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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 July 2016 (21.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/114721 A1

(51) International Patent Classification:
G06Q 20/22 (2012.01) *G06Q 20/24* (2012.01)

(21) International Application Number:
PCT/SG2016/050014

(22) International Filing Date:
14 January 2016 (14.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201500276V 14 January 2015 (14.01.2015) SG

(71) Applicant: **MASTERCARD ASIA/PACIFIC PTE LTD** [SG/SG]; 152 Beach Road, #35-00 Gateway East, Singapore 189721 (SG).

(72) Inventors: **VENUGOPALAN, Vijin**; 152, Gateway East, Beach Road, #35-00, Singapore 189721 (SG). **PRASHANT, Sharma**; 152, Gateway East, Beach Road, #35-00, Singapore 189721 (SG). **GILBEY, Benjamin**; 152, Gateway East, Beach Road, #35-00, Singapore 189721 (SG).

(74) Agent: **POH, Chee Kian, Daniel**; Marks & Clerk Singapore LLP, Tanjong Pagar, P O Box 636, Singapore 910816 (SG).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: METHOD AND SYSTEM FOR MAKING A SECURE PAYMENT TRANSACTION

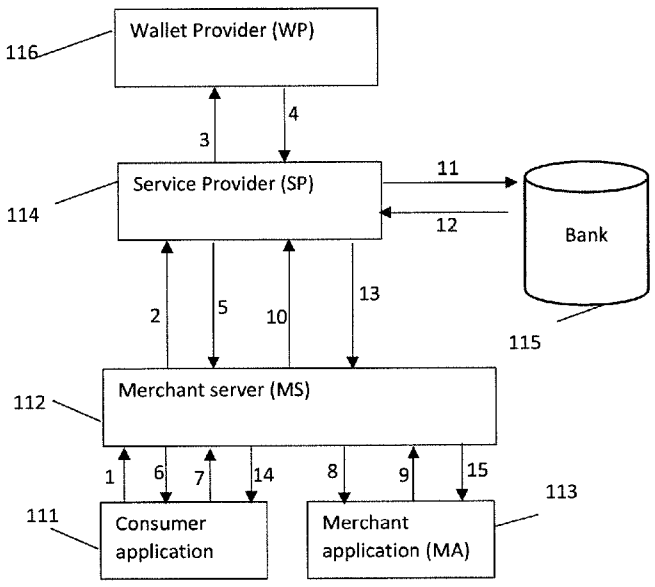

Fig. 3

(57) Abstract: A method and system are presented for making a secure payment transaction using a payment card associated with a consumer which has been registered with a digital wallet. A secure server is arranged, in response to a request from a merchant server in relation to the consumer, to extract from the digital wallet payment credentials for the payment card. The secure server uses the payment credentials and the identity of the merchant server to generate a token. The token is provided to the merchant. To effect a payment transaction, the merchant server returns the token to the secure server with details of the desired payment transaction, and the secure server arranges for the payment transaction to occur, and notifies the merchant server. The merchant server does not receive the payment credentials of the payment card during this process, so even if its security is compromised, the payment credentials are not at risk.

WO 2016/114721 A1

Method and System for making a secure payment transaction

Field of Invention

This invention relates to methods and systems for permitting consumers to make a purchase, for example, but not exclusively, at a point of sale location, such as a retail store, a café or restaurant, or at a location where they pay for a service, such as in a taxi.

Background

It has become common for consumers provided with a payment card (credit card or debit card) to employ a digital wallet to make online purchases. One well-known system is the "Masterpass™" system offered by Mastercard International Inc. and depicted in Fig. 1.

A consumer uses software such as a browser running on a computer 101 associated with the consumer. The computer 101 is connected via the internet to a merchant server 102 (i.e. one operated by a "merchant" which retails, or offers for hire or rental, product(s) and/or service(s)). The details of one or more payment cards associated with the user are stored in a server 103 under the control of a bank which issued the cards ("issuing bank"). These details include "payment credentials", such as the primary account number (PAN), which is conventionally a 16-digit number. The server 103 operates as a "digital wallet", and the server 103 is designated in Fig. 1 as a "wallet provider". When the consumer wants to make a purchase from the merchant (which may be purchase of a physical item and/or of a service), the consumer controls the computer 101 to communicate with the merchant server 102 and make the purchase. During this process the consumer instructs the merchant server 102 that the purchase is to be paid for using a payment card having details which are stored in the digital wallet. The merchant server 102 submits a request to the wallet provider 103 including identity data specifying the identity of the user, so that the wallet provider 103 can obtain the corresponding payment credentials. If the details of multiple payment cards associated with the consumer are stored in the digital wallet, the consumer selects one of the payment cards, and the wallet provider 103 obtains the payment credentials of the corresponding card.

