A PAYMENT TRANSACTION SYSTEM FOR PROCESSING A TOKENIZED TRANSACTION OVER A DOMESTIC SWITCH

Field of the Invention

The present invention relates to payment transaction system and method for processing a tokenized transaction.

Background of the Invention

Debit card transactions are typically facilitated by an entity which operates domestically, i.e. only within a particular country or region, such as NETS in Singapore, MEPS in Malaysia and EFTPOS in Australia and New Zealand. These domestic entities are referred to as domestic switches.

In some jurisdictions, access to the domestic switch's network is highly regulated by local government bodies. As such, third party entities are typically not involved in processing these transactions, whether switching or clearing services. In this regard, domestic switches perform processes relating to the transaction in-house thereby bearing the risks involved with fraudulent transactions. This results in a slower uptake in the deployment of newer technology for such transactions.

With the advent of smartphones and wearable devices, consumers have taken to using digital wallets to pay for their purchases. Digital wallets often use tokenisation as a means of securely processing payment transactions. Additionally, digital wallet payments can offer additional security by means of biometric authentication, for example finger print verification via a fingerprint sensor on the consumer's smartphone.

However, digital switch payment systems typically do not support tokenisation and as such, are not capable of processing payments made using digital wallet systems.

It is generally desirable to overcome or ameliorate one or more of the above described difficulties, or to at least provide a useful alternative.

Summary of the Invention

In accordance with the present invention, there is provided a payment transaction system for processing a tokenized transaction, the payment transaction system comprising a payment network server having one or more processors in communication with a non-transitory data storage medium having instructions stored thereon that, when executed by the one or more processors, configure the one or more processors to perform the steps of:

(a) receiving a transaction authorization request from a domestic switch, the transaction authorization request including a token and transaction information, the token being received by the domestic switch from a merchant, wherein the token is associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) performing de-tokenization on the token to identify the payment account credentials; and

(c) sending the payment account credentials to the domestic switch to facilitate authorization of the transaction by an issuer of the payment account.

In accordance with the present invention, there is also provided a payment transaction system for processing a tokenized transaction, the payment transaction system comprising:

a payment network server;

a domestic switch for sending an authorization request to the payment network server; and

the domestic switch and payment network server together comprising one or more processors in communication with a non-transitory data storage medium having instructions stored thereon which, when executed by the one or more processors, configure the payment transaction system to perform the steps of:

(a) receiving, at the domestic switch, a transaction authorization request from a request system, the transaction authorization request including a token received from a merchant, the token being associated with

payment account credentials of a payment account for use in the tokenized transaction;

(b) identifying, at the domestic switch, a payment account and issuer associated with the token;

(c) sending the transaction authorization request, from the domestic switch to the payment network server, the transaction authorization request including the token;

(d) performing, at the payment network server, de-tokenization on the token to identify the payment account credentials;

(e) sending the payment account credentials, from the payment network server to the domestic switch, to facilitate authorization of the transaction;

(f) responsive to receipt of the payment account credentials, at the domestic switch, determining if the transaction authorization request is approved; and

(g) responsive to a determination that the transaction authorization request is approved, at the domestic switch, sending message data indicating that the transaction authorization request is approved to the request system.

In accordance with the present invention, there is also provided a method for processing a tokenized transaction, the method being performed by a payment transaction system and comprising:

(a) receiving a transaction authorization request, from a domestic switch, the transaction authorization request including a token and transaction information, the token being received by the domestic switch, from a merchant, wherein the token is associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) performing de-tokenization on the token to identify the payment account credentials; and

(c) sending the payment account credentials to the domestic switch to facilitate authorization of the transaction by an issuer of the payment account.

