US 20140372321A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2014/0372321 A1

(43) Pub. Date: Dec. 18, 2014

Khan

(54) **SECURE AUTHENTICATION BETWEEN MULTIPLE PARTIES**

(71) Applicant: **EBAY INC.**, San Jose, CA (US)

(72) Inventor: **Khurram Khan**, San Jose, CA (US)

(21) Appl. No.: **14/472,052**

(22) Filed: **Aug. 28, 2014**

Related U.S. Application Data

(63) Continuation of application No. 12/494,652, filed on Jun. 30, 2009, now Pat. No. 8,825,548.

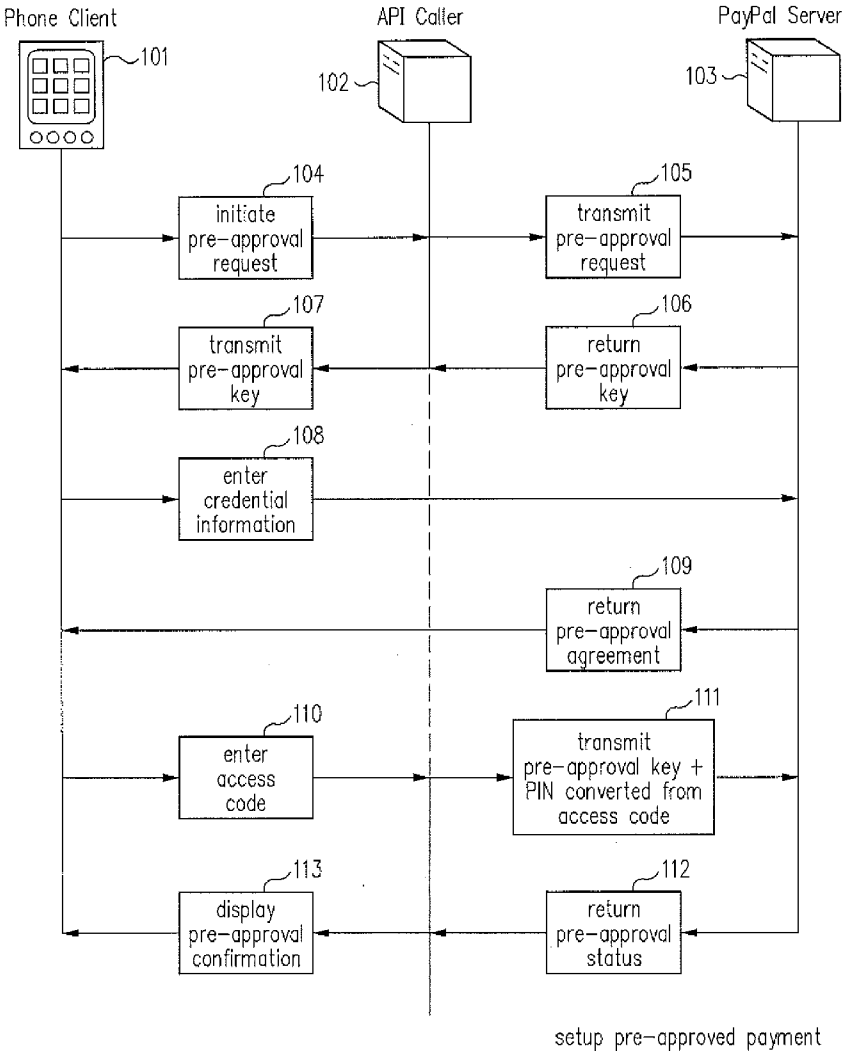
Publication Classification

(51) **Int. Cl.**
G06Q 20/40 (2006.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/4012*** (2013.01)
USPC **705/72**

(57) **ABSTRACT**

Systems and methods are disclosed herein to allow a party to a multiple-party transaction to perform authentications using identification information received from another party while allowing the party generating the identification information to maintain confidentiality of information. A user may enter an access code to identify the user to a first party that will be generating identification information to a second party in the transaction. The access code may be entered without requiring the entry of an alphanumeric PIN (Personal Identification Number). The first party may convert the access code to a second code for transmission to the second party so that the access code is not revealed to the second party. The second party may use the second code to authenticate the user, to authenticate a payment transaction or other types of communications from the user or the first party. Thus, parties in a multiple-party transaction may perform authentications while maintaining the confidentiality of information.