The wallet provider 103 sends a message to the merchant server 102 which includes the payment credentials of the (selected) payment card in the digital wallet. The merchant server

102 passes the message to its bank 104 (the "acquiring bank") which communicates with the bank which issued the payment card ("issuing bank") via a payment network, for example Banknet operated by MasterCard, to authorize and subsequently effect the transfer of the corresponding sum of money. Once the payment transaction is authorized, the merchant server 102 completes the purchase, e.g. dispatching a purchased item to the consumer.

This system, while having many advantageous features, has some disadvantageous features also. One is that it involves passing the payment credentials (which are highly confidential information) to the merchant site, which may not be entirely trustworthy (e.g. if the online merchant is hacked or a fraudulent merchant site).

Summary of Invention

The present invention proposes in general terms that, upon a request from a merchant server, a secure server uses the payment credentials stored by the wallet provider to generate a token. The token is provided to the merchant server. To effect a payment transaction, the merchant server returns the token to the secure server with details of the desired payment transaction, and the secure server arranges for the payment transaction to occur, and notifies the merchant server. The merchant server does not receive the payment credentials of the payment card during this process, so even if its security is compromised, the payment credentials are not at risk.

Furthermore, the token is preferably specific to the merchant (as well as to the payment card), so even if the token is stolen by a thief, the thief is not able to use it to make a purchase from another merchant.

Typically, the secure server is not the associated with the wallet provider. It may for example, be a separate "service provider" operated by a banking organization, such as a bank at which the merchant maintains an account (the "acquiring bank").

The invention is particularly applicable to a situation in which the consumer wants to purchase an item/service from a point-of-sale location, such as one which is physically distant from the merchant server in the sense that a telecommunications link is provided between them. The point-of-sale location may, for example, be a retail store, a restaurant or café, or even a mobile point-of-sale location such as a bus or a taxi cab. The merchant server in this case communicates with equipment located at the point-of-sale location to inform the equipment that the purchase has been authorized.

In an example, the equipment at the point-of-sale location may be responsible for calculating the transaction amount (e.g. if the purchase is of food and/or drink, the total price of the items the consumer has ordered plus any applicable taxes; or if the purchase is of a service, such as being driven on a certain journey by a taxi, the price of the service), and the transaction amount is communicated from the equipment at the point-of-sale location to the merchant server. The merchant then provides the secure server with the token and the transaction amount, so that the secure server can arrange for the transaction to be authorized and the payment to be made.

In preferred embodiments, a token is generated for each respective payment transaction. Thus, once the token has been used, a thief who acquires it cannot use it even with the same merchant.

The "payment card" referred to in this document is not necessarily a physical (e.g. plastic) card. Rather, the term refers to a credit card or debit card account, having a primary account number (PAN) maintained by a "card issuer" (typically, a bank). The PAN functions as payment credentials used when making a payment. Conventionally, the PAN is a 16-digit number, which, if a physical card exists, is printed on the card. However, a payment card can be used in the present invention irrespective of whether a physical card bearing the payment credentials exists.

Brief Description of the Drawings

Embodiments of the invention will now be described for the sake of example only, with reference to the following drawings in which:

Fig. 1 is a diagram illustrating the operation of a prior art digital wallet system;

Fig. 2 illustrates a system which is an embodiment of the present invention;

Fig. 3 illustrates, for the system of Fig. 3, process steps which are performed by the system of Fig. 2 during a transaction process which is an embodiment of the invention; and

Fig. 4 is a flow diagram showing steps in the transaction process of the embodiment of Fig. 3.

Detailed Description

Referring to Fig. 2, a system is shown which is an embodiment of the invention. The system performs a process which is described below with reference to Figs. 3 and 4.

The system of Fig. 2 includes a consumer application 111 (CA) which runs on a computer (not shown) operated by a consumer, such as a personal computer, laptop or mobile device (e.g. a mobile phone or tablet computer). The consumer application is capable of communicating with a merchant server 112 (MS), typically over the internet. The merchant server 112, which is operated by a merchant (an individual or organization which supplies products and/or services in return for payment), may in fact comprise multiple physical servers cooperating together to provide a merchant website, offering one or more products and/or services.

The CA may be supplied by the merchant, and may be arranged to present to the consumer the item(s) (product(s) and/or service(s)) which the merchant supplies. It may include a database describing these item(s), or obtain the information as required by communicating with the merchant server 112.

The merchant also operates at one or more points-of-sale distant from the merchant server (e.g. at least 500m, at least 10km, and perhaps 10s, 100s or even 1000s of kilometers distant from the merchant server). Indeed, the point-of-sale may be a mobile point-of-sale, such as one located in a vehicle (a taxi, bus, or train), which is able to give the consumer (and/or any accompanying persons) a ride. It may alternatively be at a station where vehicles arrive or depart.

