment.

[0016] Figure 6 provides an example process for centrally managing access to payment tokens, in accordance with an embodiment.

[0017] Figure **7** is a block diagram of an exemplary system for authorizing requests using payment tokens, in accordance with an embodiment.

[0018] Figure 8 provides an example process for authenticating a transaction request using a payment token, in accordance with an embodiment.

[0019] Figure 9 is a block diagram illustrating a transaction processing system that may be used with some embodiments of the present invention.

[0020] Figure 10 illustrates an exemplary computer system in which various embodiments can be implemented.

DETAILED DESCRIPTION

[0021] A "hosted order page" (HOP) is a third-party hosted webpage that accept payment data from a customer on a merchant's web site. A merchant typically redirecl a customer to a HOP on the third-party's domain/server when the customer selects a 'Buy' or 'Checkout' button from an online shopping cart. The third party, which is neith' the merchant nor the customer, uses payment data entered by the customer in order t(process a credit card transaction, etc. for the merchant so that the merchant can avoid the cost and effort of complying with the Payment Card Industry Data Security Standar (PCI DSS) and government regulations regarding storing credit card numbers.

[0022] A "silent order post" (SOP) is akin to a HOP but with only the sensitive textboxes and other input controls being hosted by the third party. That is, the mercha hosts the order page but the sensitive fields, such as the credit card number and expiration date entry textboxes, are posted only to the third party's servers.

[0023] Figure 1 is a block diagram of an example of an operating system 100 in whicl embodiments of the invention can be implemented.

[0024] Figure 1 depicts a consumer 102, a user device 108 associated with the consumer 102, a first merchant 112, a second merchant 118, a payment processing network 122, and a merchant service provider 126 ("service provider"), communicative connected. The service provider 126 includes transaction services 136 and HOP/SOP services provider 134 that provides hosted payment pages and silent order posts. The transaction services 136 includes merchant/consumer profile/account data 142 and token data 155 as well as a tokenization module 148. The system 100 illustrated in Figure 1 is referred to as a hosted service system 100, wherein the service provider 126, acting as a "host", hosts services for clients, such as the merchants 112, 118. According to the illustrated embodiment, the merchants 112, 118 and the consumer 1C can transmit information associated with electronic transactions to the service provider 126. According to some embodiments, the merchants 112, 118 may transmit information, such as order information, or a request to create an account, to tokenize payment data, and/or to process a transaction to the service provider 126, which performs one or more services based at least on the transaction information received from the merchants 112, 118.

[0025] The consumer 102 is, generally, any entity that is a purchaser of products or services via an electronic transaction. Non-limiting examples include a person or business entity that purchases, reserves, or licenses goods and / or services from ecommerce websites via the public Internet or at a retail store using a credit card, debi card, e-check, etc. The merchants 112, 118 may be, generally, any entity that offers goods or services in exchange for value.

[0026] The service provider 126 is a third party other than the consumer and merchant, that provides services in support of electronic transactions (e.g., CYBERSOURCE, AUTHORIZE.NET). Non-limiting examples of such services include services related to payment acceptance processing (e.g., HOP and SOP), credit card authorization, payment data tokenization, risk evaluation and management, fraud screening, tax calculation, export compliance verification, delivery address verification, Internet and/or e-mail address verification, payment crediting, billing, and the like. Service providers 126 may invoke service features of other service providers in support of their service offerings.

[0027] The consumer 102 and the merchants 112, 118 may communicate through a network, such as with Internet-originated transactions. As part of a purchasing process certain information is collected from the consumer 102 by the merchants 112, 118. Non-limiting examples of information collected from the consumer 102 include information about the item or service to be purchased/reserved, payment amount, shipping address, and whether the consumer wants to create an account with the merchant. However, some merchants may opt to not collect payment data, such as credit or bank card payment account numbers, and instead request that the service provider 126 collect such information on their behalf. For example, merchants may opt not to collect payment data because merchants want to avoid the costs associated with PCI compliance.

[0028] Once transaction and consumer-related information is collected by a merchant 112, 118, the merchant transmits at least a portion of the information to the service provider 126. Additional information may be transmitted along with the information described. For example, the merchant 112, 118 may transmit customized data or a specification of service provider 126 services to apply, or to ignore, in the electronic

transaction processing that is provided by the service provider 126. Although not limite to any specific information, the types of information described above are referred to collectively herein as "order information." Any or all of the information referenced above, which is transmitted from the merchant 112, 118 to the service provider 126, may be transmitted through a network in any suitable protocol. An example of a suitable protocol is Secure Sockets Layer (SSL).

[0029] The service provider 126 performs one or more services in relation to the electronic commercial transaction associated with transmitted transaction information. Typically, when not implementing embodiments described herein, the service provider 126 performs services in a manner predetermined by the service provider 126. For example, specific services are performed in a specific order for specific merchants, according to a service provider default or to an agreement between the merchant and the service provider.

[0030] An example will now be provided with reference to the encircled reference numerals 1-9 provided in Figure 1. It should be appreciated that the encircled referenc numerals are provided for illustrative convenience and are not intended to limit ways in which data may flow or the order in which steps may be executed in the system 100. For example, data may flow to and from any component of the system 100 in any ordei

[0031] Referring to encircled reference numeral 1 of Figure 1, this example begins wit the consumer 102 visiting the merchant webpage, which is provided by a merchant wel server. While visiting the merchant page, the consumer 102 can search for and view details for items and services. For example, the first merchant 112 may be an online travel company / agency (e.g., ORBITZ, EXPEDIA, etc.) that provides reservation services for the second merchant 118, which may be a rental car company. In this example, the consumer 102 may search for and view details of rental cars, and the consumer 102 may select a "Book Now" or "Make a Reservation" button to reserve a rental car. When the consumer 102 decides on an item / service to purchase / rent / reserve, the consumer may indicate his selection by selecting the item / service, such as by selecting a "Book Now", "Reserve", "Purchase" button.

[0032] As indicated at encircled reference numeral 2 of Figure 1, when the consumer 102 communicates his decision to the first merchant 112, such as by selecting the "Book Now" or "Reservation" or "Purchase" button on the merchant page, the merchant 112 invokes the service provider 126 to collect payment data from the consumer 102, such as via a HOP or SOP. This enables the merchant 112 to avoid handling the consumer's payment data.

[0033] For example, the first merchant 112 may utilize a HOP, which is provided by the service provider 126 to collect payment data on behalf of the merchant 112. In the event a HOP is used, the "Book Now" or "Make a Reservation" or "Purchase" button may include a URL that redirects the user device 108 to a location at the HOP services provider 134. When the redirect occurs, the order information, among other information may optionally be transmitted via a secure connection, such as an SSL pipe, from the merchant 112 to the HOP services provider 134 by way of the redirect through the user device 108. In some examples, the order information and other information are provided to the HOP services provider 134 in an HTML post. In any event, when the redirect occurs, the HOP services provider 134 provides a hosted payment page to the consumer 102 via the consumer device 108. For example, the hosted payment page may include a summary of the order information, input fields into which users may input their credit card information, e.g., credit card type, number, expiration data, etc., and input fields into which user may input billing address information for the credit card, and a "Purchase", "Submit" etc. button that user may select to submit their payment data to the service provider 126.

[0034] In accordance with an embodiment, the merchant 112 can elect to use a SOP. When the customers selects the "Submit", "Book Now", or "Make a Reservation" button to confirm a purchase / order / reservation, a script code in the merchant's website initiates a call to the service provider to pass or 'post' the data to the service provider's system, thereby enabling the merchant 112 to avoid handling the payment data.

[0035] In some embodiments, the merchant 112 can elect to use an inline frame, which is provided by the service provider 126 to collect payment data on behalf of the merchant 112. When using an inline frame, the "Book Now" or "Make a Reservation" or similar button may direct the user to another webpage hosted by the merchant 112,

where the service provider 126 provides an inline payment frame in the webpage for collecting payment data and related data, such as address information, from the consumer 102 on behalf of the merchant 112.

[0036] It should be noted that, in the illustrated example, when a HOP and/or SOP is provided, the payment data is transmitted via a secure connection, such as an SSL pipe, from the user device 108 to the service provider 126 and bypasses the merchant 112 altogether. Thus, the merchant 112 does not handle the payment data and therefore does not have to be PCI compliant.

[0037] As indicated at encircled reference numeral 3, the HOP / SOP services providf 134 sends via link 140 the payment data and other associated information (e.g., billing address information) to the transaction services 136, which according to some embodiments, accesses the merchant / consumer profile data 142 to determine whethi the consumer 102 already has an account / profile stored at the merchant service provider 126. If the consumer 102 already has a profile, then the transaction services 136 updates the payment data and the billing information in the consumer's account / profile with the payment data and the billing information that the consumer inputted via the HOP / SOP. If the consumer 102 does not already have a profile, then the transaction services 136 creates an account / profile for the user in the consumer / merchant profile data 142 and stores in the newly created account / profile the consumer's payment data and billing information.