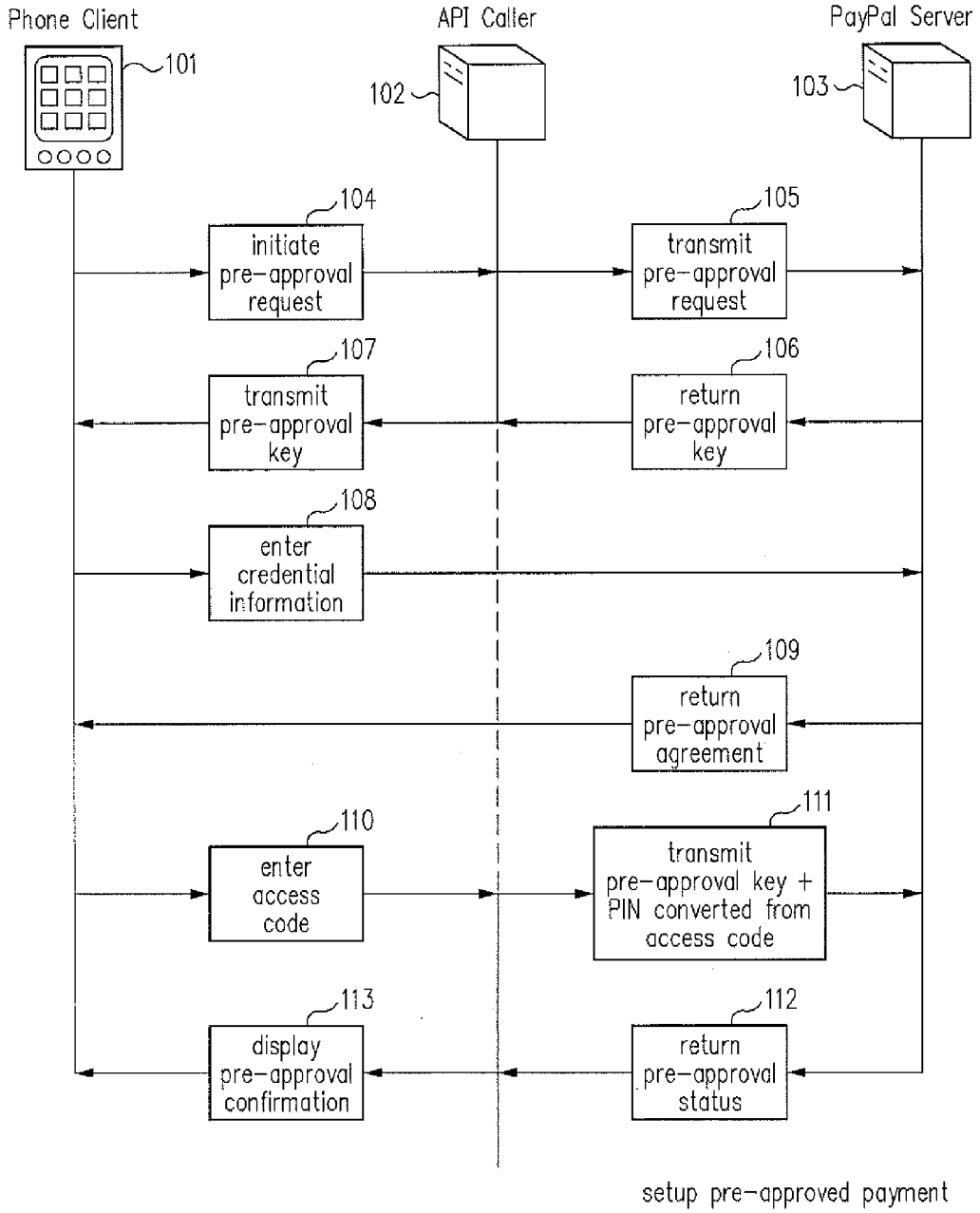

Phone Client
101
API Caller
102
PayPal Server
103
104
initiate pre-approval request
105
transmit pre-approval request
107
transmit pre-approval key
106
return pre-approval key
108
enter credential information
109
return pre-approval agreement
110
enter access code
111
transmit pre-approval key + PIN converted from access code
113
display pre-approval confirmation
112
return pre-approval status
setup pre-approved payment