In accordance with the present invention, there is also provided a method for processing a tokenized transaction, the method performed by a payment transaction system comprising:

a payment network server;

a domestic switch for sending an authorization request to the payment network server; and

the domestic switch and payment network system together comprising one or more processors in communication with a non-transitory data storage medium having instructions stored thereon which, when executed by the one or more processors, configure the payment transaction system to perform the steps of:

(a) receiving, at the domestic switch, a transaction authorization request from a request system, the transaction authorization request including a token received from a merchant, the token being associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) identifying, at the domestic switch, a payment account and issuer associated with the token;

(c) sending the transaction authorization request, from the domestic switch to the payment network server, the transaction authorization request including the token;

(d) performing, at the payment network server, de-tokenization on the token to identify the payment account credentials;

(e) sending the payment account credentials from the payment network server to the domestic switch to facilitate authorization of the transaction;

(f) responsive to receipt of the payment account, at the domestic switch, determining if the transaction authorization request is approved; and

(g) responsive to a determination that the transaction authorization request is approved, at the domestic switch, sending message data indicating that the transaction authorization request is approved to the request system.

Brief Description of the Drawings

Preferred embodiments of the invention are hereafter described, by way of non-limiting example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a system for processing a tokenized transaction;
Figure 2 is a flowchart diagram showing the interoperation of the components of the embodiments of the system for onboarding a payment card;
Figure 3 is a flowchart diagram showing the interoperation of the components of the embodiment of the system for use in processing a tokenized transaction;
Figure 4 is a block diagram of an example mobile computing device of the system shown in Figure 1; and
Figure 5 is a schematic diagram showing components of an example computing device.

Detailed Description of Embodiments of the Invention

Figure 1 shows a payment transaction system 10. The system 10 allows a digital wallet to be used to make a payment over a payment network that includes a domestic switch.

Rather than using the credentials of a payment account (e.g. the debit, pre-paid or other non-credit card number, PAN, expiry date, card verification value and so forth, or a corresponding debit, pre-paid or other card, or bank account), a digital wallet may use a tokenized version of those credentials (i.e. a token) to make a payment. The system 10 consequently provides a payment system that is capable of processing transactions made using digital wallet, and processed by a domestic switch, in a business as usual fashion without substantial changes being made to at the domestic switch.

The system 10 includes one or more of the following:

(a) mobile computing device 12;
(b) merchant terminal 14;
(c) payment gateway 14b;

(d) digital wallet system 16;
(e) acquirer 18a;
(f) domestic switch 18b;
(g) issuer 18c;
(h) communication network 20; and
(i) payment network server 22.

The components of system 10 are in communication as particularly shown in Figure 1, for example, via the network 20. The communication network 20 may include the Internet, telecommunications networks and/or local area networks.

The system 10 enables digital wallet transactions, which may also be referred to as tokenized transactions, to be processed over domestic switch payment systems. Typically, domestic switch payment systems do not support tokenized transactions and as such, are not able to process digital wallet transactions on the domestic switch payment network. The payment network server 22 provides tokenization functionality and operates in conjunction with the domestic switch 18b, thereby allowing the digital wallet transaction to be processed.

Onboarding Process 400

To use a payment card using a digital wallet, a cardholder would need to onboard his or her payment card on a digital wallet system 16. This may be performed by means of the digital wallet application 218 being executed on the cardholder's mobile device 12. The digital wallet application 218 can then be used in payment transactions in lieu of the payment card. In such a digital wallet system, the PAN of the payment card is tokenised – in other words a token is generated for use in place of the PAN to reduce the likelihood of fraud.

An exemplary onboarding process 400 is shown in Figure 2. At step 402, the digital wallet application 218 executed on a cardholder's mobile device 12 receives cardholder's request to onboard a payment card. The request includes the cardholder's payment credentials such as the PAN of the payment card. The digital wallet application 218 then generates and sends message data including the request to a digital wallet system 16. At step 404, the digital wallet system 16 receives the

message data and sends it to a third party processor system 22.

At step 406, the third party processor system 22 receives the message data including the cardholder's payment credentials. At step 408, the third party processor system 22 extracts a Bank Identification Number (BIN) from the PAN and makes a determination if the BIN is registered on database 316.