[0038] Further, as indicated at encircled reference numeral 4, the transaction servicei 136 instructs the tokenization module 148 to tokenize the payment data inputted by the consumer 102 and thereby create a payment token for the consumer's payment data (e.g., the tokenization module 148 generates a payment token that represents the consumer's credit card). It should be appreciated that the tokenization module 148 ma create a unique payment token for each payment account (e.g., for each credit card) stored in the consumer's profile. The tokenization module 148 then stores a copy of th payment token(s) in the token database 155. Further, as indicated at encircled reference numeral 5, the merchant service provider 126 sends a copy of the payment token(s) to the merchant 112, which can store the payment token(s) on its database.

For example, the merchant 112 also creates an account / profile for the consumer on it database and stores the payment token(s) in the consumer's account / profile.

[0039] As indicated at encircled reference numeral 6, the first merchant 112 sends a copy of the payment token, which represents the consumer's payment data (e.g., credi card), to the second merchant 118. This may occur, for example, in an arrangement where the first merchant 112 brokers services provided by the second merchant to the consumer 108, e.g., the first merchant 112 could be an online travel agency that advertises and brokers rental cars for the second merchant 118. The second merchan 118 may store the payment token along with information about the consumer 102 in its database. Further, as indicated at reference numeral 7, to process a transaction and receive payment, the second merchant 118 sends a copy of the payment token back tc the merchant service provider 126, along with a transaction request (e.g., a request to charge the consumer's payment account for the cost of a rental car).

[0040] As indicated at encircled reference numeral 8, the transaction services 136 accesses the token data 155 to obtain the actual payment data associated with the token, which was submitted by the second merchant 112. The transaction services 13 may also access the consumer / merchant data 142 to obtain additional information about the consumer 102 (e.g., billing address) and/or the second merchant 118, such as the second merchant's deposit account / acquiring bank information. As indicated a encircled reference numeral 9, to process the payment requested by the second merchant 118, the service provider 126 sends the actual payment data along with transaction data to the payment processing network 122 (e.g. VISA), which processes the payment and then sends a confirmation or denial message to the second merchant 118 or to the service provider 126, which forwards the notice to the second merchant 118. Figure 7 illustrates an environment 10 and process by which the payment processing network, which is illustrated in Figure 7 as an electronic transaction service provider 26, processes the transaction so as to transfer funds from the consumer's account at Issuer 38 to the second merchant's account at Acquirer 30.

[0041] An example process 200 is provided in Figure 2 whereby the process involves processing a payment transaction, according to an embodiment. The process 200 of Figure 2 is described herein as being implemented by system 100 of Figure 1.

However, it should be appreciated that the process 200 may be implemented in any suitable environment. As illustrated at block 204, a consumer 102, using a consumer device 108, accesses a website provided by a first merchant 112 and selects an item / service for purchase, or the consumer 102 selects to reserve the item / service, where the item / service is provided by a second merchant 118. For example, the first merchant 112 may be travel services website (e.g. an online travel agent, such as ORBITZ) and the second merchant 118 may be a rental car company. In operation, the first merchant 112 via its website may present to consumers rental cars that are owned and operated by the rental car company, and consumers may be able to reserve the second merchant's rental cars via the first merchant's website.

[0042] In some instances, it may be desirable for the first merchant 112 to avoid handling the consumer's payment data. This would enable the first merchant 112 to avoid PCI compliance, and to avoid being responsible for charging the consumer.

[0043] As illustrated at block 208, the merchant service provider 126 obtains the consumer's payment data. For example, the merchant service provider 126 collects the consumer's payment data via a SOP, and/or a HOP. Alternatively, in some embodiments, the merchant service provider 126 can collect the consumer's payment data via an inline payment frame. According to block 212, the merchant service provider 126 tokenizes the obtained payment data, and, as indicated at block 216, the merchant service provider 126 stores the resulting payment token along with additional information about the consumer (e.g., name, billing address, etc.) in the token data 155 and/or merchant / consumer data 142. As illustrated at block 220, the merchant service provider 126 sends a copy of the payment token to the first merchant 112, which, according to block 224, sends a copy of the payment token to the second merchant 118. As indicated at block 230, to use the payment token to obtain payment for a service / product that the second merchant 118 is to provide to the consumer 102, the second merchant 118 sends the payment token back to the merchant service provider 126. The merchant service provider 126, according to block 234, obtains the actual payment data associated with the token from the token data 155, and sends the token to a payment processing network for processing the payment on behalf of the second merchant 118. Thus, according to process 200, the first merchant 112 can sell / broke

items / services on behalf of the second merchant 118 without having to handle actual payment data. Further, according to process 200, the second merchant 118 avoids handling payment data, too.

[0044] Figure 3 provides a block diagram of an operating system 300 in which embodiments of the invention can be implemented. The components of system 300 generally correspond to the components of system 100. Further, the steps illustrated t reference numerals 1-6 in Figure 3 generally correspond to the steps illustrated by reference numerals 1-6 in Figure 1. However, the steps illustrated by reference numerals 7-10 of Figure 3 are not illustrated in Figure 1.

[0045] As indicated at encircled reference numeral 7-9 of Figure 3, instead of sending the payment token back to the merchant service provider 126 and requesting that the merchant service provider 126 use the token to obtain the consumer's actual payment data and then send the actual payment data to a payment processing network (e.g. VISA) in the form of a transaction request, the second merchant 118 sends the paymei token to the merchant service provider 126 (reference numeral 7) and requests that the merchant service provider 126 use the token to obtain the consumer's actual payment data (reference number 8) and then send the actual payment data back to the second merchant 118 (reference number 9). Thus, unlike the second merchant in Figure 1, th< second merchant 118 in Figure 3 handles the actual payment data. As indicated by reference numeral 10, upon receiving the consumer's actual payment data from the merchant service provider 126, the second merchant sends the payment data in the form of a transaction request to an Acquirer / payment processor or a merchant service provider 150 other than the merchant service provider 126.

[0046] An example process 400 is provided in Figure 4 whereby the process involves processing a payment transaction, according to an embodiment. The process 400 of Figure 4 is described herein as being implemented by system 300 of Figure 3. However, it should be appreciated that the process 400 may be implemented in any suitable environment. As illustrated at block 404, a consumer 102, using a consumer device 108, accesses a website provided by a first merchant 112 and selects an item / service for purchase, or the user 102 selects to reserve the item / service, where the item / service is provided by a second merchant 118. For example, the first merchant

112 may be travel services website (e.g. an online travel agent, such as ORBITZ) and the second merchant 118 may be a rental car company. In operation, the first mercha 112 via its website may present to consumers rental cars that are owned and operatec by the second merchant (the rental car company). Consumers can reserve the seconc merchant's rental cars via the first merchant's website.

[0047] In some instances, it may be desirable for the first merchant 112 to avoid handling the consumer's payment data. This would enable the first merchant 112 to avoid PCI compliance, and to avoid being responsible for charging the consumer.

[0048] As illustrated at block 408, the merchant service provider 126 obtains the consumer's payment data. For example, the merchant service provider 126 collects th consumer's payment data via a SOP, and/or a HOP. Alternatively, in some embodiments, the merchant service provider 126 can collect the consumer's payment data via an inline payment frame. According to block 412, the merchant service provider 126 tokenizes the obtained payment data, and, as indicated at block 416, the merchant service provider 126 stores the resulting payment token along with additiona information about the consumer (e.g., name, billing address, etc.) in the token data 15E and/or merchant / consumer data 142. As illustrated at block 420, the merchant servic provider 134 sends a copy of the payment token to the first merchant 112, which, according to block 424, sends a copy of the payment token to the second merchant 118. As indicated at block 430, to use the payment token to obtain the consumer's actual payment data, the second merchant 118 sends the payment token back to the merchant service provider 126 and requests that the merchant service provider reply with the actual payment data that corresponds with the payment token. The merchant service provider 126, according to block 434, obtains the actual payment data associated with the token from the token data 155, and, according to block 438, sends the actual payment data to the second merchant 118. The second merchant 118, according to block 442, sends the payment data in the form of a transaction request (e.g. transaction request for payment for the rental car) to an acquirer or a payment processor 150.

[0049] Thus, according to process 400, the first merchant 112 can sell / broker items / services on behalf of the second merchant 118 without having to handle actual paymer

data, whereas, according to process 400, the second merchant 118 does handle payment data.

[0050] As described above, a consumer 102 can conduct a transaction with a first merchant 112 for a product or service provided by a second merchant 118. The first merchant 112 can forward a payment token to the second merchant 118 to complete the transaction, without requiring the first merchant 112 to manage actual payment dat Once the payment token is received by the second merchant 118, the second merchar 118 can request the associated payment data to complete the transaction from the merchant service provider 126. This enables the tokenization of payment data to be decoupled from the payment transaction. However, this decoupling also increases the risk of mistaken or fraudulent use of a payment token.