FIG. 1

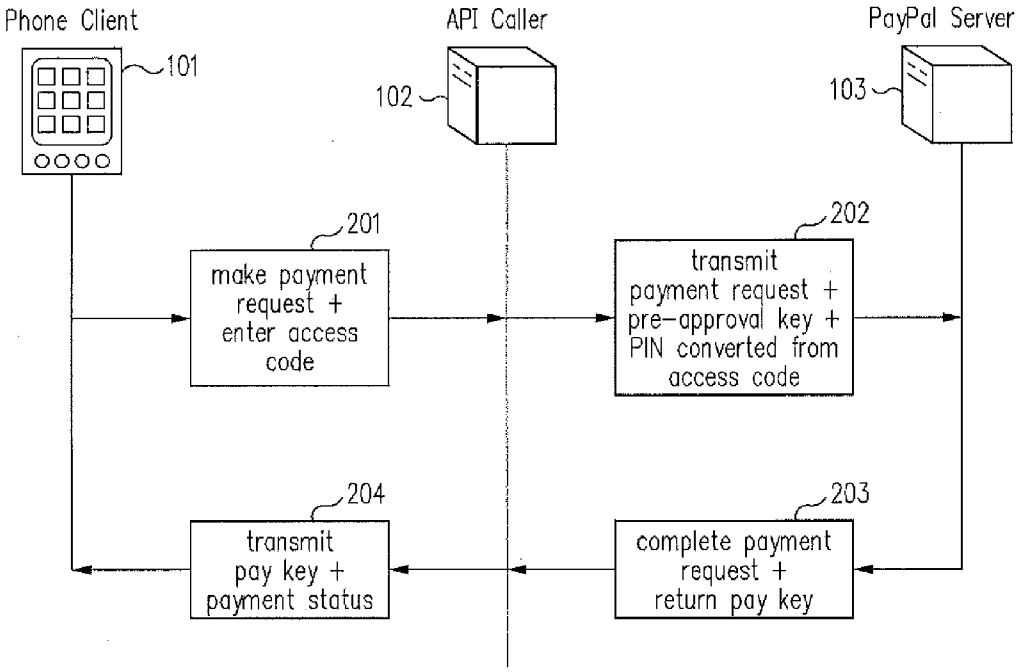
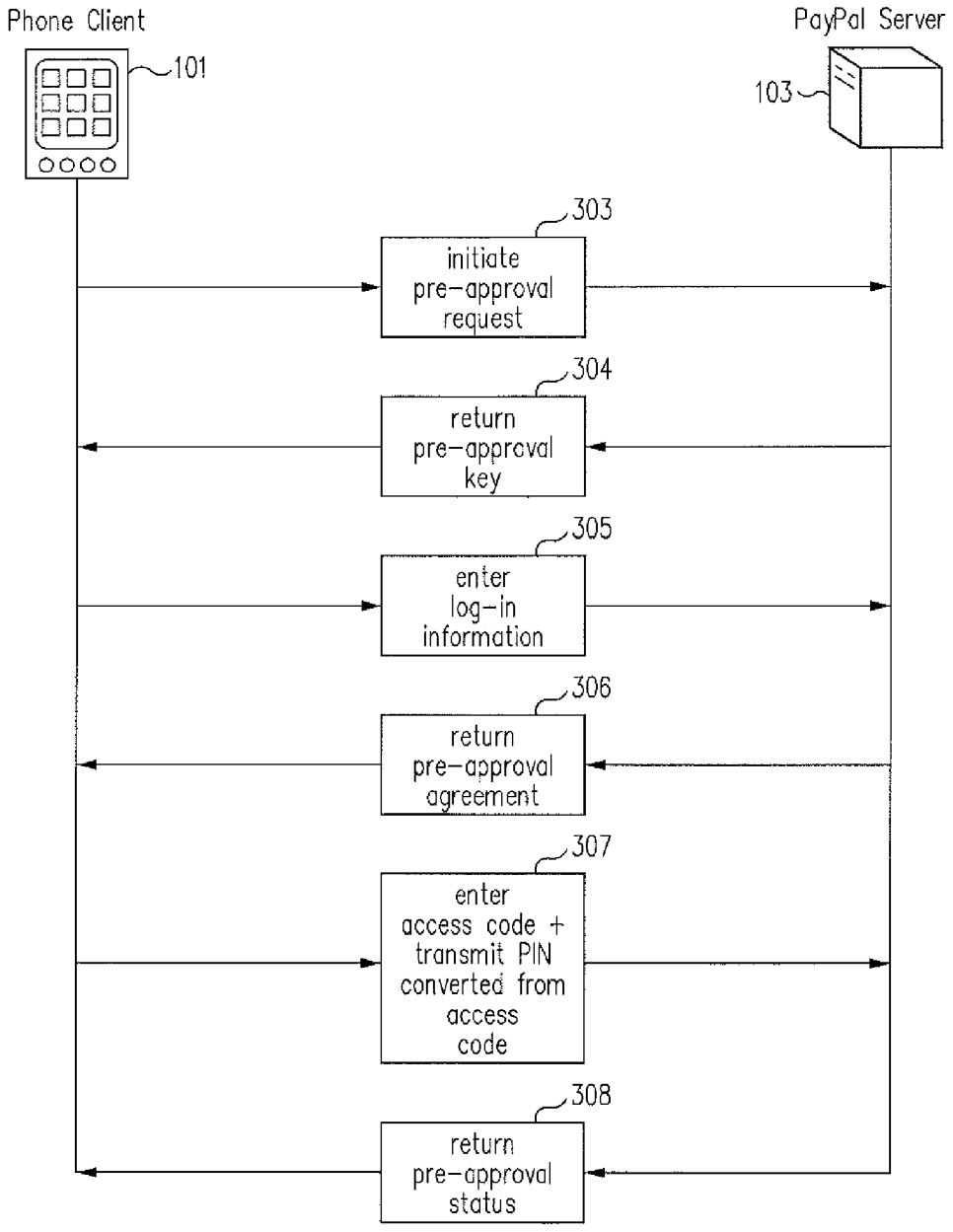

Phone Client
101
API Caller
102
PayPal Server
103
201
make payment request + enter access code
202
transmit payment request + pre-approval key + PIN converted from access code
204
transmit pay key + payment status
203
complete payment request + return pay key
make payment request using pre-approved amount