At each point-of-sale there is respective equipment running an application associated with the merchant: a "merchant application (MA)". The consumer may be at one of these points-of-sale, and/or wishes to obtain a product and/or service delivered at this point of sale. The merchant application at this one of the points-of-sale is denoted by 112 in Fig. 2, and the merchant applications at any other points-of-sale are omitted from Fig. 2. These other points-of-sale play no role in the process described below.

The point-of-sale is typically equipped with any necessary physical items and/or personnel to implement the purchase. For example, if the purchase is of a physical product, that product may be located at the point-of-sale, so that the consumer may take it away following the purchase, or so that it can be delivered to him from the point-of-sale. In another example, if the purchase is of a food and/or beverage, the point-of-sale may be a café or restaurant, where the food and/or beverage may be prepared and consumed. In a further example, the point-of-sale may be at a location where a train, bus or taxi may be mounted or dismounted, with any necessary driver also being present. In yet a further example, purchase may relate to the

rental of a physical item (e.g. a bicycle or car) and the point-of-sale may be a location where the consumer may obtain or return the physical item.

Note that the equipment running the merchant application may not be owned by the merchant, or dedicated to running the application. For example, it is possible to envisage a retail store providing equipment which is arranged to run a respective merchant application for each of a plurality of merchants. Each application would permit the consumer, when he or she is at the point-of-sale, to make a purchase of a product and/or service from the corresponding merchant.

The merchant is also able to communicate with a service provider 114 (SP). The merchant maintains a bank account with a bank 115 ("acquiring bank"), which typically also operates the service provider 114. The service provider 114 is, unlike the merchant server 112, assumed to be a secure environment. As in the system of Fig. 1, the consumer has a digital wallet provided by a wallet provider (WP) 116. The consumer has pre-registered one or more payment cards (credit cards and/or debit cards) with the wallet provider (WP) 116, which is able to access a database containing payment credentials of the registered cards, i.e. data which can be used to make a payment using the payment card. This data is typically the primary account number (PAN) which, conventionally, is a 16 digit number of the card. The wallet provider (WP) is typically operated by a bank which issued the pre-registered payment card(s). The service provider 114 is able to interact with the wallet provider 116 to access the payment credentials, but since the wallet provider 116 is assumed to be secure, this does not compromise the security of the system. Note that the system of Fig. 1 does not contain an element corresponding to the service provider 114. The service provider 114 is PCI (payment card industry) compliant; that is, it conforms to the PCI data security standard (PCI DSS) maintained by the PCI Security Standards Council.

Turning to Fig. 3 the various communications within the system when a payment transaction is to be made, are shown, numbered 1-15. Fig. 4 is a flowchart showing the steps 1-15 of the method which results in the respective communications 1-15.

In step 1, the consumer operates the consumer application 111 (CA), and decides to make a purchase, and instructs the consumer application 111 accordingly. At this stage, the consumer application 111 may display a number of different payment options (e.g. using respective payment methods), and the consumer selects to make a payment by the method proposed here. For example, he may click on branding (a payment acceptance brand) displayed by the

consumer application 111 and associated with the present method. That is, it includes an acceptance of the use of a payment card registered with the digital wallet 116. Note that the displayed payment options may include multiple digital wallets (e.g. associated with different issuing banks), so that the consumer can select the appropriate digital wallet. The consumer application 111 then sends a request to the merchant server 112 (MS) to obtain payment credentials. This includes a message that a payment card registered with the digital wallet is to be used. The request further includes data specifying the identity of the point-of-sale, i.e. one at which the consumer is located and/or from which he or she wishes to receive a product and/or service. Specifically, it includes merchant information such as a unique merchant identifier for which a payment acceptance mark has been established.

In step 2, the merchant server 112 requests payment credentials from the service provider 114 (SP) by sending it a message.

In step 3, the service provider 114 requests payment credentials from the wallet provider 116 (WP) by sending it a message including the identity data.

The wallet provider 116 then verifies the identity of the consumer by further steps which are not shown in Fig. 1, but are as in conventional methods. . Typically, the WP renders to the consumer (e,g. using the CA which connects to the WP using the internet) a page where the consumer will have to enter identity data, such as a user name and, typically, a secret password. Alternatively, the wallet provider may use a so-called "2 factor authentication", by sending a one-time-pass (OTP) by SMS to a mobile device (perhaps the one on which the CA is running) associated with the consumer. This information is not transmitted through the service provider, but directly between the consumer and the wallet provider. The consumer can transmit the OTP back to the service provider 114 (e.g. directly over a telecommunications network, or the Internet). Using the identity of the consumer, the wallet provider 116 obtains payment credentials of a payment card associated with the consumer from its database.

If multiple payment cards associated with the consumer are registered with the wallet provider 116 which the consumer selected, then the consumer is enabled to select one of them. This may be done by a separate process (not shown) of communication between the consumer and the wallet provider 116.