[0051] Figure 5 is a block diagram of an exemplary system 500 in which token acces; is centrally managed, in accordance with an embodiment. As discussed above with respect to Figures 1-4, the merchant service provider 126 can receive a consumer's payment data and create and store a payment token. As shown in Figure 5, rather tha sending the payment token to the first merchant 112, at 502 the merchant service provider 126 can send payment token access data to the first merchant. This access data can include a key, transaction ID, or other data which corresponds to the newly created payment token. After receiving the payment token access data, at 504 the firs- merchant can send transaction details to the second merchant 118. The transaction details can include the payment token access data which the second merchant 118 cai use to complete the transaction. At 506, the second merchant 118 can send a request including the payment token access data to the merchant service provider 126 to complete the transaction. A token access service 508 can receive the payment token access data and retrieve the payment token from the token data store 155. As described above, the merchant service provider 126 can complete a transaction by retrieving the actual payment data corresponding to the token and either processing th payment itself, or returning the actual payment data to the second merchant 118 for further processing. Additionally, the merchant service provider can send a copy of the payment token to the second merchant 118 to store for use in subsequent transactions with the consumer. Although in Figure 5 the token access service 508 is provided by

the merchant service provider 126, in some embodiments a token access service can be provided as a standalone service which is separate from the merchant service provider.

[0052] Figure 6 provides an example process for centrally managing access to payment tokens, in accordance with an embodiment. At 600, the merchant service provider tokenizes payment data. The payment data can be received by the merchant service provider from a first merchant as described above with respect to Figures 1-4. At 602, the merchant service provider can store the payment token. At 604, the merchant service provider can send payment token access data to the first merchant. Thus, unlike other embodiments discussed above, the first merchant does not receive ; copy of the payment token directly, but instead receives access data, such as a key or transaction ID corresponding to the token, which can be used to retrieve a copy of the token from the merchant service provider if needed. At 606, the first merchant can sen transaction details to a second merchant. As described above, the first merchant acts as a broker for goods or services offered by the second merchant. The transaction details sent to the second merchant can include the payment token access data. At 608, the second merchant can send a request to the merchant service provider to complete the transaction. This request can include the payment token access data anc can specify whether the second merchant requests that the merchant service provider process the payment or return the actual payment details to the second merchant for further processing. This request can additionally include a request for the payment token, for use in future transactions. By centrally managing access to payment tokens at the merchant service provider, the likelihood of misuse of payment tokens, either accidental or malicious, is reduced.

[0053] Figure 7 is a block diagram of an exemplary system for authorizing requests using payment tokens, in accordance with an embodiment. In the embodiment shown in Figure 7, a second merchant 700 can send 702 the payment token to merchant service provider 704 to complete the transaction. As described above with respect to Figures 1 and 3, this can include having the merchant service provider 704 complete the transaction by submitting the payment data to a payment processing network 122, or receiving the payment data in return for the payment token so that the second

merchant 704 can submit the payment data to their acquirer or payment processor. T< reduce the risk of payment tokens being used in fraudulent transactions, the payment token can be verified and the request can be authorized.

[0054] In accordance with an embodiment, payment tokens can be associated with context information. The context information can include one or more of an expiration time/date for the token, merchant identifiers for the first and second merchants, and a transaction identifier. Additionally, trust relationships can exist between the merchants and between each merchant and the merchant service provider. Data describing the trust relationships can be stored by the merchant service provider in, for example, merchant/consumer data 142. When a request is received by the merchant service provider 704 from the second merchant 700 to complete a transaction using a paymen token, a token request authorization module 706 can be used to authorize the request by comparing the context information associated with the payment token with the merchant/consumer data 142. For example, the token request authorization module 706 can determine whether the second merchant is "trusted" by merchant service provider 704 and that the payment token has not expired. If the second merchant is trusted and the payment token is not expired then the request can be authorized. Ono the request is authorized, a token verification module 708 can compare 712 the payment token which accompanied the request to the payment token in token data 15 If the payment tokens match, then the payment data corresponding to the payment token can be retrieved. The payment data can then either be sent to a payment processor by the merchant service provider, as described above in Figure 1, or returne to the second merchant 700 for processing, as described above in Figure 3.

[0055] In accordance with an embodiment, additional authorization and verification methods may be used to determine that a particular transaction request using a payment token is valid. For example, if the second merchant does not have a preexisting relationship with the merchant service provider, and is not a trusted merchant, the merchant service provider can determine whether the second merchant trusted by the first merchant. For example, a particular merchant can maintain a truste merchant list with the merchant service provider which includes a plurality of second merchants with which the particular merchant regularly conducts business. If, for

example, an online travel agent facilitates reservations with a particular group of hotels, each hotel in that group may be added to the online travel agent's trusted merchant list maintained by the merchant service provider. This list can be updated accordingly as the members of the group change over time.

[0056] Figure 8 provides an example process for authorizing a transaction request using a payment token, in accordance with an embodiment. As shown in Figure 8, at 800, the second merchant sends a request to complete a transaction using a payment token to a merchant service provider. The request can include the payment token, context information associated with the payment token, and transaction details. The payment token can be sent to the merchant service provider with a request for the merchant service provider to retrieve the actual payment data associated with the payment token and complete the transaction by submitting the actual payment data an< transaction details to a payment processing network. Alternatively, the request can be for the return of the actual payment data associated with the payment token, such that the second merchant can complete the transaction itself.

[0057] When the second merchant sends the payment token back to the merchant service provider to complete a transaction with a consumer (for example, step 230 in Figure 2), the merchant service provider can authenticate the payment token and authorize the request. At 802, the merchant service provider can authenticate the request using merchant data and the context information. For example, the merchant service provider can determine whether a trusted relationship exists between the second merchant and the merchant service provider, or between the first merchant anc the second merchant. Additionally, the merchant service provider can determine whether the token has expired based on the context information.

[0058] At 804, the merchant service provider verifies the payment token by comparinc it with token data stored by the merchant service provider. This token data can include a copy of the token as originally created. Once the payment token is verified, the request can be completed. At 806, based on the request, the merchant service provide processes the transaction using the actual payment data corresponding to the paymen token, or returns the actual payment data to the second merchant for processing.

[0059] Figure 9 is a block diagram illustrating a transaction processing system 10 that may be used with some embodiments of the present invention. Figure 9 illustrates the primary functional elements that are typically involved in processing a payment transaction and in the authorization process for such a transaction. As shown in Figure 7, in a typical payment transaction, a consumer wishing to purchase a good or service from a merchant uses a payment device 20 to provide payment transaction data that may be used as part of a consumer authentication or transaction authorization process Payment device 20 may be a debit card, credit card, smart card, mobile device containing a contactless chip, computer, or other suitable form of device.

[0060] The portable payment device is presented to a mobile payment acceptance device 22 of a merchant 24. For example, the acceptance device 22 could be a device reader or point of sale (POS) terminal 22 which is able to access data stored on or within the payment device. In embodiments, the portable payment device communicates account/payment data to the merchant 24 via a "card not present" transaction over a communications network, such as a cellular network, the Internet, etc. The account data (as well as any required consumer data) is communicated to the merchant 24 and ultimately to a merchant service provider 26 (such as AUTHORIZE.NET). As part of the authentication or authorization process performed by the merchant service provider, the merchant service provider 26 may access database 28, which typically stores data regarding the customer/consumer/user (as the result of a registration process with the merchant, for example), the consumer's payment device, and the consumer's transaction history with the merchant. The database 28 may also include information about the merchant 24, such as a list of the merchant's approved payment acceptance devices 22. For example, upon receiving information about the payment device 20 from the merchant's mobile payment acceptance device 22, the merchant service provider 26 may extract information that identifies the mobile payment acceptance device 22 and validate that information against a list of approved mobile payment acceptance devices. The merchant service provider 26 typically communicates with acquirer 30 (which manages the merchant's accounts) as part of the overall authentication or authorization process. The merchant service provider 26 and/or acquirer 30 provide data to payment processing network 34, which, among other

functions, participates in the clearance and settlement processes that are part of the overall transaction processing.

[0061] Communication and data transfer between merchant service provider 26 and payment processing network 34 are typically by means of an intermediary, such as acquirer 30. As part of the consumer authentication or transaction authorization process, payment processing network 34 may access account database 36, which typically contains information regarding the consumer's account payment history, chargeback or transaction dispute history, credit worthiness, etc. Payment processing network 34 communicates with issuer 38 as part of the authentication or authorization process, where issuer 38 is the entity that issued the payment device to the consumer and manages the consumer's account. Customer or consumer account data is typicall' stored in customer/consumer database 40 which may be accessed by Issuer 38 as par of the authentication, authorization or account management processes. Note that instead of, or in addition to, being stored in account database 36, consumer account data may be included in, or otherwise part of, customer/consumer database 40.

[0062] According to an embodiment, in standard operation, an authorization request message is created by the mobile payment acceptance device 22 during a consumer purchase of a good or service using a portable payment device. In some embodiments the mobile payment acceptance device 22 of the merchant 24 may be a wireless phone or personal digital assistant that incorporates a contactless card or chip or payment acceptance application. The authorization request message is typically sent from the payment application of the mobile payment acceptance device 22 to the merchant service provider 26, and then to the merchant's acquirer 30, to a payment processing network 34, and then to an issuer 38. An authorization request message can include a request for authorization to conduct an electronic payment transaction and data relevar to determining if the request should be granted as well as device identification information related to the mobile payment acceptance device 22, which the merchant service provider 26 validates against the list of approved mobile payment acceptance devices 22. For example, it may include one or more of an account holder's payment account number, currency code, sale amount, merchant transaction stamp, acceptor city, acceptor state/country, etc. An authorization request message may be protected

using a secure encryption method (e.g., 128-bit SSL or equivalent) in order to prevent unauthorized access to account or transaction data.