FIG. 2



setup pre-approved money transfer

FIG. 3

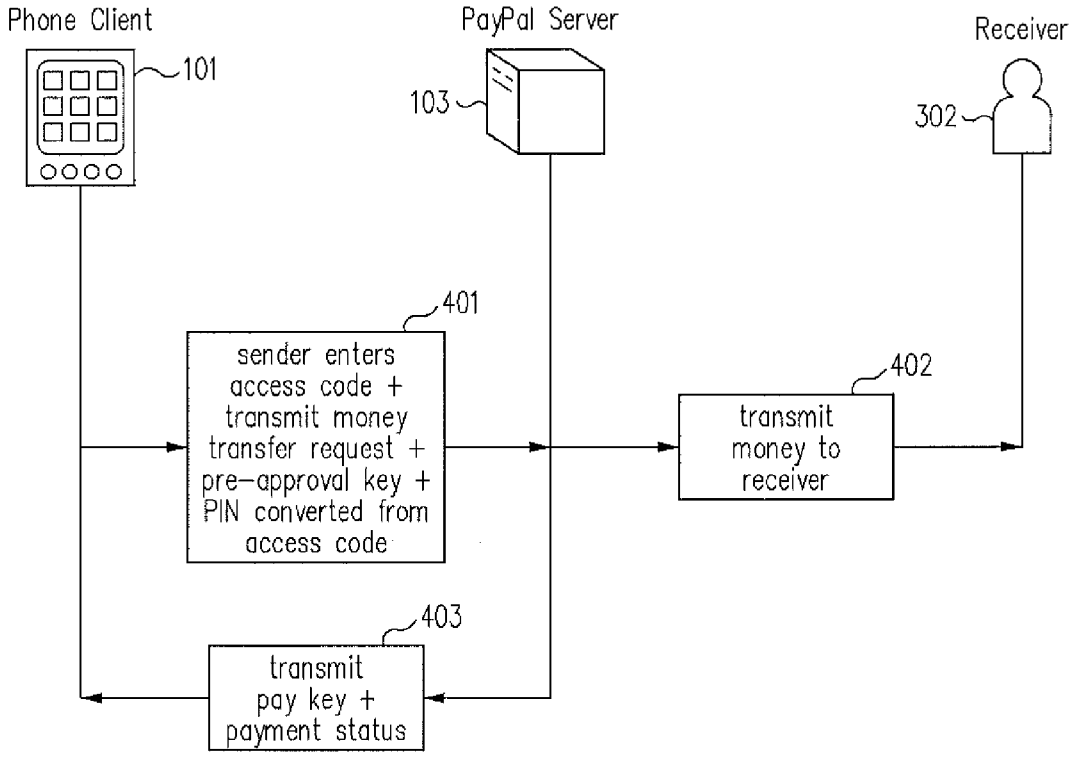

Phone Client
101
PayPal Server
103
Receiver
302
401
sender enters access code + transmit money transfer request + pre-approval key + PIN converted from access code
402
transmit money to receiver
403
transmit pay key + payment status
make money transfer request using pre-approved money

FIG. 4

SECURE AUTHENTICATION BETWEEN MULTIPLE PARTIES

CROSS REFERENCE TO RELATED APPLICATION

[0001] This patent application is a continuation of U.S. patent application Ser. No. 12/494,652 filed on Jun. 30, 2009, which is incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates generally to online payment transactions. In particular, the present disclosure relates to methods and systems for authentication while maintaining confidentiality of information for online payment transactions involving multiple parties.

BACKGROUND

[0003] Online payment transactions have greatly facilitated the purchase of goods, services, and the movement of money over the Internet. In online payment transactions, multiple parties are frequently involved. For example, a user may use a portable device to access a merchant's website to make purchases and to request that payments for the purchases be transferred from the user's account with a payment provider such as PayPal to the merchant's account. To complete the purchase, the user needs to authorize the payment transaction with the payment provider. Authorization of the payment transaction may require the user to enter identification information such as a PIN (Personal Identification Number) that is known only to the user and the payment provider so that the payment provider may authenticate the user. However, there are times when the payment provider may receive the identification information from a third party. For example, a user may desire to make multiple purchases from a merchant at different times. To facilitate online payment transactions for multiple purchases from the same merchant or for scenarios where the user may be unavailable to authorize each payment transaction, it is desirable to allow a user to pre-approve future payment or payments to an online merchant prior to the purchase. Payment pre-approval enables the user to return multiple times to a merchant to make purchases without having to return to the payment provider to authorize a payment for each purchase. To prevent fraudulent purchases by unauthorized users using the pre-approved payment, the payment provider may require identification information of the user from the merchant or other third party for the payment provider to authenticate the transaction. The identification information may be information that is disclosed by the user only to the merchant or other third party such that revealing the identification information to the payment provider may breach the confidentiality of the information. Therefore, it is desirable to enable authentication in transactions involving multiple parties while allowing the parties to maintain the confidentiality of information shared between the parties.

BRIEF SUMMARY

[0004] Systems and methods are disclosed herein to allow a party to a multiple-party transaction to perform authentications using identification information received from another party while allowing the party generating the identification information to maintain confidentiality of information not to be shared. A user may enter an access code to identify the user to a first party that will be generating the identification information to a second party in the transaction. The access code may be entered without requiring the entry of an alphanumeric PIN (Personal Identification Number). The first party may convert the access code to a second code representing the identification information for transmission to the second party so that the access code is not revealed to the second party. The second party may use the second code to authenticate the user, to authenticate a payment transaction, or to authenticate other types of communications from the user or the first party. Thus, parties in a multiple-party transaction may perform authentications while maintaining the confidentiality of the access code. For example, a user using a mobile phone to access a merchant's website may identify him/her to the mobile phone using an access code such as a pattern of finger movement over the touch screen, a voice phrase, an image, the user's biometric information, or even the way a phone is moved. The mobile phone converts the access code to an alphanumeric code. The mobile phone transmits the alphanumeric code to the payment provider through the merchant's website such that the payment provider may use the alphanumeric code to authenticate the user for payment transactions. Therefore, the payment provider is able to authenticate the user without requiring the mobile phone to reveal the access code.

[0005] In accordance with one or more embodiments of the present disclosure, a payment authentication apparatus includes a processor on a server, and a memory to store machine-readable instructions for execution by the processor to provide a payment authentication application. The payment authentication application receives a payment request PIN of a user from a merchant or a communication device, compares the payment request PIN against a stored PIN of the user to authenticate a payment request. The payment request PIN is derived from an access code received from a consumer and the access code is hidden from the payment authentication application.

[0006] In accordance with one or more embodiments of the present disclosure, a method for authenticating a payment request by a payment provider includes receiving a payment request PIN of a user pre-approval key from a merchant or a communication device, where the payment request PIN is derived from an access code that is received from a consumer and the access code is hidden from the payment provider, verifying the payment request PIN against a stored PIN of the user, and approving the payment request.