At step 410, the third party processor system 22 appends a unique wallet ID, which is an identifier for digital wallet providers such as ApplePay™ that subscribe to a tokenization service, to the payment credentials, the PAN for example. At step 412, the payment network server 22 sends a tokenisation request including payment credentials, appended wallet ID from step 410 to the domestic switch 18b.

At step 414, the domestic switch 18b receives the tokenisation request and checks if the request includes a wallet ID. Responsive to a determination that the request includes a wallet ID, step 416 is executed whereby the domestic switch 18b generates a request for tokenisation approval and sends it to the issuer 18c.

At step 418, the issuer 18c receives the tokenisation request and makes a determination if the tokenisation is to be approved. In response to the determination that the tokenisation is approved, the issuer 18c sends message data to the domestic switch 18b.

At step 420, the domestic switch 18b receives the approval for tokenisation. The domestic switch 18b then sends message data to the third party processor system 22 indicating the approval. At step 422, the tokenisation platform of the third party processor system 22 generates a personalization script including a token and corresponding keys based on the payment credentials e.g. PAN. The third party processor system 22 stores the generated token and keys in database 316. The third party processor system 22 then generates message data including the token to the digital wallet system 16.

At step 424, the digital wallet system 16 receives the token. At step 426, the digital wallet 16 receives personalization script and personalises the token for the mobile device 12.

At step 428, the digital wallet app 218 executed on the mobile device 12 receives and stores the token from the digital wallet system 16. At step 430, the digital wallet app 218 generates on display 202 of the mobile device 12 "Request approved" or similar indication that the onboarding process has been successful.

The process 400 provisions a token to the mobile device 12 allowing a cardholder to use the digital wallet app 218 executed on the mobile device 12 to affect transactions using his or her payment card associated with the token.

In this embodiment, the domestic switch 18b typically cannot process transactions where a token has been provided in place of account credentials (e.g. an account number of an account from which funds can be debited to settle a transaction). The domestic switch 18b cannot, for example, perform de-tokenisation of a token. This prevents cardholders from using a digital wallet for making a transaction over the domestic switch 18b.

Transaction Approval Process 500

The transaction approval process 500 enables a transaction originating from a mobile computing device 12, for example, to be authorized by an issuer 18c. To perform a transaction using a tokenized payment card, which has been onboarded with process 400, a cardholder uses a digital wallet application 218 executed on mobile device 12 to initiate a payment.

The payment may be initiated for an online transaction. For example, an in app payment where card transactions are performed using a merchant mobile app which interfaces with a digital wallet app 218 for payments. In this example, a token associated with digital wallet account credentials is sent from the digital wallet app 218 to the merchant app, or through a web browser operating on the mobile computing device 12, and forwarded to a payment gateway 14b together with the merchant ID (MID).

The payment may also be initiated at a merchant's terminal 14 such as at a cashier in a retail store. Initiation of payment may occur, for example, after a basket has been

generated at the merchant terminal – e.g. one or more products have been scanned using a barcode reader and the basket thus comprises the one or more products.

To initiate payment, the merchant terminal 14 interfaces with the mobile device 12 via a reader such as a NFC reader. At step 502, the mobile computing device 12 transmits a token associated with payment account credentials of a payment account to the merchant terminal via an interface as above-described. At step 504, the merchant terminal receives the token from the mobile computing device 12 and generates a transaction request. The transaction request includes merchant identifier (ID) and transaction information, for example transaction amount, transaction identifier such as a receipt number and so forth. The transaction request is sent to a request server such as an acquirer 18a.

At step 506, the acquirer 18a receives the transaction request including the token and transaction information. The acquirer 18a sends the request to the domestic switch 18b. At step 510, the domestic switch 18b identifies the payment network server 22 associated with the transaction information, for example by comparing the BIN against a BIN range (e.g. first 6 digits of the token) to identify if the BIN corresponds with a token issued by the tokenisation platform of the payment network server 22.

The domestic switch 18b sends the authorization request to the payment network server 22. At step 512, the payment network server 22 receives the authorization request including the token and transaction information. Transaction information includes one or more of the following:

(a) merchant specific information, e.g. Merchant Category Code;
(b) token;
(c) currency;
(d) amount; and
(e) cryptogram.