[0063] After the Issuer receives the authorization request message, the Issuer determines if the transaction should be authorized and sends an authorization respons message back to the payment processing network to indicate whether or not the currer transaction is authorized. The payment processing system then forwards the authorization response message to the acquirer. The acquirer then sends the respons message to the merchant service provider 26, which then sends the response messagi to the merchant's mobile payment acceptance device 22. The merchant is thus made aware of whether the Issuer has authorized the transaction, and hence whether the transaction can be completed.

[0064] At a later time, a clearance and settlement process may be conducted by elements of the payment/transaction processing system depicted in Figure 2. A clearance process involves exchanging financial details between an Acquirer and an Issuer to facilitate posting a transaction to a consumer's account and reconciling the consumer's settlement position. Clearance and settlement can occur simultaneously o as separate processes.

[0065] Payment processing network 34 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a web server. Payment processing network 34 may use any suitable combination of wired or wireless networks, including the Internet, to permit communication and data transfer between network elements. Among other functions, payment processing network 34 may be responsible for ensuring that a consumer is authorized to conduct a transaction (via an authentication process), confirm the identity of a party to a transaction (e.g., via receipt of a personal identification number), confirm a sufficient balance or credit line to permit a purchase, or reconcile the amount of a purchase with the consumer's account (via entering a record of the transaction amount, date, etc.).

[0066] The payment device 20 may take one of many suitable forms. As mentioned above, the portable payment device can be a mobile device that incorporates a contactless element such as a chip for storing payment data (e.g., a BIN number, account number, etc.) and a near field communications (NFC) data transfer element such as an antenna, a light emitting diode, a laser, etc. The portable payment device may also include a keychain device (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. The device containing the contactless card or chip, or other data storage element may be a cellular (mobile) phone, personal digital assistant (PDA), pager, transponder, or the like. The portable payment device may also incorporate the ability to perform debit functions (e.g., a debit card), credit functions (e.g., a credit card), or stored value functions (e.g., a stored value or prepaid card).

[0067] Figure 10 shows a block diagram of an exemplary computer apparatus that ca be used in some embodiments of the invention (e.g., in any of the components shown i the prior Figures). The subsystems shown in Figure 10 are interconnected via a syster bus 1005. Additional subsystems such as a printer 1010, keyboard 1020, fixed disk 1030 (or other memory comprising computer-readable media), monitor 1040, which is coupled to display adapter 1050, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 1060, can be connected to the computer system by any number of means known in the art, such as through serial port 1070. Fc example, serial port 1070 or external interface 1080 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 1005 allows the central processor 1090 to communicate with each subsystem and to control the execution of instructions from system memory 1095 or the fixed disk 1030, as well as the exchange of information between subsystems. The system memory 1095 and/or the fixed disk 103(may embody a computer-readable medium.

[0068] The previous description of the embodiments is provided to enable any person skilled in the art to practice the invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of

inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the widest scope consistent with the principles and novel features disclosed herein. For example, although some specific embodiments describe the use of a message conversion process with typical brick and mortar type merchants, embodiments of the invention can also be used in on-line e-commerce type transactions.

[0069] Embodiments of the invention are not limited to the above-described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing system, and acquirer, some entities perform all of these functions and may be included in embodiments of invention.

[0070] Further, additional embodiments of the invention may be directed to methods and systems involving merchants, and their access devices, as well as issues. For example, other embodiments may include the following additional embodiments.

[0071] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person o ordinary skill in the art can know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0072] 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 randor 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 CDROM. Any such computer-readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system o network.

[0073] 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.

[0074] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary. A recitation of "she" is meant to be gender neutral and may be read as "he" or "she", unless specifically indicated to the contrary.

[0075] All patents, patent applications, publications, and descriptions mentioned abov are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method, comprising:

receiving, at a merchant service provider, payment data associated with a transaction between a consumer and a first entity, wherein the payment data is receive from the consumer and bypasses the first entity;

generating, at the merchant service provider, a payment token that represents the payment data;

transmitting, from the merchant service provider, a copy of the payment token to the first entity, wherein the first entity transmits the copy of the payment token and order information associated with the transaction to a second entity specified in the transaction; and

receiving, at the merchant service provider, a request to complete the transaction from the second entity, wherein the request includes the copy of the payment token from the second entity.

2. The method of claim 1 further comprising:

authorizing the request to complete the transaction based on merchant information stored at the merchant service provider and context information associated with the payment token.

3. The method of claim 1 further comprising:

verifying that the copy of the payment token received from the second entity matches a copy of the payment token stored at the merchant service provider.

4. The method of claim 2 wherein authorizing the request to complete the transaction comprises:

determining whether the first entity has indicated that the second entity is a trusted entity.

5. The method of claim 2 wherein authorizing the request to complete the transaction comprises:

determining whether the merchant service provider has indicated that the second entity is a trusted entity.

6. The method of claim 2 wherein the context information includes or or more of an expiration time/date for the payment token, merchant identifiers for the first and second entities, and a transaction identifier.

7. The method of claim 1 wherein the request to complete the transaction includes a request for the merchant service provider to process the transaction on behalf of the second entity.

8. The method of claim 1 wherein the request to complete the transaction includes a request to return the payment data corresponding to the paymer token to the second entity.

9. The method of claim 1 wherein the merchant service provider is a hosted order page (HOP) service provider and the payment data is received through a HOP.

10. The method of claim 1 wherein the merchant service provider is a silent order post (SOP) service provider and the payment data is received through a SOP.

11. An apparatus for enabling a consumer to purchase a transit product, comprising:

an electronic processor programmed to execute a set of instructions; and

a memory coupled to the electronic processor and storing the set of instructions;

wherein when executed by the electronic processor, the set of instruction: cause the apparatus to

receive, at a merchant service provider, payment data associated with a transaction between a consumer and a first entity, wherein the payment data is received from the consumer and bypasses the first entity;

generate, at the merchant service provider, a payment token that represents the payment data;

transmit, from the merchant service provider, a copy of the paymer token to the first entity, wherein the first entity transmits the copy of the payment

token and order information associated with the transaction to a second entity specified in the transaction; and

receive, at the merchant service provider, a request to complete the transaction from the second entity, wherein the request includes the copy of the payment token from the second entity.

12. The system of claim 11 wherein the set of instructions further caus the apparatus to authorize the request to complete the transaction based on merchant information stored at the merchant service provider and context information associated with the payment token.

13. The system of claim 11 wherein the set of instructions further caus the apparatus to verify that the copy of the payment token received from the second entity matches a copy of the payment token stored at the merchant service provider.

14. The system of claim 12 wherein authorizing the request to complel the transaction comprises:

determining whether the first entity has indicated that the second entity is a trusted entity.

15. The system of claim 12 wherein authorizing the request to complel the transaction comprises:

determining whether the merchant service provider has indicated that the second entity is a trusted entity.

16. The system of claim 12 wherein the context information includes one or more of an expiration time/date for the payment token, merchant identifiers for the first and second entities, and a transaction identifier.

17. The system of claim 11 wherein the request to complete the transaction includes a request for the merchant service provider to process the transaction on behalf of the second entity.

18. The system of claim 11 wherein the request to complete the transaction includes a request to return the payment data corresponding to the paymer token to the second entity.

19. The system of claim 11 wherein the merchant service provider is a hosted order page (HOP) service provider and the payment data is received through a HOP.

20. The system of claim 11 wherein the merchant service provider is a silent order post (SOP) service provider and the payment data is received through a SOP.