[0007] In accordance with one or more embodiments of the present disclosure, a computer program in a payment authentication device includes a computer readable medium having instruction code for execution by a processor to perform a method. The method includes receiving a payment request PIN of a user from a merchant or a communication device, where the payment request PIN is derived from an access code received from a consumer and the access code is hidden from the computer program product, verifying the payment request PIN of the user against a stored PIN of the user, and approving the payment request.

[0008] These and other embodiments of the present disclosure will be more fully understood by reference to the following detailed description of the embodiments when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. **1** shows transactions between multiple parties to set up a pre-approved payment with a payment provider

using a PIN derived from an access code according to one or more embodiments of the present disclosure;

[0010] FIG. **2** shows transactions between multiple parties when an user makes a payment using a pre-approved amount according to one or more embodiments of the present disclosure;

[0011] FIG. **3** shows transactions between multiple parties to set up pre-approved money transfer with a payment provider using a PIN derived from an access code according to one or more embodiments of the present disclosure;

[0012] FIG. **4** shows transactions between multiple parties when a sender makes a money transfer request on behalf of the payment account holder to a receiver using pre-approved money according to one or more embodiments of the present disclosure;

[0013] Embodiments of the present disclosure and their advantages are best understood by referring to the detailed description that follows. It should be appreciated that like reference numerals are used to identify like elements illustrated in one or more of the figures.

DETAILED DESCRIPTION

[0014] Systems and methods are disclosed herein to allow a party to a multiple-party transaction to perform authentications of users, transactions, or other types of communications using identification information received from another party while allowing the party generating the identification information to maintain confidentiality of information when generating the identification information. In multi-party transactions, authentications may have to be performed by a party using information provided by other parties to the transaction. The information passed between multiple parties may contain identification information such as an alphanumerical PIN to enable the receiving party to configure a user account, to authenticate the user against the user account, or to verify the authenticity of a communication. Embodiments of the present disclosure allow the party generating the identification information to derive the identification information from a non-alphanumerical access code selected by the user.

[0015] Transmission of the derived identification information instead of the access code allows the generating party to maintain the confidentiality of the access code. For example, a multi-party transaction may involve a user using a portable device to access a merchant's website to make purchases. The user may request that the payment for the purchases be transferred from a pre-approved payment account with a payment provider such as PayPal to the merchant's account. To facilitate payment transactions using the pre-approved payment account, PayPal may not require the user to log on to the user's account to authorize the payment request. Instead, PayPal may authenticate the payment request using identification information received from the merchant's website or the portable device. Therefore, the merchant's website or the portable device may request the user to enter an access code.

[0016] The access code selected by the user may be a pattern of finger movement over the touch screen, a voice phrase, an image, biometric information such as fingerprints, or even the way the portable device is moved. The merchant's website or the portable device may convert the access code into an alphanumerical PIN code for transmission to PayPal. When the user initially signed up for the pre-approved payment account, PayPal had also stored the alphanumerical PIN code for configuring the account. Thus, PayPal verifies the received alphanumerical PIN code against the stored alphanumerical PIN code to authenticate the payment request while allowing the merchant's website or the portable device to maintain the confidentiality of the access code.

[0017] FIG. **1** shows transactions between multiple parties to set up pre-approved payments with a payment provider using a PIN derived from an access code according to one or more embodiments of the present disclosure. The multiple parties are a phone client **101**, an API caller **102** representing a merchant website or a phone client website acting as a facilitator for a merchant, and a payment provider such as the PayPal server **103**. A user using the phone client **101** accesses API caller **102** and makes purchases through API caller **102** using PayPal server **103** as the payment provider. In the conventional case of a single transaction with no pre-approved payments, the user is asked to log-in to the user's PayPal account to authorize a payment or, for a new user, asked to establish an account before the user may request payment authorization. The user may establish an account and/or log-in using a PIN that is known only to the user and PayPal server **103** and may interact directly with PayPal server **103** to authorize the payment. Alternatively, the user may desire to make multiple purchases through API caller **102** over a period of time.

[0018] To facilitate multiple purchases through API caller **102** without requiring the user to log-in to PayPal server **103** to authorize each purchase payment, it may be convenient for the user to request a pre-approval amount to be applied for future purchases. Thereafter, when the user makes a purchase through API caller **102**, API caller **102** may interact with PayPal server **103** to authorize the payment using the pre-approved amount. Because the user does not interact directly with PayPal **103** to authorize payments using the pre-approved payment, API caller **102** may have to provide identification information of the user to PayPal server **103** to enable PayPal server **103** to authenticate the user and the transaction.

[0019] In one or more embodiments of the present invention, the phone client **101** generates the identification information from a user-entered access code and transmits the identification information to PayPal server **103** through API caller **102**. The access code is confidential to the phone client **101** and generation and transmission of the identification information rather than the access code allows the phone client **101** to maintain the confidentiality of the access code while enabling PayPal sever **103** to authenticate the transaction. The phone client **101** also generates the identification information from the access code and transmits the identification information to PayPal server **103** when the user initially requests the pre-approved amount from PayPal server **103**. PayPal server **103** then stores the identification information to associate the user with the pre-approved amount so that PayPal server **103** may authenticate the user when the user makes future payment requests using the pre-approved amount.