At step 514, the payment network server 22 performs de-tokenization on the token to identify the payment account credentials. In some embodiments, de-tokenization involves the payment network server 22 further performing the step of retrieving, from data storage, the payment account credentials associated with the token. The

payment network server 22 may also perform cryptogram validation to further evaluate the transaction, as part of the authentication request.

The results from the de-tokenization and authentication process are sent to the domestic switch 18b to facilitate authorization of the transaction request. The results may include payment account credentials and at least part of the transaction information. Payment account credentials associated with the token may include digital wallet credentials or cardholder credentials such as a PAN, including the identity of the issuer 18c. In the case of digital wallet credentials, a further step of retrieving payment account credentials from a digital wallet system associated with the digital wallet account would be required.

At step 516, the domestic switch 18b receives the results and makes a determination if the transaction has been authenticated. If the transaction has been authenticated, the domestic switch 18b sends the authorization request at step 518 comprising the payment account credentials to the issuer 18c. At step 520, the issuer 18c, then makes a determination if the authorization request is to be approved based on the transaction information.

Responsive to a determination that the authorization request is approved, the issuer 18c sends message data to the domestic switch 18b indicating status of the authorization request, e.g. transaction approval. At step 522, the domestic switch 18b receives transaction approval from issuer 18c. The domestic switch 18b sends transaction approval message to one or both of the payment network server 22 and the merchant terminal 14. At step 524, the payment network server 22 receives message data indicating approval of the transaction and sends message data to the mobile device 12 associated with a user that the transaction authorization request has been approved.

Alternatively, responsive to a determination that the authorization request is declined, message data is sent to one or both of the payment network server 22 and the merchant terminal 14. The payment network server 22 receives message data indicating declination of the transaction and sends message data to a mobile device 12 associated with a user that the transaction authorization request has been declined.

At step 526, the mobile device 12 receives message data indicating transaction approval. At step 528, the mobile device 12 generates a transaction approval message on display 202 to evidence approval of the transaction – e.g. "Transaction approved".

At step 532, the merchant terminal 14 receives message data indicating transaction approval. At step 534, the merchant terminal 14 displays a similar transaction approval message on display 202.

Mobile Computing Device 12

Figure 4 is a block diagram showing an exemplary mobile computing device 12 in which embodiments of the invention may be practiced. The mobile computing device 12 may be a mobile computing device such as a smart phone, a personal data assistant (**PDA**), a palm-top computer, and multimedia Internet enabled cellular telephones. For ease of description, the mobile computing device 12 is described below, by way of non-limiting example, with reference to a mobile device in the form of an iPhone ™ manufactured by Apple™, Inc., or one manufactured by LG™, HTC™ and Samsung™, for example.

As shown, the mobile computing device 12 includes the following components in electronic communication via a bus 206:

(a) a display 202;
(b) non-volatile (non-transitory) memory 204;
(c) random access memory ("RAM") 208;
(d) N processing components 210;
(e) a transceiver component 212 that includes N transceivers; and
(f) user controls 214.

Although the components depicted in Figure 4 represent physical components, Figure 4 is not intended to be a hardware diagram. Thus, many of the components depicted in Figure 4 may be realized by common constructs or distributed among additional physical components. Moreover, it is certainly contemplated that other existing and yet-to-be developed physical components and architectures may be utilized to

implement the functional components described with reference to Figure 4.

The display 202 generally operates to provide a presentation of content to a user, and may be realized by any of a variety of displays (e.g., CRT, LCD, HDMI, micro-projector and OLED displays).

In general, the non-volatile data storage 204 (also referred to as non-volatile memory) functions to store (e.g., persistently store) data and executable code.

In some embodiments for example, the non-volatile memory 204 includes bootloader code, modem software, operating system code, file system code, and code to facilitate the implementation components, well known to those of ordinary skill in the art, which are not depicted nor described for simplicity.