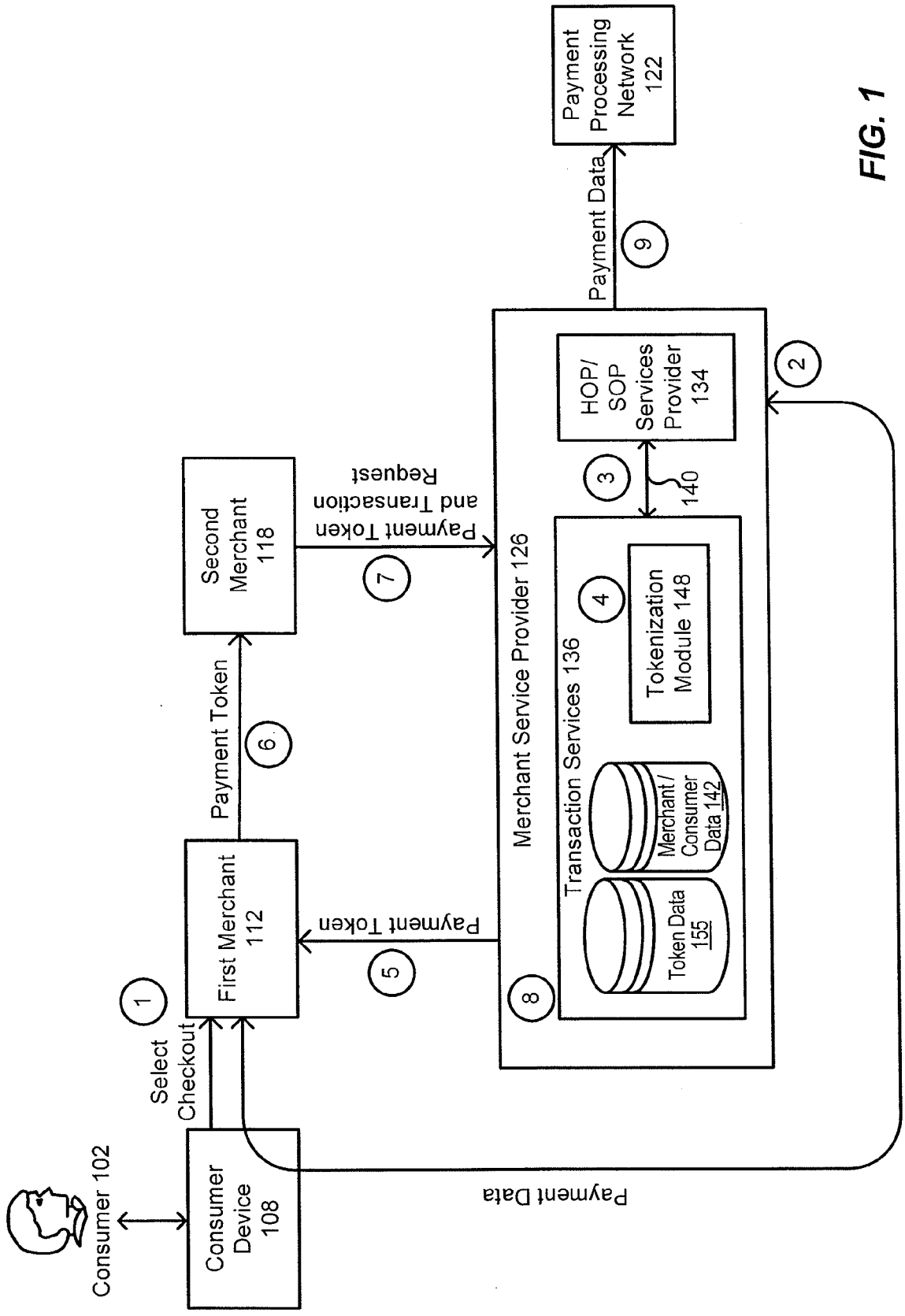
100
Consumer 102
Consumer Device 108
Select Checkout
1
First Merchant 112
Payment Token
6
Second Merchant 118
Payment Token and Transaction Request
7
Payment Token
5
Merchant Service Provider 126
Transaction Services 136
Token Data 155
Merchant / Consumer Data 142
4
Tokenization Module 148
8
3
140
HOP/ SOP Services Provider 134
2
Payment Data
9
Payment Processing Network 122
Payment Data

FIG. 1

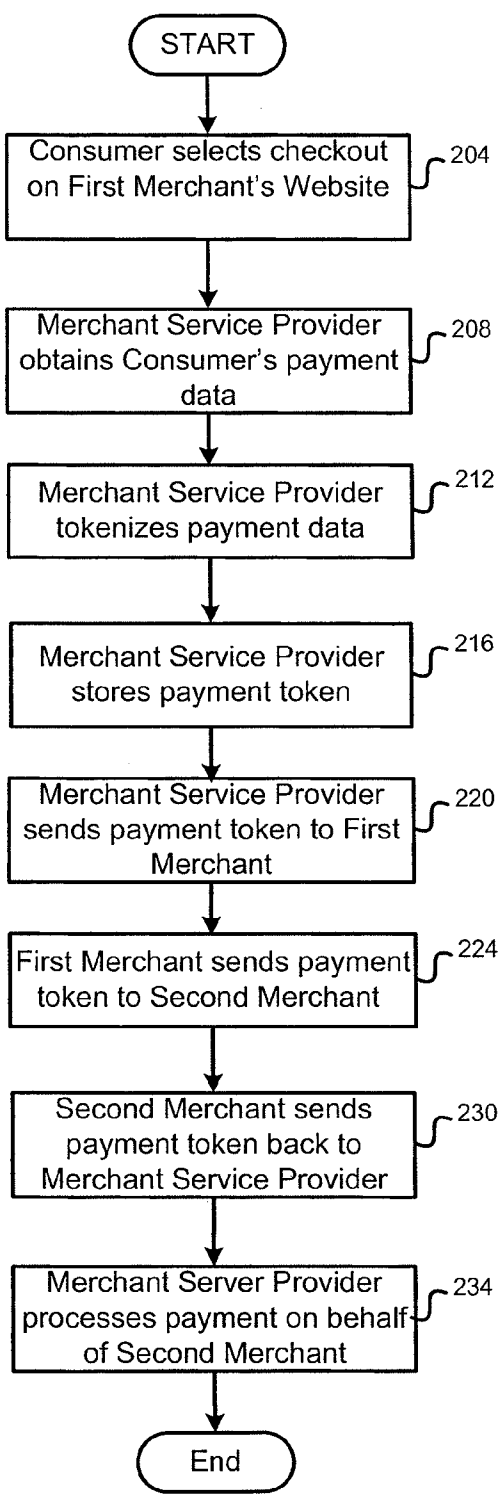
200
START
Consumer selects checkout on First Merchant's Website
204
Merchant Service Provider obtains Consumer's payment data
208
Merchant Service Provider tokenizes payment data
212
Merchant Service Provider stores payment token
216
Merchant Service Provider sends payment token to First Merchant
220
First Merchant sends payment token to Second Merchant
224
Second Merchant sends payment token back to Merchant Service Provider
230
Merchant Server Provider processes payment on behalf of Second Merchant
234
End

FIG. 2

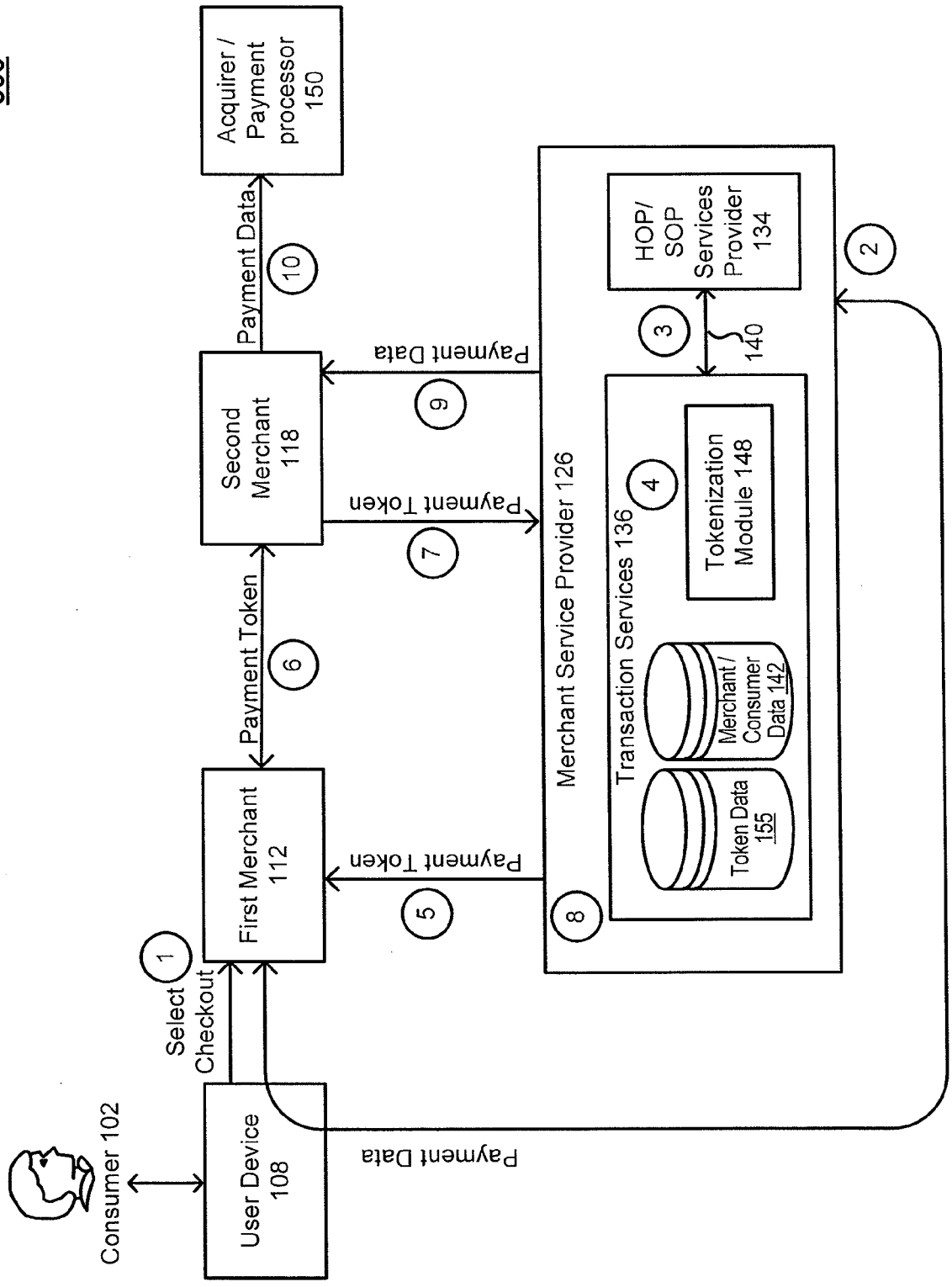
300
Consumer 102
User Device 108
First Merchant 112
Second Merchant 118
Acquirer / Payment processor 150
Merchant Service Provider 126
Transaction Services 136
Tokenization Module 148
Merchant / Consumer Data 142
Token Data 155
HOP/ SOP Services Provider 134
140
Select Checkout
Payment Token
Payment Data
1
2
3
4
5
6
7
8
9
10