In step 4, the wallet provider 116 sends the service provider 114 the (real) payment credentials of the selected payment card from the wallet provider 116.

The service provider 114 then generates a token for the selected payment card. The token is preferably generated using the real payment credentials, and preferably, but not necessarily, has the format of payment card credentials (e.g. it too is a 16 digit number). It preferably also encodes the identity of the merchant. The token may be regarded an alternative payment credential linked to the original (i.e. real) payment credential transmitted by the wallet provider 116. The token may be a hexadecimal number or may mimic an ISO (independent sales organization) based card number. It may be generated by any conventional method, or for example, as described in U.S. Patent Application No. 14/514,290. It may subsequently be encrypted.

In step 5, the service provider 114 sends the token to the merchant server 112.

In step 6, the merchant server 112 sends the consumer application 111 a message saying that the merchant server 112 has received a token. The token is retained in the merchant server 112.

In step 7, the consumer initiates the purchase, rental or hire of a particular item (product and/or service). For example, if the consumer has ordered or been given a certain food and/or beverage, the consumer indicates that he or she wants to pay the bill for them. The consumer controls the consumer application 111 to send a message to the merchant server 112 specifying the item to be bought,

In step 8 the merchant server 112 sends the merchant application 113 a message indicating that the consumer wants to make the purchase.

In step 9 the merchant application 113 sends the merchant server 112 a message which includes the amount of the transaction ("the final transaction amount"). For example, depending upon the nature of the merchant, this might be the total (including taxes) restaurant or café bill, taxi fare, etc.

In step 10, the merchant server 112 sends the consumer's token for the selected payment card, and the final transaction amount obtained in step 9, to the service provider 114, as a transaction authorization request.

In step 11, the service provider 114 decrypts the token received in the transaction authorization request (if it was encrypted), and performs a de-tokenization operation on the token, to retrieve the (real) payment credentials which the service provider 114 received in step 4. Detokenization means that the service provider 114 converts the token obtained from the merchant server 112 to the real payment credentials (funding PAN), such as by looking the token up in a mapping table. The service provider 114 sends the real payment credentials to the acquiring bank 115. Then, according to the same steps as the prior art the bank 115 obtains authorization from the issuer of the payment card ("issuing bank") for a payment of the final transaction amount via the payment network. The payment settlement and reconciliation will subsequently be carried out, according to a conventional protocol.

In step 12, the bank sends an authorization response to the service provider 114, indicating that the payment has been approved.

In step 13, the service provider 114 forwards the authorization response to the merchant server 112.

In step 14, the merchant server 112 notifies the consumer application 111 that the payment has been authorized. In step 15, the merchant server 112 notifies the merchant application 113 that the payment has been authorized. Note that steps 14 and 15 may alternately be performed in the opposite order or simultaneously.

Note that during this process the real payment credentials are only sent to the (secure) service provider 114, not to the (insecure) merchant server 112. Furthermore, the service provider 114 may store the payment credentials only for the time taken to generate the token, after which they can be deleted; the service provider regenerates the payment credentials in step 11.

The service provider 114 will only perform step 11 if it receives the token from the same merchant whose identity was used to generate the token. Thus, the token can only be used to make a payment using the merchant server 112. Therefore, if the token is stolen, the thief will not be able to use it to make a payment to another merchant.

Furthermore, the service provider 114 will preferably only accept a given token once. That is, when it receives the transaction authorization request, it checks that it has not previously received the token it contains, and only completes step 11 in the case that this check is positive. This means that after the transaction is completed, a thief who obtains it will not be able to use the token to make a subsequent payment via the merchant server 112. When the

consumer wants to make a further transaction using the merchant 112, the entire process of Figs. 3 and 4 must be repeated, including generating a new token. This new token will be different from the old token. For example, it may be generated using a clock time from a reference clock (e.g. maintained at the service provider 114) or counter associated with the wallet, so that differing instances of generated tokens generated are different.

Variants of the embodiment

Many embodiments are possible within the scope and spirit of the invention as will be clear to a skilled reader.

Firstly, although the embodiment shown in Fig. 2 includes both a merchant server 112 (MS) and also a separate merchant application 113 (MA) running on equipment at a point-of-sale, in certain embodiments of the invention there is no separate merchant application at a point-of-sale. Instead, the merchant server itself may be capable of fulfilling the purchase, either by performing a service (such as making a travel booking) or fulfilling a product purchase product (e.g. by dispatching the purchased product to the consumer, or by sending an order to a separate warehouse to do so). In this case, steps 8, 9 and 15 of Figs. 3 and 4 are omitted.