In many implementations, the non-volatile memory 204 is realized by flash memory (e.g., NAND or ONENAND memory), but it is certainly contemplated that other memory types may be utilized as well. Although it may be possible to execute the code from the non-volatile memory 204, the executable code in the non-volatile memory 204 is typically loaded into RAM 208 and executed by one or more of the N processing components 210.

The N processing components 210 in connection with RAM 208 generally operate to execute the instructions stored in non-volatile memory 204. As one of ordinarily skill in the art will appreciate, the N processing components 210 may include a video processor, modem processor, DSP, graphics processing unit (GPU), and other processing components.

The transceiver component 212 includes N transceiver chains, which may be used for communicating with external devices via wireless networks. Each of the N transceiver chains may represent a transceiver associated with a particular communication scheme. For example, each transceiver may correspond to protocols that are specific to local area networks, cellular networks (e.g., a CDMA network, a GPRS network, a UMTS networks), and other types of communication networks.

The mobile computing device 12 can execute mobile applications. The digital wallet

application 218 could be a mobile application, web page application, or computer application. The digital wallet application 218 may be accessed by a computing device such as mobile computing device 12, computing device 300, payment token or wearable devices such as a smartwatch. The digital wallet application 218 can be used with payment cards including credit cards, debit cards, store cards, etc. For ease of description, the digital wallet application 218 is described by way of reference to credit cards only. However, the digital wallet application 218 and the system 10 can be used with any suitable payment card.

The transceiver component 212 is also adapted to effect contactless payments. For example, the transceiver component 212 is able to effect contactless payment using Near-Field Communications (NFC) according to the EMV (Europay, MasterCard, Visa) standard. Digital payment methods based on the EMV standard may include Apple Pay™, MasterPass™, or SamsungPay® for example, each of which employs a virtual wallet. Digital payments may also be made on online transactions.

It should be recognized that Figure 4 is merely exemplary and in one or more exemplary embodiments, the functions described herein may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be transmitted or stored as one or more instructions or code encoded on a non-transitory computer-readable medium 204. Non-transitory computer-readable medium 204 includes both computer storage medium and communication medium including any medium that facilitates transfer of a computer program from one place to another. A storage medium may be any available medium that can be accessed by a computer.

Computing Device 300

The payment network server 22 may be operated by a payment network company (such as Mastercard, Visa or China UnionPay).

Figure 5 shows an example computing device 300 that is capable of implementing the payment network server 22 and other components of the system 10. In some embodiments, each of the component of the system 10 may comprise multiple servers in communication with each other, for example over a local area network or a wide-

area network such as the Internet. As described in the preceding section, the payment network server 22 is able to communicate with other components of the system 10 (e.g. mobile computing device 12, digital wallet system 16, and domestic switch 18b) over the wireless communications network 20 using standard communication protocols.

The components of the computing device 300 can be configured in a variety of ways. The components can be implemented entirely by software to be executed on standard computer server hardware, which may comprise one hardware unit or different computer hardware units distributed over various locations, some of which may require the communications network 20 for communication. A number of the components or parts thereof may also be implemented by application specific integrated circuits (ASICs) or field programmable gate arrays.

In the example shown in Figure 5, the computing device 300 is a commercially available server computer system based on a 32 bit or a 64 bit Intel architecture, and the processes and/or methods executed or performed by the computing device 300 are implemented in the form of programming instructions of one or more software components or modules 322 stored on non-volatile (e.g., hard disk) computer-readable storage 324 associated with the computing device 300. At least parts of the software modules 322 could alternatively be implemented as one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) and/or field programmable gate arrays (FPGAs).

The computing device 300 includes at least one or more of the following standard, commercially available, computer components, all interconnected by a bus 335:

(a) random access memory (RAM) 326;

(b) at least one computer processor 328, and

(c) external computer interfaces 330:

(i) universal serial bus (USB) interfaces 330a (at least one of which is connected to one or more user-interface devices, such as a keyboard, a pointing device (e.g., a mouse 332 or touchpad),

(ii) a network interface connector (NIC) 330b which connects the computing device 300 to a data communications network, such

as the wireless communications network 20; and

(iii) a display adapter 330c, which is connected to a display device 334 such as a liquid-crystal display (LCD) panel device.