FIG. 3

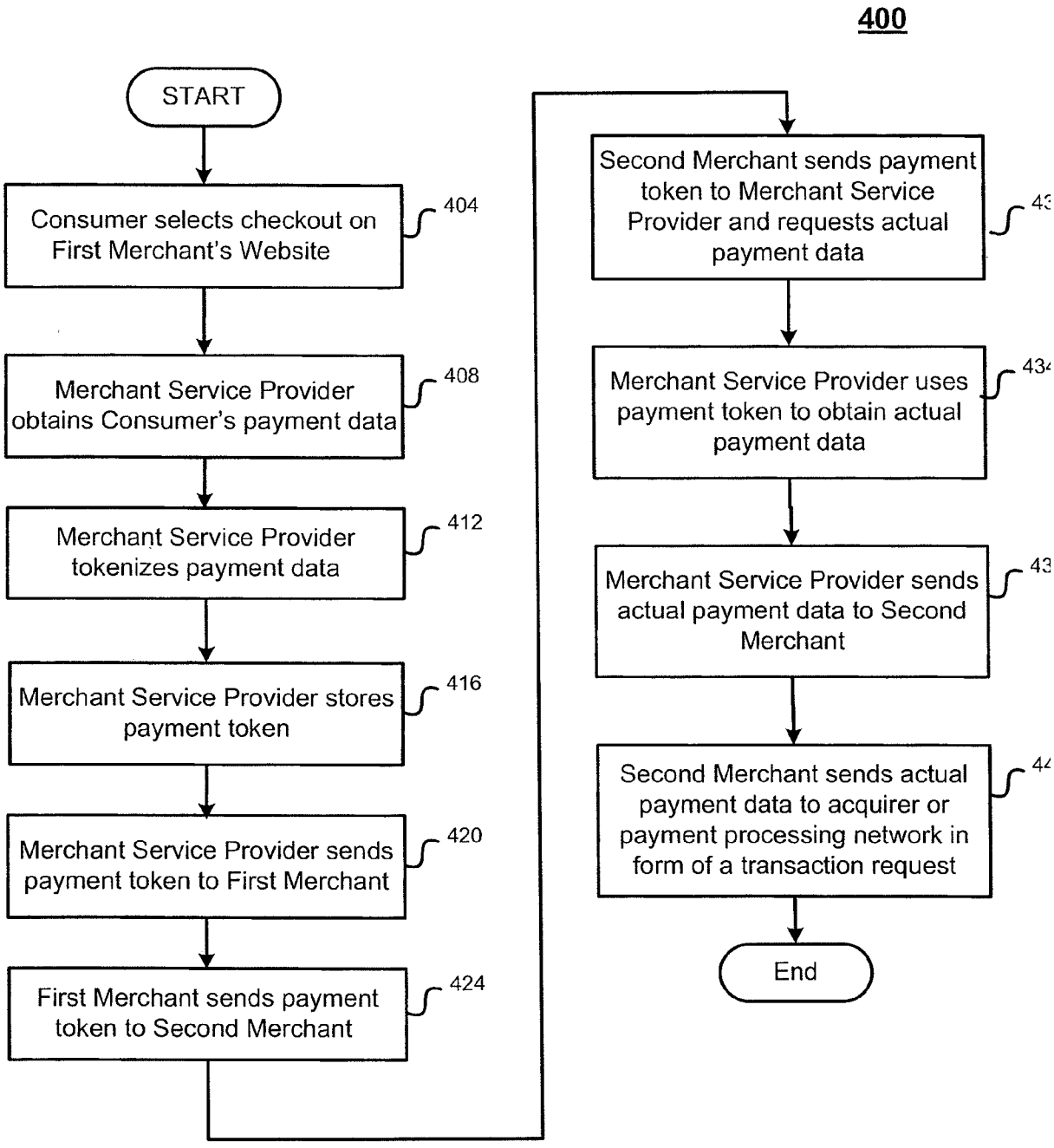
400
START
Consumer selects checkout on First Merchant's Website
404
Merchant Service Provider obtains Consumer's payment data
408
Merchant Service Provider tokenizes payment data
412
Merchant Service Provider stores payment token
416
Merchant Service Provider sends payment token to First Merchant
420
First Merchant sends payment token to Second Merchant
424
Second Merchant sends payment token to Merchant Service Provider and requests actual payment data
Merchant Service Provider uses payment token to obtain actual payment data
Merchant Service Provider sends actual payment data to Second Merchant
Second Merchant sends actual payment data to acquirer or payment processing network in form of a transaction request
End

FIG. 4

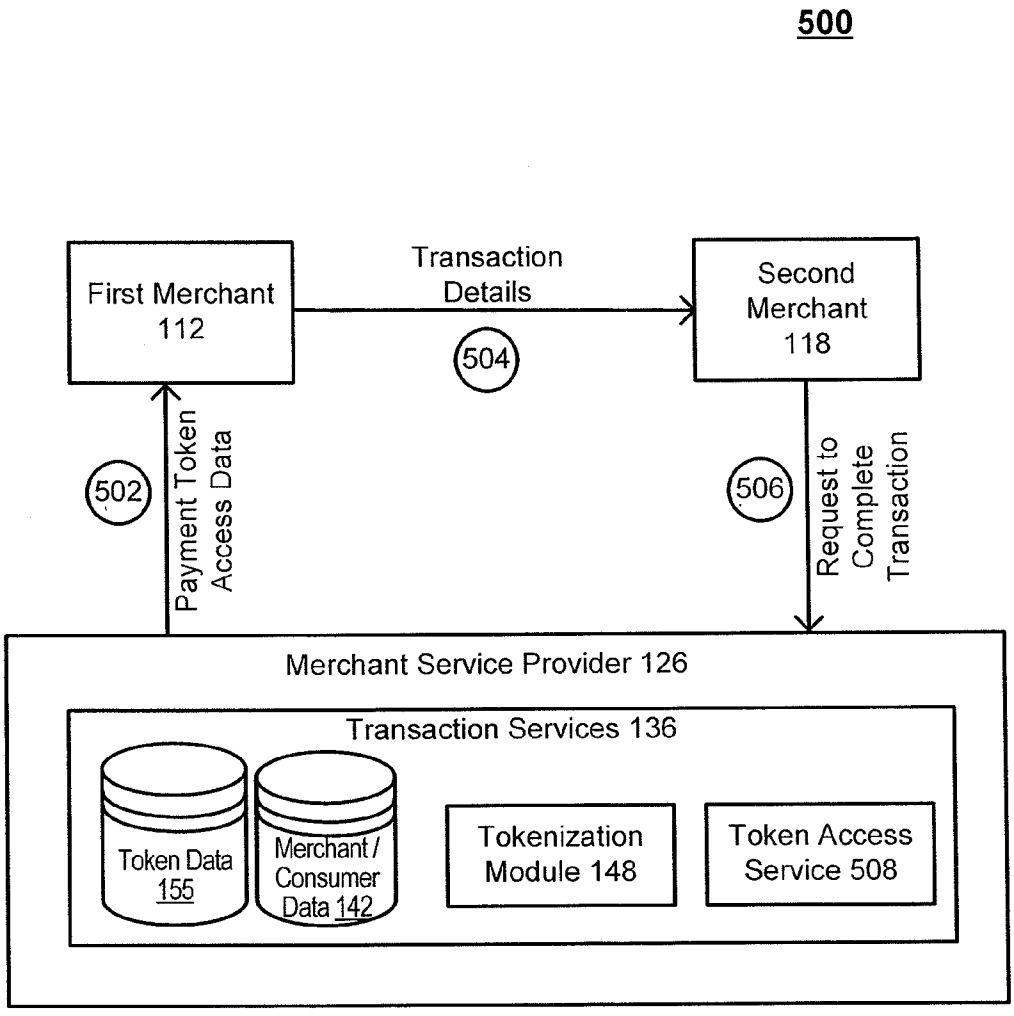
500
First Merchant 112
Transaction Details
504
Second Merchant 118
502
Payment Token Access Data
506
Request to Complete Transaction
Merchant Service Provider 126
Transaction Services 136
Token Data 155
Merchant / Consumer Data 142
Tokenization Module 148
Token Access Service 508