Secondly, the token need not necessarily encode the (real) payment credentials. Instead, the service provider 114 could issue tokens which are generated using a random or unpredictable number generator. The service provider 114 might keep a database which, for each token it has issued, contains the corresponding payment credentials, so that when the service provider receives a token, it can extract the payment credentials from its database. Alternatively, the service provider 114 might keep a database which, for each token it has issued, indicates the identity of the corresponding consumer, so that the service provider 114 can obtain the payment credentials again from the wallet provider 116.

Thirdly, in principle the operations of the wallet provider 116 and the service provider 114 could be performed by a single server (so that the messages of steps 3 and 4 are unnecessary). This variation would, for example, be appropriate if the card issuing bank happens to be the same as the acquiring bank 113.

Fourthly, although Figs. 2 and 3 refer to a single merchant server 112 and a single service provider server 114, in some embodiments either of these roles may be implemented using multiple servers which cooperate together to play the role. Thus, for example, a merchant may maintain multiple servers, e.g. distant from each other, which cooperate to present a consumer website to consumers.

Claims

1. A method of securing a payment to a merchant using a payment card which has been registered with a database and which is associated with a consumer, the database containing payment credentials for the payment card, the method comprising the operations of:

(a) a merchant server associated with the merchant receiving from the consumer an instruction that a payment card registered with the database is to be used for the payment;

(b) the merchant server transmitting to a service provider a message indicating that a payment transaction is to be made;

(c) the service provider at a processor (i) obtaining the payment credentials of the payment card from the database, (ii) generating a token, and (iii) transmitting the token to the merchant server;

(d) the merchant server obtaining a transaction account, and transmitting to the service provider a transaction authorization request comprising the transaction amount and the token; and

(e) the service provider, at a processor, upon receiving the transaction authorization request, obtaining authorization for a transaction of the transaction amount from an issuer server, and sending a message to the merchant server indicating that the authorization has been received.

2. A method according to claim 1 in which, in operation (c), the processor of the service provider generates the token using the identity of the merchant server, the service provider verifying in operation (e) that the transaction authorization request the service provider receives in operation (d) is from the same merchant server.

3. A method according to claim 1 or claim 2 in which the database is maintained by a wallet provider operated by the issuing bank of the payment card, and the service provider is operated by a bank at which the merchant maintains an account.

4. A method according to claim 3 in which the service provider obtains the payment credentials by submitting a request to the wallet provider, whereupon the wallet provider interacts with the consumer to confirm the identity of the consumer, and upon confirming the identity of the user, transmits the payment credentials for the payment card to the service provider.

5. A method according to any preceding claim, in which in operation (c) the processor of the service provider generates the token using the payment credentials of the payment card, and upon receiving the token from the merchant server in operation (d) the processor of the service provider regenerates the payment credentials from the token.

6. A method according to any preceding claim, in which the merchant server is in communication with one or more merchant applications running at one or more corresponding points-of-sale distant from the server, and

following step (e) the merchant server transmits to the merchant application at one of the points-of-sale a message indicating that the payment is approved, the consumer receiving, in response to the payment, a product or a service at the said point-of-sale.

7. A method according to any preceding claim in which, upon receiving the transaction authorization request, the processor of the service provider checks that it has not previously received a transaction authorization request containing the same token, operation (e) only being performed in the case that the check has a positive result.

8. A service provider server for securing a payment to a merchant using a payment card which has been registered with a database and which is associated with a consumer, the database containing payment credentials for the payment card, the server being in communication with a merchant server operated by the merchant, and including a processor arranged:

to receive from the merchant server a message indicating that a payment transaction is to be made;

to obtain the payment credentials of the payment card from the database;

to generate a token;

to transmit the token to the merchant server;

to receive from the merchant server a transaction authorization request comprising the transaction amount and the token;

to obtain authorization for a transaction of the transaction amount from a server of an issuer associated with the payment card; and

to send a message to the merchant server indicating that the authorization has been received.

9. A service provider server according to claim 8 in which the processor is arranged to generate the token using the identity of the merchant server, and

upon receiving the transaction authorization request from the merchant server, to verify that the token it contains is from the same merchant server.

10. A service provider server according to claim 8 or claim 9, in which the processor is arranged to generate the token using the payment credentials of the payment card, and

upon receiving the token from the merchant server, to regenerate the payment credentials from the token.

11. A service provider server according any of claims 8 to 10, in which the processor is arranged:

upon receiving the transaction authorization request, to check that the service provider server has not previously received a transaction authorization request containing the same token, and

only to obtain authorization for the transaction in the case that the check has a positive result.

12. A service provider according to any of claims 8 to 11, in which the processor is arranged to encrypt the token before passing it to the merchant server, and upon receiving it from the merchant server to decrypt it.