The computing device 300 includes a plurality of standard software modules, including:

(a) an operating system (OS) 336 (e.g., Linux or Microsoft Windows);

(b) web server software 338 (e.g., Apache, available at http://www.apache.org);

(c) scripting language modules 340 (e.g., personal home page or PHP, available at http://www.php.net, or Microsoft ASP); and

(d) structured query language (SQL) modules 342 (e.g., MySQL, available from http://www.mysql.com), which allow data to be stored in and retrieved/accessed from an SQL database 316.

Advantageously, the database 316 forms part of the computer readable data storage 324. Alternatively, the database 316 is located remote from the server 14 shown in Figure 5.

Together, the web server 338, scripting language 340, and SQL modules 342 provide the computing device 300 with the general ability to allow the other components of the system 10 to communicate with the system 300 and in particular to provide data to and receive data from the database 316. It will be understood by those skilled in the art that the specific functionality provided by the computing device 300 to such users is provided by scripts accessible by the web server 338, including the one or more software modules 322 implementing the processes performed by the computing device 300, and also any other scripts and supporting data 344, including markup language (e.g., HTML, XML) scripts, PHP (or ASP), and/or CGI scripts, image files, style sheets, and the like.

The boundaries between the modules and components in the software modules 322 are exemplary, and alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into submodules to be executed as multiple

computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may combine multiple instances of a particular module or submodule. Furthermore, the operations may be combined or the functionality of the operations may be distributed in additional operations in accordance with the invention. Alternatively, such actions may be embodied in the structure of circuitry that implements such functionality, such as the micro-code of a complex instruction set computer (CISC), firmware programmed into programmable or erasable/programmable devices, the configuration of a field-programmable gate array (FPGA), the design of a gate array or full-custom application-specific integrated circuit (ASIC), or the like.

Each of the blocks of the flow diagrams of the processes of the computing device 300 may be executed by a module (of software modules 322) or a portion of a module. The processes may be embodied in a non-transient machine-readable and/or computer-readable medium for configuring a computer system to execute the method. The software modules may be stored within and/or transmitted to a computer system memory to configure the computer system to perform the functions of the module.

The computing device 300 normally processes information according to a program (a list of internally stored instructions such as a particular application program and/or an operating system) and produces resultant output information via input/output (I/O) devices 330. A computer process typically includes an executing (running) program or portion of a program, current program values and state information, and the resources used by the operating system to manage the execution of the process. A parent process may spawn other, child processes to help perform the overall functionality of the parent process. Because the parent process specifically spawns the child processes to perform a portion of the overall functionality of the parent process, the functions performed by child processes (and grandchild processes, etc.) may sometimes be described as being performed by the parent process.

The payment transaction system 10 may comprise an acquirer system 18a, an issuer system 18c, and a domestic switch system 18b (such as NETS).

In some embodiments, the payment transaction system 10 further includes or is in communication with a payment network server 22, a merchant terminal 14 or a

payment gateway 14b. The entities of the system 10 are able to communicate through standard communication protocols provided for by communications network 20, in order to receive requests for payment authorization, process such requests, and convey responses back to the requestor.

In a conventional four party payment system, a payment authorization request for a credit card transaction is requested by a merchant terminal 14, for example, and sent to the acquirer 18a, which is forwarded to a payment network server 22 and finally routed to an issuer 18c for authorization.

For a domestic switch payment system, the transaction authorization request is received by the acquirer system 18a, which routes the authorization request to the domestic switch 18b and to the issuer system 18c in a manner known in the art. The authorization request may be formatted according to the ISO 8583 standard, for example, and may include a primary account number (PAN) of the payment instrument being used for the transaction, a merchant identifier (MID), and an amount of the transaction, as well as other transaction-related information as will be known by those skilled in the art. The issuer system 18c receives the request, applies authorization logic to approve or decline the request, for example by comparing the transaction amount with a transaction limit associated with the cardholder, and sends an authorization response (approve or decline, optionally with a code indicating the reason for the decline) back to the domestic switch 18b and the payment network server 22 in a known fashion.