FIG. 5

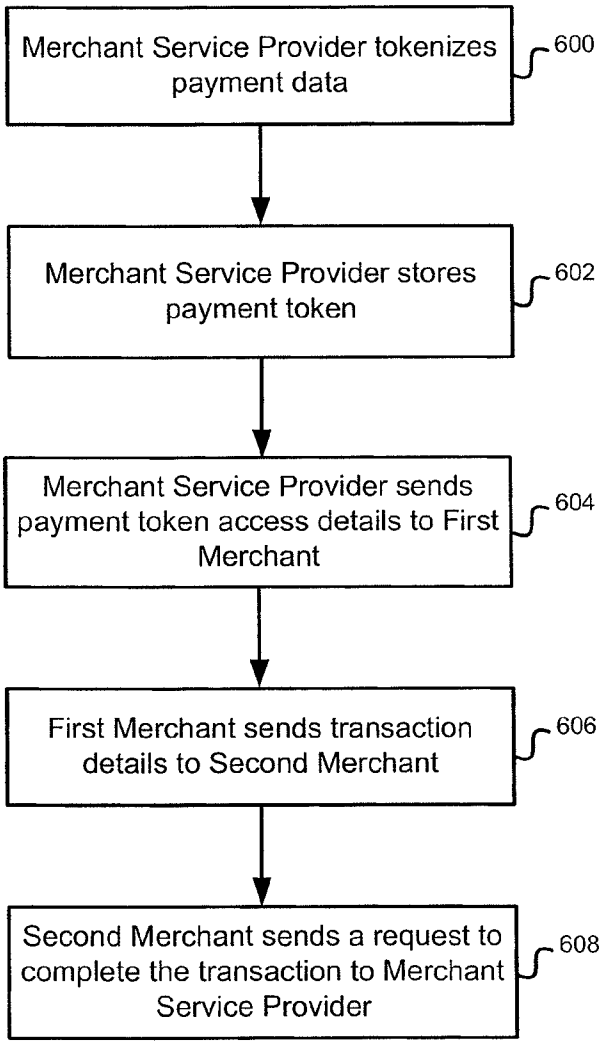
Merchant Service Provider tokenizes payment data
600
Merchant Service Provider stores payment token
602
Merchant Service Provider sends payment token access details to First Merchant
604
First Merchant sends transaction details to Second Merchant
606
Second Merchant sends a request to complete the transaction to Merchant Service Provider
608

FIG. 6

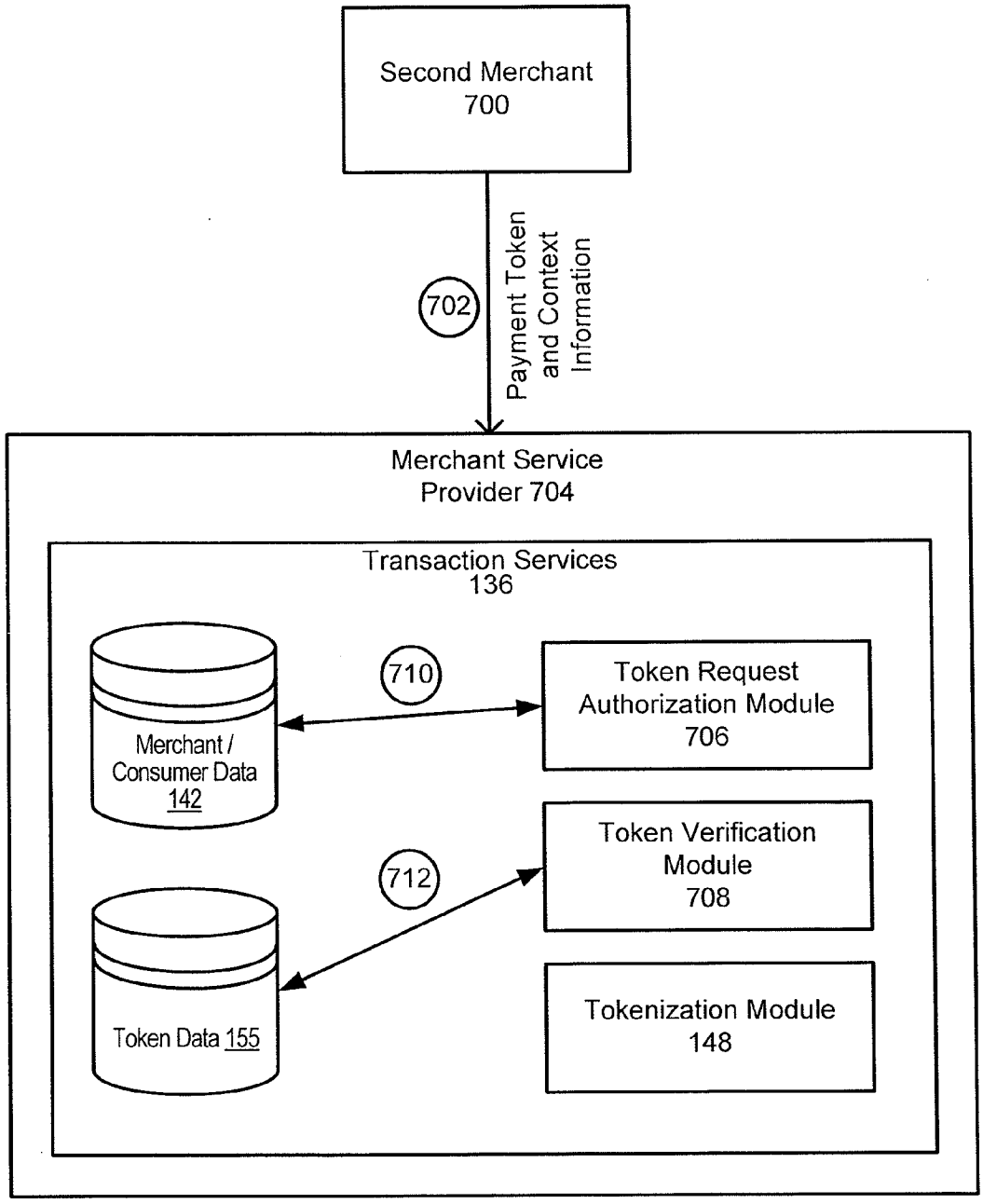
Second Merchant
700
702
Payment Token and Context Information
Merchant Service Provider 704
Transaction Services
136
710
Merchant / Consumer Data
142
Token Request Authorization Module
706
712
Token Verification Module
708
Token Data 155
Tokenization Module
148

FIG. 7

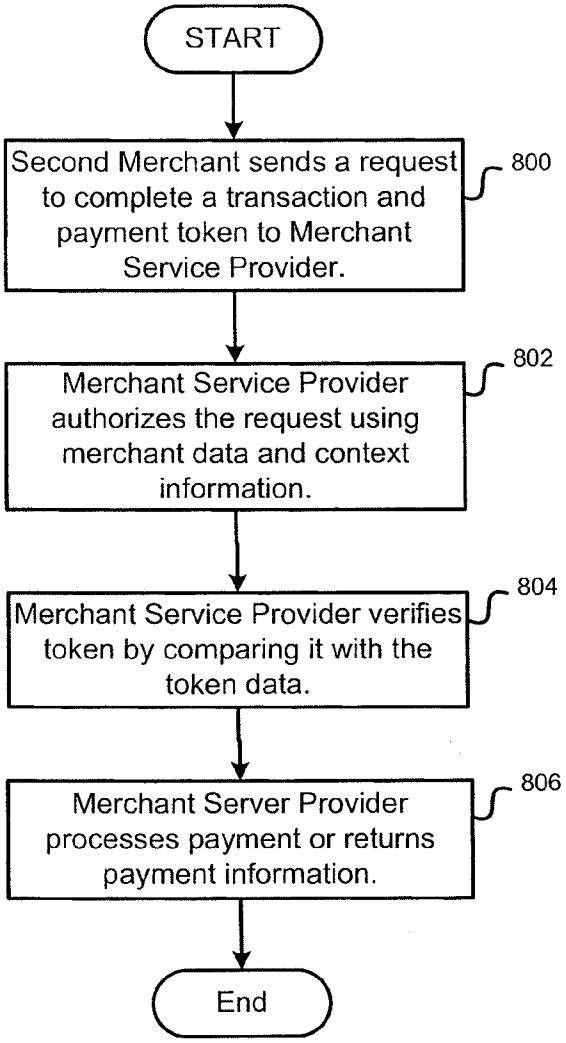
START
Second Merchant sends a request to complete a transaction and payment token to Merchant Service Provider.
800
Merchant Service Provider authorizes the request using merchant data and context information.
802
Merchant Service Provider verifies token by comparing it with the token data.
804
Merchant Server Provider processes payment or returns payment information.
806
End