[0020] In step **104**, the user using the phone client **101** connects with API caller **102** to initiate the pre-approval request. The phone client **101** may be a Google G1 phone, an iPhone, other types of smart phones, a PDA, a laptop, or other types of communication devices. API caller **102** displays a screen on the phone client **101** for the user to sign up for the pre-approved payment through PayPal. The user may elect to sign up for the pre-approved payment and may be requested to fill out payment constraint information on API caller **102**. Payment constraint information allow the user to customize the pre-approval request by, for example, allowing the user to

set limits on the total pre-approved amount, the maximum amount per transaction, or to specify an expiration date etc. API caller **102** makes a pre-approval API call to PayPal sever **103** to transmit the pre-approval request in step **105**.

[0021] PayPal server **103** processes the pre-approval request and returns back a pre-approval key in step **106** to API caller **102**. The pre-approval key can be considered a token returned by the PayPal server **103** to uniquely identify the pre-approved payment associated with the pre-approval request for future purchases. This pre-approval key is to be submitted to PayPal server **103** when the user makes future payment requests to PayPal Server **103** to authorize purchase payments using the pre-approved payment. PayPal sever **103** may also return a pre-approval URL to API caller **102**. API caller **102** transmits the pre-approval key and the pre-approval URL back to the phone client in step **107**. The pre-approval URL directs the user to the PayPal server **103** and the user is prompted to enter credential information for the pre-approval agreement. If the user does not have an account with PayPal, the user will be asked to establish an account name and a password. Otherwise, the user will be asked to log-in to the user's PayPal account. The phone client **101** then makes an API authentication call to PayPal **103** to transmit the credential information in step **108**.

[0022] PayPal server **103** processes the credential information and responds with confirmation status information and details of the pre-approval agreement in step **109**. Phone client **101** then displays the confirmation status and details of the pre-approval agreement to the user for approval. The details of the pre-approval agreement may include the payment constraint information the user entered earlier in step **104** such as the total pre-approved amount, the expiration date, and the maximum amount per transaction. The pre-approval agreement may require the user to enter a PIN to allow PayPal server **103** to associate the user with the pre-approved payment so that PayPal server **103** may authenticate future purchases made by the user using the pre-approved payment. As mentioned, the PIN may be generated from an access code to maintain the confidentiality of the access code.

[0023] In step **110**, user approves the pre-approval agreement and enters an access code. The access code may be a pattern of finger movement over the touch screen, a voice phrase, an image, biometric information such as fingerprints, or even the way the portable device is moved. Phone client **101** may convert the access code to a PIN and transmit the PIN along with the user's approval of the pre-approval agreement to API caller **102**. Alternatively, phone client **101** may transmit the access code to API caller **102** for API caller **102** to convert the access code to the PIN. In step **111** API caller **102** makes another API call to PayPal server **103** to transmit the pre-approval key and the PIN to PayPal server **103**. PayPal server **103** processes the API call, stores the PIN, associates the pre-approval key with the PIN, and returns pre-approval status in step **112** to API caller **102**. Finally, API caller **102** displays a pre-approval confirmation page to phone client **101** in step **113**.

[0024] FIG. **2** shows transactions between multiple parties when a user makes a payment request using the pre-approved payment according to one or more embodiments of the present disclosure. After the user has signed up with a payment provider for a pre-approved payment to be used with a merchant, the user may proceed to make purchases from the merchant. The multiple parties are again a phone client **101**, an API caller **102** representing a merchant website or a phone client website acting as a facilitator for a merchant, and a payment provider such as the PayPal server **103**. To facilitate the transaction, API caller **102** may interact with PayPal server **103** to authorize payments using the pre-approved payment. Because the user does not interact directly with PayPal **103** to authorize payments, API caller **102** has to provide a PIN to PayPal server **103** to enable PayPal server **103** to authenticate the user and the transaction. This PIN is the same PIN that was received by PayPal server **103** when the user initially signs up for the pre-approved payment. The PIN is also generated from the same access code entered when the user initially signs up for the pre-approved payment in order to maintain the confidentiality of the access code.

[0025] In step **201**, the user using the phone client **101** connects with the API caller **102** to select items for purchase. When the user is ready to make the purchase, the phone client **101** may display a screen to allow the user to pay using the pre-approved payment from PayPal. When the user makes a payment request to use the pre-approved payment, the phone client **101** prompts the user to enter the access code. The user enters the same access code that was entered when the user signed up for the pre-approval amount. As before, the access code may be a pattern of finger movement over the touch screen, a voice phrase, an image, biometric information such as fingerprints, or even the way the portable device is moved. As before, phone client **101** may convert the access code to a PIN and transmit the PIN to API caller **102**. Alternatively, phone client **101** may transmit the access code to API caller **102** for API caller **102** to convert the access code to the PIN.

[0026] In step **202**, API caller **102** makes an API call with the payment request, the PIN, and the pre-approval key received during the pre-approval request process to PayPal server **103**. PayPal server **103** uses the PIN and the pre-approval key to authenticate the user and to process the payment request. Upon approval, PayPal server **103** transfers the payment to complete the payment request, and responds with payment status and a pay key in step **203**. In step **204**, API caller **102** transmits the payment status and a pay key to the phone client **101**. The pay key is considered a token returned by PayPal server **103** to uniquely identify the payment request. Upon receiving the payment status and the pay key, the phone client **101** displays a confirmation page to the user.