13. A method for securing a payment to a merchant using a payment card which has been registered with a database and which is associated with a consumer, the database containing payment credentials for the payment card, the method comprising the operations of a processor of a service provider:

receiving from a merchant server operated by the merchant a message indicating that a payment transaction is to be made;

obtaining the payment credentials of the payment card from the database;

generating a token;

transmitting the token to the merchant server;

receiving from the merchant server a transaction authorization request comprising the transaction amount and the token;

obtaining authorization for a transaction of the transaction amount; and

sending a message to the merchant server indicating that the authorization has been received.

14. A method according to claim 13 in which the processor generates the token using the identity of the merchant server, and

upon receiving the transaction authorization request from the merchant server, verifies that the token it contains is from the same merchant server.

15. A method according to claim 13 or claim 14 in which the processor generates the token using the payment credentials of the payment card, and

upon receiving the token from the merchant server, regenerates the payment credentials from the token.

16. A method according to any of claims 13 to 15 in which the processor encrypts the token before transmitting it to the merchant server, and decrypts the token upon receiving it from the merchant server.

17. A method according any of claims 13 to 16, in which the processor:

upon receiving the transaction authorization request, checks that the service provider server has not previously received a transaction authorization request containing the same token, and

only obtains authorization for the transaction in the case that the check has a positive result.

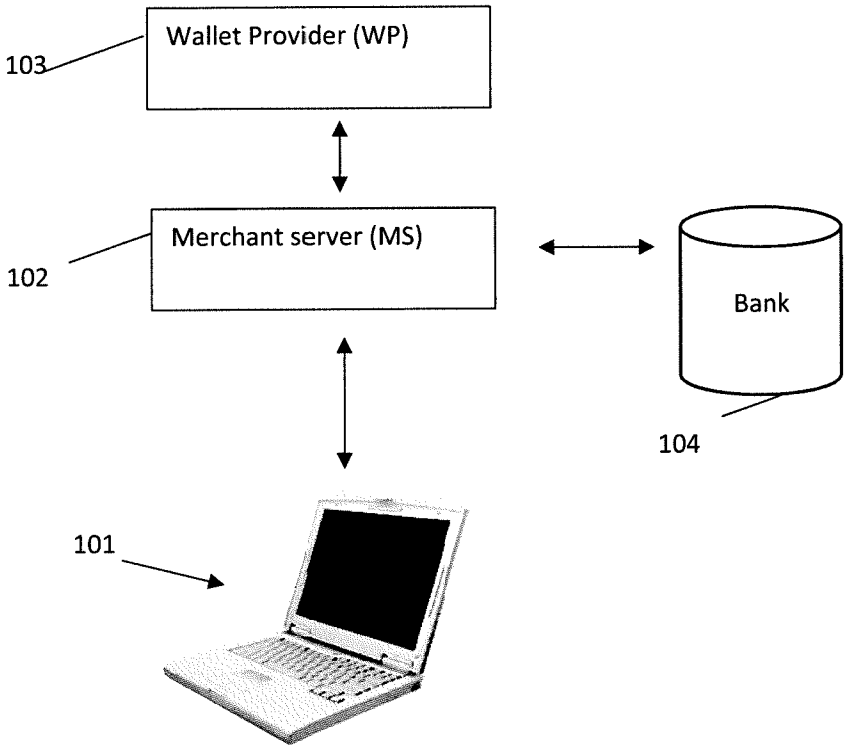

Fig. 1

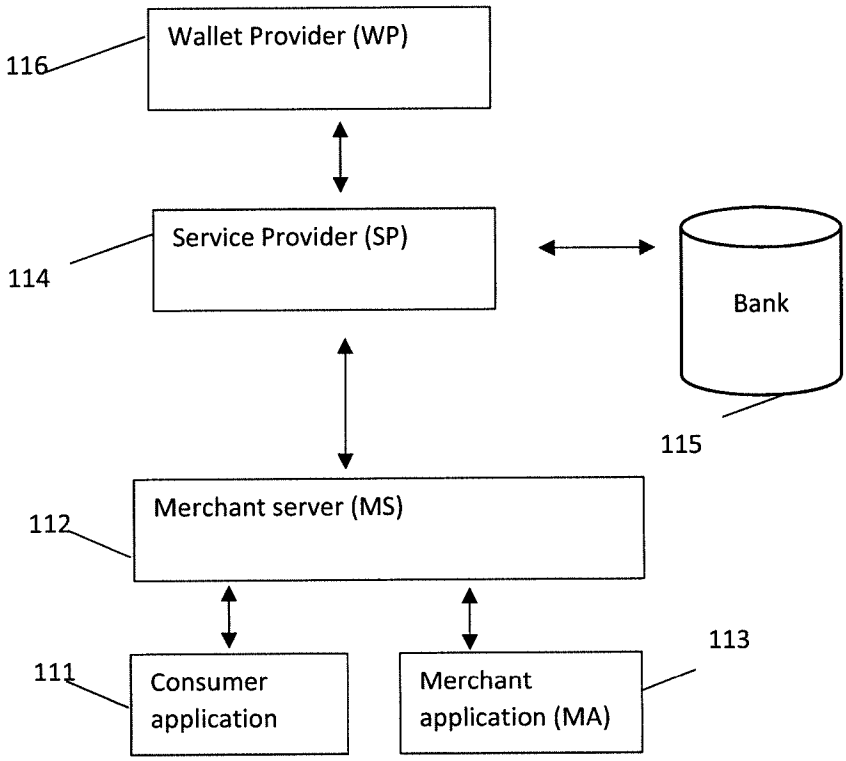
Wallet Provider (WP)
116
Service Provider (SP)
114
Bank
115
Merchant server (MS)
112
Consumer application
111
Merchant application (MA)
113