FIG. 8

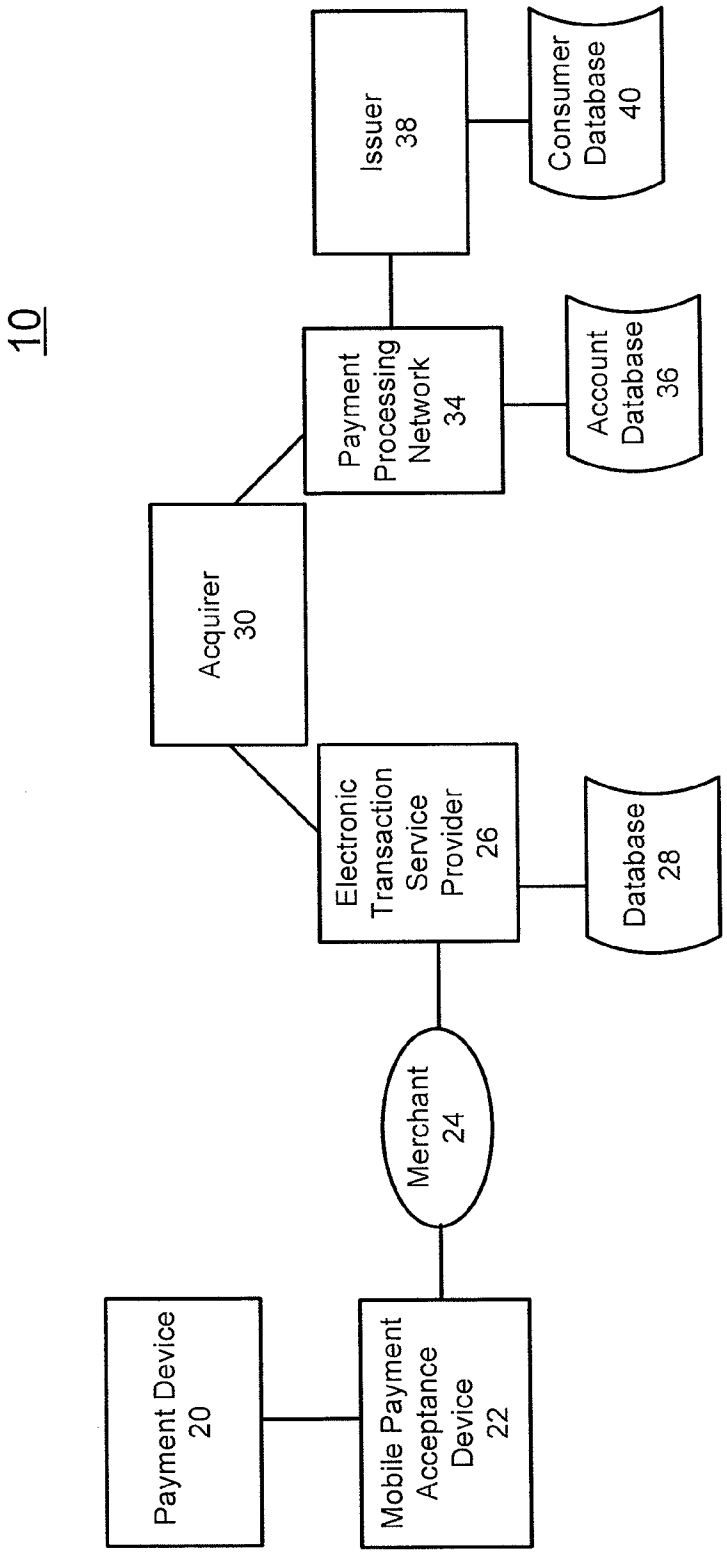
10
Payment Device 20
Mobile Payment Acceptance Device 22
Merchant 24
Electronic Transaction Service Provider 26
Database 28
Acquirer 30
Payment Processing Network 34
Account Database 36
Issuer 38
Consumer Database 40

FIG. 9

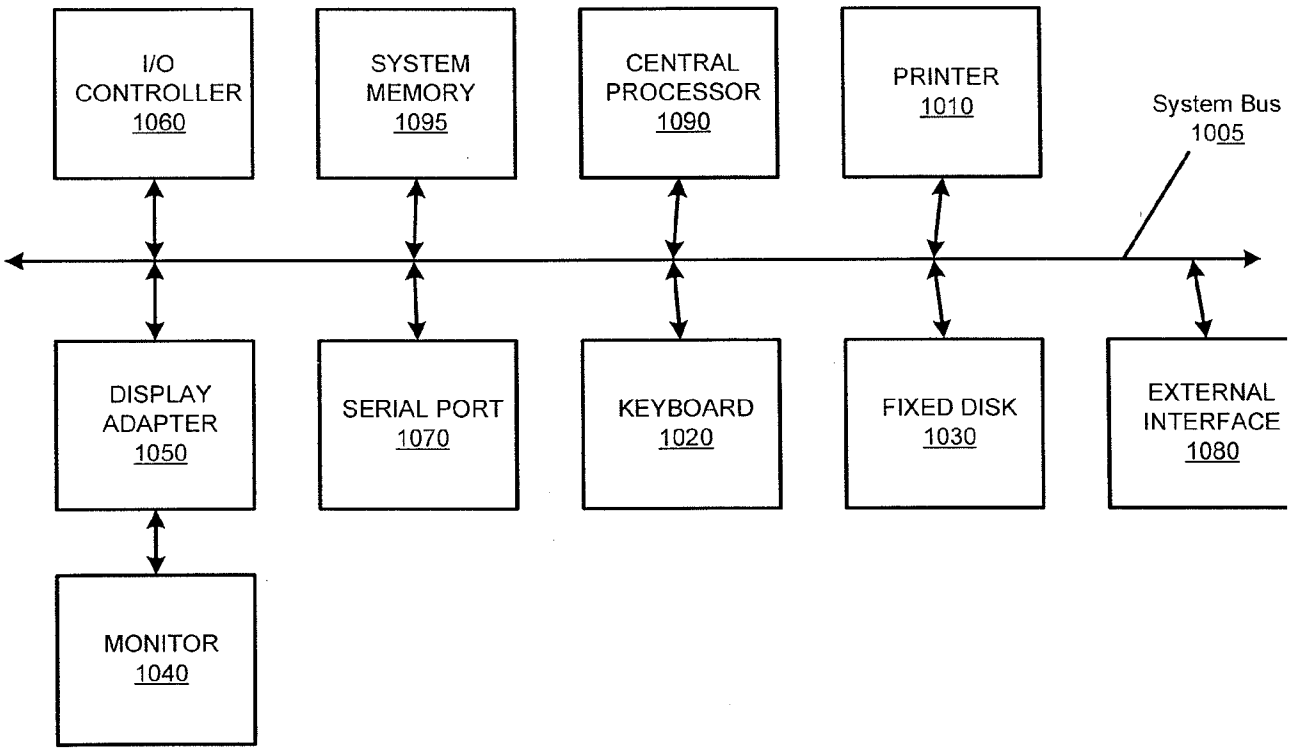
I/O CONTROLLER 1060
SYSTEM MEMORY 1095
CENTRAL PROCESSOR 1090
PRINTER 1010
System Bus 1005
DISPLAY ADAPTER 1050
SERIAL PORT 1070
KEYBOARD 1020
FIXED DISK 1030
EXTERNAL INTERFACE 1080
MONITOR 1040

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/023460

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i, G06Q 30/06(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/40, G06Q 30/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords :tokenization, payment, merchant, token

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010-0017413 Al (JAMES IAN EDWARD) 21 January 2010 See abstract , paragraphs [0006] , [0103H0108] , [0127]- [0134] , claims 1-9 and figure 37.	1-20
Y	US 2007-0288377 Al (YOSEF SHAKED) 13 December 2007 See abstract , paragraphs [0041] -[0045] , claim 1 and figure 1.	1-20
A	US 2009-0292619 Al (KAGAN GERSHON et al.) 26 November 2009 See abstract , claims 1-6 and figures 1,5.	1-20
A	US 2009-0132413 Al (ENGELBRECHT BO K.) 21 May 2009 See abstract , claims 1-2 and figure 1.	1-20
A	KR 10-2006-0018792 A (SK TELECOM CO., LTD.) 02 March 2006 See abstract , claims 1-5 and figure 3.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 June 2013 (17.06.2013)	**18 June 2013 (18.06.2013)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
KIM, Sung Gon
Telephone No. 82-42-481-8746

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/023460

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0017413 Al	21.01.2010	AR072514A1	01.09.2010
		AU 2009-271102 Al	21.01.2010
		CA 2730138 Al	21.01.2010
		CN 102089781 A	08.06.2011
		EP 2335213 A2	22.06.2011
		JP 2011-528473A	17.11.2011
		KR 10-2011-0053219 A	19.05.2011
		MX 2011000653 A	23.05.2011
		TW 201009733 A	01.03.2010
		WO 2010-009059 A2	21.01.2010
		WO 2010-009059 A3	15.04.2010
US 2007-0288377 Al	13.12.2007	WO 2007-148234 A2	27.12.2007
		WO 2007-148234 A3	23.04.2009
US 2009-0292619 Al	26.11.2009	EP 2008236 A2	31.12.2008
		EP 2008236 A4	05.10.2011
		WO 2007-118052 A3	13.12.2007
US 2009-0132413 Al	21.05.2009	AU 2005-305398 Al	18.05.2006
		CA 2625808 Al	18.05.2006
		EP 1828866 Al	05.09.2007
		JP 2008-521086 A	19.06.2008
		WO 2006-052203 Al	18.05.2006
KR 10-2006-0018792 A	02.03.2006	AU 2005-275633 Al	02.03.2006
		CA 2577682 Al	02.03.2006
		CN101048790 A00	03.10.2007
		EP 1784772 Al	16.05.2007
		EP 2587420 Al	01.05.2013
		JP 05007821 B2	22.08.2012
		JP 2008-511067 A	10.04.2008
		US 2008-0189186 Al	07.08.2008
		WO 2006-022513 Al	02.03.2006