In some embodiments, the payment authorization request may be received via the issuer system 18c, which approves or declines the request (which again may be in ISO 8583 format, and comprise a PAN, MID, transaction amount etc.) and sends a response directly back to the requestor, e.g. the merchant terminal 14.

The system 10 may also process a pre-authorization (or "pre-auth") request, in which funds are not transferred on approval of the request, but are instead placed on hold. The pre-auth can later be completed, for example by the merchant server, in order to release the funds. Alternatively, the pre-auth can be cancelled, thus effectively cancelling the transaction.

In an embodiment of the invention, the merchant terminal 14 receives a token from a mobile computing device 12, the token associated with payment account credentials of a payment account, such as a credit card or debit card account. The acquirer 18a receives a transaction authorization request including the token from the merchant and sends the request to the domestic switch 18b. The authorization request may also include transaction details and a cryptogram. In this embodiment, the domestic switch 18b is incapable of independently processing the token and as such, forwards a authorization request to the payment network server 22 for de-tokenization to be performed. As known to those who are skilled in the art, de-tokenization refers to the process of substituting a payment account number (also referred to as a primary account number) for a token that represented the payment account number. The payment network server 22 may also verify the cryptogram as part of the authorization request process.

The embodiments of this invention enable tokens to be used in a domestic switch payment system thereby allowing digital wallets to be used to initiate a payment.

Merchant Terminal 14

The merchant's terminal 14 is a payment terminal such as a point of sale terminal or payment card terminal for interfacing with payment cards or mobile device 12 to make electronic funds transfers. The merchant terminal 14 interfaces with payment cards or mobile device 12 by means of a reader such as a magnetic swipe reader, EMV chip reader or near field communication (NFC) contactless communication.

The merchant's terminal 14 may be embodied by a computing device 300 such as that shown in Figure 5. In another embodiment, the merchant's terminal 14 is embodied by a mobile computing device 12 such as one described in Figure 4. In these embodiments, an external interface reader to interface with payment cards or mobile computing device 12 is provided for either by the computing device 300 or mobile computing device 12 or an external hardware reader in communication with the computing device 300 or mobile computing device 12.

The merchant's terminal 14 is in communication with the merchant's point-of-sales system. In some embodiments, the merchant's terminal 14 also provides for the

point-of-sales system.

A payment may also be initiated on behalf of a merchant for an online transaction. In these embodiments, a payment gateway 14b is used to communicate with acquirer 18a to request for a transaction authorization associated with a transaction.

Throughout this specification, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

The reference to any prior art in this specification is not, and should not be taken as, an acknowledgment or any form of suggestion that the prior art forms part of the common general knowledge.

Claims Defining the Invention

1. A payment transaction system for processing a tokenized transaction, the payment transaction system comprising a payment network server having one or more processors in communication with a non-transitory data storage medium having instructions stored thereon that, when executed by the one or more processors, configure the one or more processors to perform the steps of:

(a) receiving a transaction authorization request from a domestic switch, the transaction authorization request including a token and transaction information, the token being received by the domestic switch from a merchant, wherein the token is associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) performing de-tokenization on the token to identify the payment account credentials; and

(c) sending the payment account credentials to the domestic switch to facilitate authorization of the transaction by an issuer of the payment account.

2. The payment transaction system claimed in claim 1, wherein the payment account is an account associated with an issuer.

3. The payment transaction system claimed in any one of claims 1 to 2, wherein after the step of sending the payment account credentials to the domestic switch, the payment transaction system is further configured to perform the steps of:

(d) receiving, from the domestic switch, message data indicating approval of the transaction; and

(e) sending the message data to a mobile computing device associated with a user.