[0027] FIG. **3** shows transactions between multiple parties to set up a pre-approved money transfer with a payment provider using a PIN derived from an access code according to one or more embodiments of the present disclosure. A pre-approved money transfer may be used in scenario where a payment account owner wants another party, called the sender, to have restricted access right to send money from the payment account owner's PayPal account on behalf of the payment account owner without requiring the sender to log-in to the payment account owner's PayPal account. Of course, a payment-approved money transfer may also be initiated by the payment account owner when it's inconvenient for the payment account owner to log-in to the owner's PayPal account. Pre-approved money transfer differs from the pre-approved payment of FIGS. **1** and **2** in that the sender transfers money from the payment account owner's PayPal account without calling explicitly for the exchange of goods or services. Thus, a merchant may not necessarily be a party to the transactions, although it can be.

[0028] The multiple parties are a phone client **101**, a receiver **302** of FIG. **4**, and a payment provider such as the PayPal server **103**, The phone client **101** may be used initially

by the PayPal account owner to request pre-approval of the money transfer and also by the sender to make money transfer requests on behalf of the PayPal account owner to the receiver **302**. Because the sender interacts with PayPal server **103** to authorize money transfer using the pre-approved money without logging into the PayPal account holder's account, the sender may have to provide identification information of the payment account holder to enable PayPal server **103** to authenticate the money transfer request.

[0029] In one or more embodiments of the present invention, the phone client **101** generates the identification information from a sender-entered access code and transmits the identification information to PayPal server **103**. Similar to the pre-approved payment scenario, the access code is confidential to the phone client **101** and transmission of the identification information rather than the access code allows the phone client **101** to maintain the confidentiality of the access code while enabling PayPal sever **103** to authenticate the request. The phone client **101** also generates the identification information from the access code and transmits the identification information to PayPal server **103** when the PayPal account holder initially signs up for the pre-approved money transfer from PayPal server **103**. PayPal server **103** then stores the identification information to associate the PayPal account holder with the pre-approved money transfer amount so that PayPal server **103** may authenticate a sender with knowledge of the access code when the sender make future money transfer requests using the pre-approved money.

[0030] In step **303**, the PayPal account holder using the phone client **101** connects with PayPal server **103** to initiate the pre-approval request. PayPal server **101** displays a screen on the phone client **101** for the user to sign up for the pre-approved money transfer through PayPal. The PayPal account holder may elect to sign up for the pre-approved money transfer and may be requested to fill out transfer constraint information on PayPal server **103**. The transfer constraint information allows the user to customize the pre-approval request by, for example, allowing the user to set limits on the total pre-approved amount, the maximum amount per transfer, or to specify an expiration date etc.

[0031] Phone client **101** makes a pre-approval API call to PayPal sever **103** to transmit the pre-approval request with the transfer constraint information. PayPal server **103** processes the pre-approval request and returns back a pre-approval key in step **304** to phone client **101**. The pre-approval key can be considered a token returned by PayPal server **103** to uniquely identify the pre-approved amount associated with the pre-approval request for future money transfers. This pre-approval key is to be submitted to PayPal server **103** when the sender makes future requests to PayPal Server **103** to authorize money transfer using the pre-approved payment. The PayPal account holder is prompted to login to the account holder's PayPal account. The phone client **101** then makes an API authentication call to transmit the login information to PayPal **103** in step **305**. PayPal server **103** processes the login information and responds with confirmation status information and details of the pre-approval agreement in step **306**. Phone client **101** then displays the confirmation status and details of the pre-approval agreement to the PayPal account holder for approval.

[0032] The details of the pre-approval agreement may include the transfer constraint information the user entered earlier in step **303** such as the total pre-approved amount, the expiration date, and the maximum amount per transfer. The pre-approval agreement may require the user to enter a PIN to allow PayPal server **103** to associate the PayPal account holder with the pre-approved money transfer so that PayPal server **103** may authenticate future money transfer requests made by the PayPal account holder or the sender. As before, the PIN may be generated from an access code to maintain the confidentiality of the access code. In step **307**, the PayPal account holder approves the pre-approval agreement and enters an access code. As before, the access code may be a pattern of finger movement over the touch screen, a voice phrase, an image, biometric information such as fingerprints, or even the way the portable device is moved. Phone client **101** may convert the access code to a PIN and make an API call to transmit the PIN along with the pre-approval key to PayPal server **103**. PayPal server **103** processes the API call, stores the PIN, associates the pre-approval key with the PIN, and returns pre-approval status in step **308** to the phone client **101** for the phone client **101** to display a pre-approval confirmation to the PayPal account holder.

[0033] FIG. **4** shows transactions between multiple parties when a sender makes a money transfer request on behalf of the payment account holder to a receiver using pre-approved money according to one or more embodiments of the present disclosure. After the payment account holder has signed up with a payment provider for pre-approved transfer money, the sender may have restricted access right to transfer money from the payment account holder's account on behalf of the payment account holder. The multiple parties are a phone client **101**, a receiver **302**, and a payment provider such as the PayPal server **103**. Because the sender does not log into a PayPal account holder's account to authorize money transfer, the sender has to provide a PIN to PayPal server **103** to enable PayPal server **103** to authenticate the sender and the money transfer. This PIN is the same PIN that was received by PayPal server **103** when the PayPal account holder initially signs up for the pre-approved money transfer. The PIN is also generated from the same access code entered by the PayPal account holder when the PayPal account holder initially signs up for the pre-approved money transfer in order to maintain the confidentiality of the access code.