Fig. 2

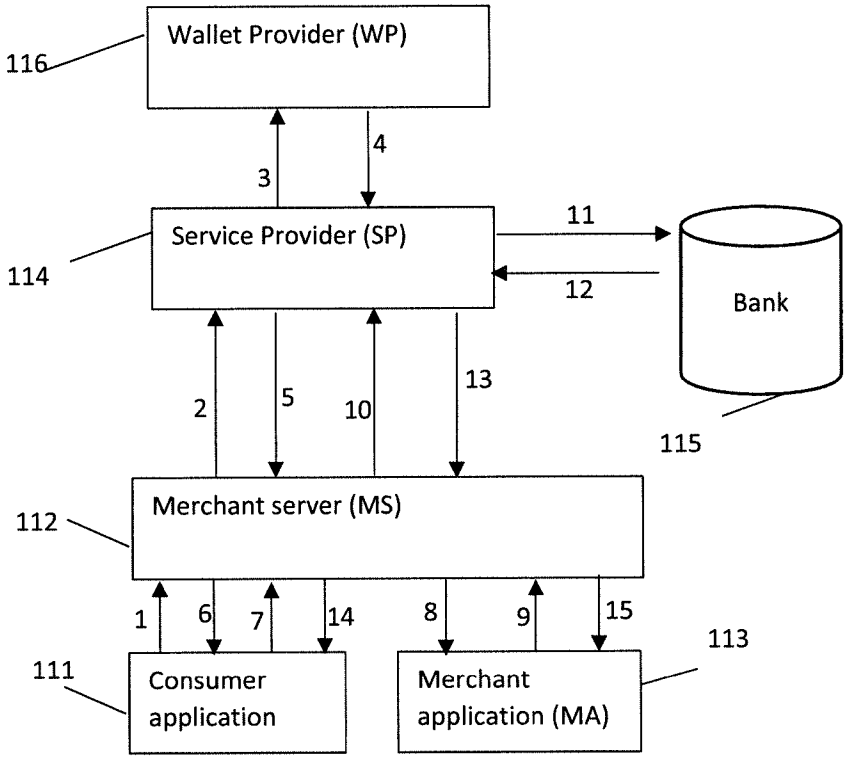
Wallet Provider (WP)
116
3
4
Service Provider (SP)
114
11
12
Bank
115
2
5
10
13
Merchant server (MS)
112
1
6
7
14
8
9
15
113
111
Consumer application
Merchant application (MA)