4. The payment transaction system claimed in any one of claims 1 to 2, wherein after the step of sending the payment account credentials to the domestic switch, the payment transaction system is further configured to perform the steps of:

(d) receiving, from the domestic switch, message data indicating declination of the transaction; and

(e) sending the message data to a mobile computing device associated with a user.

5. The payment transaction system claimed in any one of claims 1 to 4, wherein the domestic switch receives the transaction authorization request from an acquirer, the acquirer having received the transaction authorization request from the merchant.

6. The payment transaction system claimed in any one of claims 1 to 5, wherein the token is received by the payment transaction system from a mobile computing device, via the domestic switch.

7. A payment transaction system for processing a tokenized transaction, the payment transaction system comprising:

a payment network server;

a domestic switch for sending an authorization request to the payment network server; and

the domestic switch and payment network server together comprising one or more processors in communication with a non-transitory data storage medium having instructions stored thereon which, when executed by the one or more processors, configure the payment transaction system to perform the steps of:

(a) receiving, at the domestic switch, a transaction authorization request from a request system, the transaction authorization request including a token received from a merchant, the token being associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) identifying, at the domestic switch, a payment account and issuer associated with the token;

(c) sending the transaction authorization request, from the domestic switch to the payment network server, the transaction authorization request including the token;

(d) performing, at the payment network server, de-tokenization on the

token to identify the payment account credentials;

(e) sending the payment account credentials, from the payment network server to the domestic switch, to facilitate authorization of the transaction;

(f) responsive to receipt of the payment account credentials, at the domestic switch, determining if the transaction authorization request is approved; and

(g) responsive to a determination that the transaction authorization request is approved, at the domestic switch, sending message data indicating that the transaction authorization request is approved to the request system.

8. The system claimed in claim 7, wherein the step of determining if the transaction authorization request is approved includes:

(f1) sending, to the issuer system, message data including an authorization request;

(f2) receiving, from the issuer system, message data including authorization request status; and

(f3) responsive the authorization request status indicates approval for making the transaction, determining that the transaction authorization request is approved.

9. The system claimed in claim 7 or 8, wherein the payment network server is a third party processor system.

10. A method for processing a tokenized transaction, the method being performed by a payment transaction system and comprising:

(a) receiving a transaction authorization request, from a domestic switch, the transaction authorization request including a token and transaction information, the token being received by the domestic switch, from a merchant, wherein the token is associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) performing de-tokenization on the token to identify the payment

account credentials; and

(c) sending the payment account credentials to the domestic switch to facilitate authorization of the transaction by an issuer of the payment account.

11. A method for processing a tokenized transaction, the method performed by a payment transaction system comprising:

a payment network server;

a domestic switch for sending an authorization request to the payment network server; and

the domestic switch and payment network system together comprising one or more processors in communication with a non-transitory data storage medium having instructions stored thereon which, when executed by the one or more processors, configure the payment transaction system to perform the steps of:

(a) receiving, at the domestic switch, a transaction authorization request from a request system, the transaction authorization request including a token received from a merchant, the token being associated with payment account credentials of a payment account for use in the tokenized transaction;

(b) identifying, at the domestic switch, a payment account and issuer associated with the token;

(c) sending the transaction authorization request, from the domestic switch to the payment network server, the transaction authorization request including the token;

(d) performing, at the payment network server, de-tokenization on the token to identify the payment account credentials;

(e) sending the payment account credentials from the payment network server to the domestic switch to facilitate authorization of the transaction;

(f) responsive to receipt of the payment account, at the domestic switch, determining if the transaction authorization request is approved; and

(g) responsive to a determination that the transaction authorization request is approved, at the domestic switch, sending message data indicating that the transaction authorization request is approved to the request

system.

12. The system claimed in claim 11, wherein the step of determining if the transaction authorization request is approved includes:

(f1) sending, to the issuer system, message data including an authorization request;

(f2) receiving, from the issuer system, message data including authorization request status; and

(f3) responsive the authorization request status indicates approval for making the transaction, determining that the transaction authorization request is approved.