[0034] In step **401**, the sender using the phone client **101** connects with the PayPal server **102** to request money transfer on behalf of the PayPal account holder. The phone client **101** may display a screen to allow the sender to request money transfer using the pre-approved transfer money from PayPal. When the sender makes a money transfer request to use the pre-approved money, the phone client **101** prompts the sender to enter the access code. The sender enters the same access code that was entered when the PayPal account holder initially signed up for the pre-approval money. As before, the access code may be a pattern of finger movement over the touch screen, a voice phrase, an image, biometric information such as fingerprints, or even the way the portable device is moved.

[0035] Phone client **101** may convert the access code to a PIN and make an API call with the money transfer request, the PIN, and the pre-approval key received during the pre-approval request process to PayPal server **103**. PayPal server **103** uses the PIN and the pre-approval key to authenticate the user and to process the money transfer request. Upon approval, PayPal server **103** transfers money from the PayPal account holder's account to the receiver **302** in step **402** to complete the transfer request, and responds with payment status and a pay key in step **403**. The pay key is considered a

token returned by PayPal server **103** to uniquely identify the money transfer request. Upon receiving the payment status and the pay key, the phone client **101** display a confirmation page to the sender.

[0036] Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the spirit of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components, and vice-versa.

[0037] Application software in accordance with the present disclosure, such as program code and/or data for processing the payment or money transfer request, may be stored on one or more computer readable mediums. It is also contemplated that the application software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

[0038] Although embodiments of the present disclosure have been described, these embodiments illustrate but do not limit the disclosure. For example, use of a non-alphanumeric access code with a phone client is described; however other types of access code may also be suitable for use on other types of hardware platform. In addition, although PayPal is used as the payment service provider in the embodiments, any suitable on-line payment provider or financial services provider may be used to process pre-approval, payment, or money transfer requests from the hardware platform. It should also be understood that embodiments of the present disclosure should not be limited to these embodiments but that numerous modifications and variations may be made by one of ordinary skill in the art in accordance with the principles of the present disclosure and be included within the spirit and scope of the present disclosure as hereinafter claimed.

We claim:

1. A system comprising:

a non-transitory memory comprising information for an account of a user; and

one or more hardware processors in communication with the non-transitory memory and configured to:

process an approval request to generate a payment key, wherein the approval request comprises an agreement to make payments from the account of the user to a merchant;

communicate the payment key to the merchant and the user;

receive login information for the account;

receive a personal identification number (PIN) from the user, wherein the PIN authenticates the user during use of the payment key by the merchant;

associate the PIN with the payment key using the login information;

receive a payment request including the PIN and the payment key from the merchant;

verify the PIN and the payment key to authorize the payment request without requiring the login information for the account; and

transfer a payment for the payment request from the account of the user to the merchant.

2. The system of claim **1**, wherein the PIN is generated from an access code entered by the user using a user device.

3. The system of claim **2**, wherein the PIN is generated by one of the user device and a merchant device for the merchant.

4. The system of claim **1**, wherein the login information is received from a communication device.

5. The system of claim **4**, wherein the login information is not provided to the merchant.

6. The system of claim **5**, wherein the communication device prevents the login information from being provided to the merchant.

7. The system of claim **4**, wherein the payment request is received from the communication device.

8. The system of claim **1**, wherein the login information comprises an account identifier and an authorization password.

9. A method comprising:

processing, using one or more hardware processors, a payment request to generate a key, wherein the payment request comprises a request to make payments from an account of a user to a merchant;

communicating the key to the merchant and the user;

receiving credential information for the account;

receiving a personal identification number (PIN) from the user, wherein the PIN authenticates the user during use of the key by the merchant;

associating the PIN with the key using the credential information;

receiving a payment authorization including the PIN and the key from the merchant;

verifying the PIN and the key to authorize the payment authorization without requiring the credential information for the account; and

transferring a payment for the payment authorization from the account of the user to the merchant.

10. The method of claim **9**, wherein the PIN is derived from an access code entered into a user device for the user.

11. The method of claim **10**, wherein the access code comprises a pattern of finger movement of the user entered into the user device.

12. The method of claim **10**, wherein the access code comprises biometric information of the user entered into the user device.

13. The method of claim **9**, wherein the approval request includes payment constraint information to set limits on the payment request.

14. The method of claim **9**, wherein at least one of the approval request and the payment request are received from the user.

15. The method of claim **9**, wherein at least one of the approval request and the payment request are received from the merchant.

16. The method of claim **9**, wherein the login information is received from the user, and wherein the merchant does not receive the login information.

17. The method of claim **9**, wherein the user communicates the login information to a device.

18. A non-transitory computer-readable medium comprising instructions which, in response to execution by a computer system, cause the computer system to perform a method comprising:

accessing, using one or more hardware processors, an approval request to generate a payment key, wherein the approval request comprises an agreement to make payments from an account of a user to a merchant;

transmitting the payment key to the merchant and the user;

receiving login information for the account;

receiving a personal identification number (PIN) from the user, wherein the PIN authenticates the user during use of the payment key by the merchant;

associating the PIN with the payment key using the login information;

receiving a payment request including the PIN and the payment key from the merchant;

processing the PIN and the payment key to authorize the payment request without requiring the login information for the account; and

processing a payment for the payment request from the account of the user to the merchant.

19. The non-transitory computer-readable medium of claim **18**, wherein the approval request is received from a merchant device acting as a facilitator for transactions with the merchant.

20. The non-transitory computer-readable medium of claim **19**, wherein the payment request is received from the merchant device.

* * * * *