Fig. 3

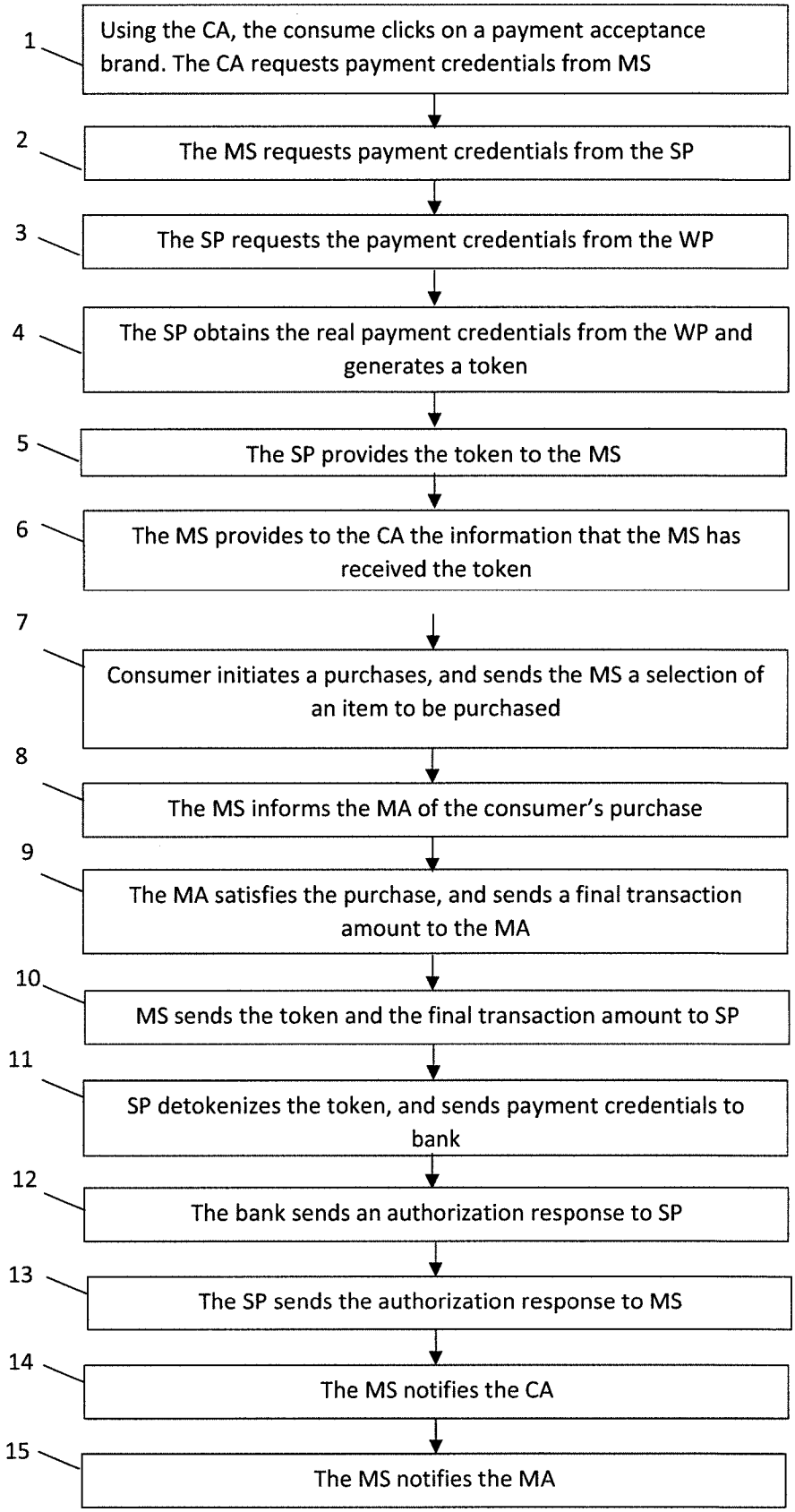
1
Using the CA, the consume clicks on a payment acceptance brand. The CA requests payment credentials from MS
2
The MS requests payment credentials from the SP
3
The SP requests the payment credentials from the WP
4
The SP obtains the real payment credentials from the WP and generates a token
5
The SP provides the token to the MS
6
The MS provides to the CA the information that the MS has received the token
7
Consumer initiates a purchases, and sends the MS a selection of an item to be purchased
8
The MS informs the MA of the consumer's purchase
9
The MA satisfies the purchase, and sends a final transaction amount to the MA
10
MS sends the token and the final transaction amount to SP
11
SP detokenizes the token, and sends payment credentials to bank
12
The bank sends an authorization response to SP
13
The SP sends the authorization response to MS
14
The MS notifies the CA
15
The MS notifies the MA

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050014

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06Q20/22(2012.01)i, G06Q20/24(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)

Int.Cl. G06Q20/22, G06Q20/24

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2016
Registered utility model specifications of Japan 1996-2016
Published registered utility model applications of Japan 1994-2016

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2011-209861 A (FUJITSU FRONTECH LIMITED) 2011.10.20, the whole document (Family:none)	1-17
A	EP 1028401 A2 (CITIBANK,N.A.) 2000.08.16, paragraph [0028] & JP 2000-322486 A & CN 1266240 A	1-17
A	JP 2004-94619 A (DAI NIPPON PRINTING CO., LTD.) 2004.03.25, the whole document (Family:none)	1-17
A	JP 2008-152338 A (HITACHI SOFTWARE ENGINEERING CO., LTD.) 2008.07.03, the whole document (Family:none)	1-17

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
04.04.2016	12.04.2016

Name and mailing address of the ISA/JP	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	SATO, Yuko Telephone No. +81-3-3581-1101 Ext. 3562

5L 3787

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050014

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-24716 A (JUKI KK) 2002.01.25, the whole document (Family:none)	1-17
A	EP 1400906 A1 (SONY CORPORATION) 2004.03.24, the whole document & JP 2002-366868 A & US 2004/0059682 A1 & WO 2002/101614 A1 & CN 1465026 A	1-17
A	US 2005/0154643 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2005.07.14, the whole document (Family:none)	1-17
A	US 5883810 A (MICROSOFT CORPORATION) 1999.03.16, the whole document (Family:none)	1-17